FEDERAL TRADE COMMISSION

INDEX

Session 2 (continued/morning):

Session 3 (afternoon): 148

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY

SESSION THREE: CONSUMER ONLINE PRIVACY (CONTINUED)

Thursday, June 12, 1997

Volume 3

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

The above-entitled matter came on for public hearing, pursuant to notice, at 9:00 a.m.

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

David Medine, Associate Director for Credit Practices, Chairman

Commissioner Starek

Commissioner Varney

Martha Landesberg, Attorney

Lisa Rosenthal, Attorney

P R O C E E D I N G S

- - - - -

MR. MEDINE: Good morning and welcome to the third day of the FTC's privacy week and the last session on consumers' online privacy. This afternoon we will turn to the very important topic of children's online privacy. I want to mention that this morning's session on unsolicited commercial E-mail is being cybercast on Democracy.Net and listeners on Democracy.Net who wish to submit comments for the public record may do so at www.democracy.net, so we have an interactive session going on as we speak.

Again, this morning we're going to be focusing on the subject of unsolicited commercial E-mail and we're going to do that in three panels. The first will focus on who and what the practice is all about, how it takes place. The second panel will discuss what are the economic benefits and costs of the practice. And the third will discuss what controls, if any, are appropriate in addressing the practice.

Jason Catlett who is the CEO and founder of Junkbusters who was with us has agreed to come back again and give us a bit of education about unsolicited E-mail, so I'll turn it over to him.

PANEL V: UNSOLICITED COMMERCIAL E-MAIL: OVERVIEW

"Methods used, number and types of messages, sources of e-mail addresses and consumer and internet service provider (ISP) views."

Ram Avrahami

Jason Catlett, Chief Executive Officer, Junkbusters Corp.

Raymond B. Everett

Jill A. Lesser, Deputy Director, Law and Public Policy, America Online, Inc.

Simona Nass, Panix/Public Access Networks Corp.

George F. Nemeyer, Tigerden Internet Services, Internet Service Providers Consortium

Shabbir J. Safdar, Founder, Voters Telecommunications Watch

Sanford Wallace, President, Cyber Promotions, Inc.

***

MR. CATLETT: Thank you, David. I'm honored that the Commission staff has asked Junkbusters to present some examples of spam and to say a little bit about how spam factories work.

Junk E-mail probably causes more anger than any other issue on the Internet; however, I think it's worth trying to at least start with a dispassionate and rational examination of what spam is. We should even allow ourselves a little good humor while discussing this serious and important topic, because even spam can have its funny side in small quantities. In bulk, of course, it can cause substantial injury.

First, I would like to ask how many people here have received at least one piece of junk E-mail in their lives? How many have received at least 10? At least 100? It's still a substantial number. At least 1,000? Still a few hands. Anyone more than 10,000 pieces of junk mail? One. Anyone more than 100,000 pieces of mail? Well, we have something to be grateful for.

People who never received junk E-mail before are often kind of disappointed by their first piece. They've heard all these terrible things about junk E-mail and when they actually see some, it strikes them as pathetic and mundane. It's kind of like reading about Moses and the plague of locusts in the book of Exodus and then seeing a single dead grasshopper. Well, there's a big difference between one insect and a swarm of millions descending on your backyard.

Now Junkbusters has a sizable collection of junk E-mail in its forensic lab, but I was reluctant to present real examples before the Commission because we don't like to single out any individual for doing what's become a common practice. So, what I've done here is to put together a composite of parts taken from dozens of pieces of real spam, rather like than an Identikit portrait or an idealized botanical drawing.

The result might look to novices like a parody, but really everything that I'll show you today is fairly ordinary and representative of the kind of spam flying around the Internet as we speak. Not all junk E-mail looks like this, but much of it does.

Something you learn after reading a few hundred pieces of spam is that they come in different types. The amateur's junk is a very different species from what a spam factory produces, as different as a grasshopper and a cicada. The amateur's spam is much easier to exterminate than the professional's, so I've put together some idealized specimens of each. Let's dissect them.

For those of you listening on the Web broadcast you can find these specimens at URLJunkbusters.com/

spams.html.

This one briefly says, "Forgive the intrusion, but I'm compelled to tell you how to make a lot of money." It goes on with some multilevel marketing scheme pitches. The first characteristic we notice about it is it's a truly awful sales pitch. It's marginally literate, it's riddled with spelling errors, it's made up of patently false claims that are thrown together in an incoherent presentation that nobody able to read would seem likely to fall for.

Second, contrary to the end where the spammer tells us, "You are not on any mailing lists so there's no need to ask to be deleted," the recipient obviously is on a mailing list because he's received the spam. The spammer simply hasn't bothered to come up with an address where requests to remove can be sent.

The body text of the E-mail already suggests that the spammer is a novice, but what confirms this is the header information, most of which isn't displayed by the E-mail readers unless specifically requested.

The From, Received and Message ID headers are consistently indicating here that the spammer is sending E-mail through the Compuserve account and is asking for responses back to the Compuserve address. These amateurs are easy to deal with, simply send E-mail to the Postmaster or sometimes an account called Abuse at the company, in this case it's Compuserve, and they take care of it.

Almost all major online service companies have strict policies against spamming and they're pretty vigilant in terminating accounts that violate their terms of service. An angry recipient could also reply to this spammer directly and many do.

The good news is that most of these small-time spammers don't keep it up for long. The bad news is that they are being born in increasing numbers, so as many more people get on to the Internet more people get the impression that what spam promoters euphemistically call bulk commercial E-mail is a legitimate marketing tool. These small-time spammers are never going to use any remove list or E-mail preference service from anywhere.

The really bad news is that most spammers that do survive do so by learning to cover their tracks or they get software or a spam factory to do this for them. Let's look at a specimen from one of these electronic mills.

As a general -- the head of the body first, please, thanks. As a general rule you can believe exactly nothing that you read in spam, but some of the statements in this one are true, such as the claim that spamming is a numbers game. Most spammers don't bother to try to remove even undeliverable addresses from their lists because the cost to them of sending an additional piece of E-mail is such a minute fraction of a cent that it doesn't justify the slightest effort.

Another practice that's referred to in the slide coming up now -- number two, thanks, Larry -- is the practice of what's euphemistically called harvesting E-mail addresses. It's a euphemism, because harvesting implies that the harvester has planted some seed and it owns the land, which is simply untrue here. Junkbusters uses the term scavenging instead. Where do they get these addresses? They get them from Usenet groups, chat rooms, user directories and in certain circumstances a Web site can determine the E-mail address of a visitor to that site without their knowledge, although this is possible only in a small percentage of cases.

Another true statement in this spam is the fact that ISPs try to cut off spammers, and that spam factories also are run from Internet connection to Internet connection. In recent months a few major companies have announced policies which are tolerant or favorable towards spam and I hope that we'll hear from them today.

Many spam factories surreptitiously deliver their spams to unsuspecting sites to deliver for them. Older versions of the mail delivery software will do this. In the early days of the Internet this was regarded as a helpful feature. Now it's seen as a loophole for bandwidth thieves.

The subject title in the spam, "Don't ISPs Just Make You Mad" doesn't give any strong indication that the message is junk precisely because many people delete items of E-mail that are obviously spam before even displaying the full text of the mail.

The body copy of the spam accurately explains what is going on in these headers. The sender has removed all real E-mail addresses from the spam. The official-sounding Authenticated Sender and even the address of the person it was delivered to are fake. This surprises many recipients. The From and To addresses are the same nonexistent address. The dommain.com, with two Ms, doesn't exist.

A recipient that tried to reply to this address in the normal manner will only get an automated reply called a bounce from some innocent ISP, usually their own, saying that the mail could not be delivered. This wastes time and effort by computers and this cost is not borne by the spammer.

The spammer's instruction for removal at the bottom also goes to a nonexistent address. Some spammers choose addresses that do exist but unrelated to them. Others actually maintain their own pseudo-remove addresses but simply use the results as an additional source of addresses to spam. There are some independently run list cleaning sites that do really seem to work on certain high-volume spam factories, but most spammers will always ignore them.

Let's turn to the headers. The headers here contain a good deal of what's been called spamouflage, disinformation designed to placate or confuse the irate recipient and to thwart or weaken their efforts to stop the spam factory sending them more junk. Here at the bottom in caps the spammer seems to be trying to wrap himself in some anti-pornography flag, making himself appear more legitimate.

This spammer appears to be trying to move up the food chain positioning himself as a carrier of other people's spam rather than a producer, thereby evading responsibility for the injury caused by the spam. To me, the most offensive part of this header information is the offer for a product to filter unsolicited commercial E-mail called the Pro Tech Shun/Rack-It.

Finally, I'd like to draw your attention to a kind of spam that doesn't exist yet, and that's unsolicited E-mail from major marketing companies. We can only speculate on what this might look like based on the Direct Marketing Association's guidelines, which now permit DMA members to send spam, even though none of them I'm aware of are doing so.

A major company's spam would contain genuine instructions on how to request no further E-mail be sent from that company and also for all DMA members via their proposed

EMPS. The subject heading probably would still stress opportunity, but by the end of the first paragraph there would be a clear indication that the E-mail is a solicitation.

The body of the text might address you by name looked up from some commercial data base and it might refer to the Web site where your E-mail address was harvested, although they probably would not use the word "scavenged." The sales pitch would probably look much like the direct mail that you get in your physical mailbox, possibly without pictures but with more URLs.

The future I'm sketching might sound very similar to the physical present, but there's one very important economic difference. For each piece of physical direct mail you get somebody paid a dollar. For that dollar the same sender could afford to send upwards of 10,000 pieces of spam.

So I conclude with a note of warning, junk E-mail was a novelty two years ago, today it's a big problem. Two years from now it could easily be much, much worse and that's why we're here today.

MR. MEDINE: Thank you very much. Now, again, maybe you could just leave that last part up and a couple of questions. One is what is the incentive -- you talked about how the addresses, the return addresses, are not accurate indications of where the E-mail comes from. Do you know why there's such a great effort done to not put correct information there?

MR. CATLETT: Perhaps Sanford Wallace would like to answer that question.

MR. MEDINE: Well, why don't we -- he'll have a chance to discuss it --

MR. CATLETT: Well, my view is that they wish to avoid the inconvenience of people sending requests to remove the name from the list or worse. Spammers do receive a lot of abusive mail and they also seek to avoid that.

MR. MEDINE: Is that called flaming?

MR. CATLETT: Yes, that's correct.

MR. MEDINE: Is there any other indication on this message or a typical commercial E-mail message that would actually lead you to the source or is it possible to totally obfuscate the source of the E-mail?

MR. CATLETT: Typically the source is obfuscated. There's usually a post office box address, there may be simply an 800 number. And people who provide integrated junk E-mail services typically advertise themselves to be bulletproof, indicating that it's not possible to retaliate.

MR. MEDINE: So there's nothing inherent about the way the Internet operates that would require something traceable in the delivery of the message?

MR. CATLETT: That would be extremely difficult to do. In some cases, for example, in 1996 a very large spam was sent out soliciting child pornography and the FBI got hundreds of calls and they went through an enormous effort to trace the source of the spam, and it turned out to be a hoax. So usually that can be done, but there's not that economic or other incentive to do so.

COMMISSIONER VARNEY: I have a question. Could you put the slide up that is how to remove yourself from the E-mail lists, please. To remove your E-mail address you want to send an E-mail to this -- is it your experience that the majority of unsolicited E-mail has inaccurate removal instructions?

MR. CATLETT: Yes.

COMMISSIONER VARNEY: Then I guess I have a question for staff. Isn't that fraud or deception under our existing authority?

MR. MEDINE: Yes, I think it may well be.

COMMISSIONER VARNEY: Thank you. The same question, when you get an unsolicited E-mail with a header that the sender has deliberately or intentionally run it through a server to lead you to believe that the E-mail is coming from a known source or a trusted source, how much does that happen?

MR. CATLETT: That is common. There are a number of suits, for example, currently at Compuserve where spammers are being charged with this action, and judges have found this to be trespass.

COMMISSIONER VARNEY: Do you have any evidence as to why the mailers do that?

MR. CATLETT: Covering their tracks. And also because they are so often denied access by legitimate ISPs, they seek to insert their junk at points where they're not accountable.

COMMISSIONER VARNEY: And again to staff, wouldn't we be able to examine that practice under deception and fraud authority?

MR. MEDINE: Again, I think that's something that may well fall under such a law.

COMMISSIONER VARNEY: Okay, thank you.

MR. MEDINE: When the practice apparently is to use return addresses of E-mail of real entities, not those of the unsolicited E-mailer, what's the incentive for doing that as opposed to just making up a return address?

MR. CATLETT: It's very difficult to fathom the mind of a spammer. Most of those people are not excellent in the area of marketing or operation.

COMMISSIONER VARNEY: Maybe we should now hear from them.

MR. MEDINE: We will.

MR. CATLETT: I think you'll get a better quality of spammer at this table than you get from . . .

MR. MEDINE: All right. Well, thank you very much for that presentation. We would now like to turn to our first panel to discuss -- give us really a sense of how unsolicited E-mail works. And we're fortunate enough to have folks on the panel who know exactly how and can talk us through that.

I would like to introduce Sanford Wallace, who is president of Cyberpromotions. And sort of a basic question, if you could really walk us through how unsolicited E-mail works as a practical matter.

MR. WALLACE: Sure.

MR. MEDINE: And by the way, just for terminology sake, are you comfortable with the term "spam" or do you prefer "unsolicited E-mail"?

MR. WALLACE: Whatever you want to say, it's all right with me.

MR. MEDINE: Will you walk us through what the technology -- how are you able to send large quantities of messages, how are you able to get the addresses and so forth.

MR. WALLACE: Well, to address your question about how we were able to send E-mail, we, like every other service provider on the Internet, have invested hundreds of thousands of dollars in equipment which gives us high-speed access to the Internet from multiple backbones and the equipment necessary to send out and receive millions of pieces of E-mail. We have spent years of research and investment to make this technology available to us.

The actual act of sending E-mail or unsolicited commercial E-mail is no different than sending any other type of E-mail. We're essentially using the protocols that were defined years ago by the founders of the Internet and we're just using it in a commercial form.

I'm sorry, what was your second question?

MR. MEDINE: Well, just going along those lines, I mean, when I send an E-mail, I compose it and I hit the send mail and I get one E-mail. How is it that you -- what's the technology that enables you to send a million E-mails or 100,000 E-mails?

MR. WALLACE: Well, the technology already exists for anybody with an Internet connection to send out E-mail to multiple recipients. All you have to do is use a standard program like Eudora, for instance, which is freeware, which allows you to send hundreds and hundreds of different E-mails simultaneously because that's the way the protocol is designed.

As Cyberpromotions we've invested in high speed equipment and we've written custom scripts and programs to allow us to send E-mail to a large number of recipients at the same time, a lot of that is proprietary information.

COMMISSIONER VARNEY: David, can I ask you a couple of questions, and if I get too close to the proprietary information, please say so.

Your company, as I understand it, you have clients that want to reach a large number of people on the Internet to sell their product or introduce their products, so they'll come to you and they'll say, Now I've got this widget and everybody who is -- got the following characteristics, can you do targeting to a large group or do you just do -- tell me a little bit about that side of it.

How do you decide who gets them?

MR. WALLACE: Okay. Well, we really don't decide who gets them almost ever. We're not primarily in the business at this point of sending unsolicited E-mail ourselves, but what we do is we give them software to harvest E-mail addresses from different targeted sources.

So, for instance, if somebody wanted to send to people who were interested in fishing, we then go look into public data bases of people who have filled out forms or filled out -- filled out a profile that says that they're interested in fishing and we sell them the software, we sell the marketers the software to target that particular market.

We also sell --

COMMISSIONER VARNEY: Do you sell the software to do the harvesting? Let me tell you another example, because I don't fish, but I do drive. So, lately we've been looking, as somebody was saying yesterday, we've been on admins a lot looking at different information on cars. And now we're starting to get a lot of unsolicited E-mails about cars, some of which are frankly very interesting. They've got all kinds of different ways to buy cars.

Does your company create and sell the software to do the harvesting as well as create and sell the software to do the mailing? Do you do both?

MR. WALLACE: Yes, we certainly do. The software allows people to harvest targeted E-mail addresses and we also sell all the software products that send mail, also have remove features built into it as well. So we haven't just taken the approach of send out all the mail you want for any reason, we have attempted to authenticate the practice as well.

COMMISSIONER VARNEY: Okay. And, David, cut me off if I'm getting too long here.

So there's really -- there's kind of two threads here that I want to work with for a minute. One is the idea of the software that does the harvesting and you talked about that for a minute, and I think that sort of ties into what we talked a little bit about yesterday, I don't know that you were here yesterday, where we were talking about cookies and about how people, marketers, can harvest data.

Is that kind of an element or part of how your harvesting works, that software can go out and can pick up cookies and then compile E-mail lists?

MR. WALLACE: I think that's a very important question and I think that's one of our very important points that I came here to talk about. All the software that we sell that harvests E-mail addresses specifically harvests addresses from public data bases. It doesn't sneak around behind the scenes.

For instance, just because you visit a Web page doesn't mean that someone is going to harvest your E-mail address. It was mentioned earlier that that was a possibility. There was a bug in a Netscape version, 2.0 I believe, and they fixed it immediately, so that practice is really not utilized.

COMMISSIONER VARNEY: What are public data bases?

MR. WALLACE: In other words, people who fill out a profile -- and America Online used to be one of the places that we harvested E-mail addresses from. People who advertise in classified ads on the Internet, people who participate in a worldwide forum called Usenet Newsgroups, for people who post their E-mail addresses on their Web page for anybody in the Internet to see publicly, these are the areas that we focus on harvesting addresses. So, we don't believe that there is any type of a privacy infringement because people put their addresses there in the first place to a worldwide audience.

COMMISSIONER VARNEY: So then what you're saying is if I go to a Web site like admin and for whatever reason I register there and it's free but I do want to look at -- for those who don't know, that's a site that talks a lot about used cars and the values of cars and how you determine it and where you get deals on it and stuff -- but you have to register to get in, so I go in, I've been there three or four times.

Now, is that in your view a "public data base" that you can harvest from?

MR. WALLACE: Well, actually, we don't really get involved in any of that type of practice. What you're mentioning right there is really -- when you sign your E-mail address into a Web site as an interested prospect, I think in every form of marketing you're going to see that you're going to start getting mail of some sort because you already started showing an interest in that subject matter.

What we do is we just have programs that look into public areas. It doesn't work off of forms like you mentioned there. It looks for people who have an E-mail address posted on a Web page for everybody to see.

COMMISSIONER VARNEY: Okay.

MR. MEDINE: If you register with a Web site, that is not available to anybody but the Web site; is that right?

MR. WALLACE: Unless the Web site decides to distribute that E-mail address, but that's a practice that we're not involved in.

COMMISSIONER VARNEY: Okay. So, on one side you've got software that does the harvesting, and as I understand your position is you harvest from what you're calling public data bases, we may disagree as to whether or not they're public, but they are data bases where people have gone that are widely visited, available to anyone, and they have put information there that your software can then go grab, right? Is that accurate?

MR. WALLACE: Yes, that's correct.

COMMISSIONER VARNEY: Then what happens is now you sell somebody the software, and presumably taught them how to use it effectively, and if it's somebody who wants cars or fishing or whatever there are public spaces, usenet groups that discuss that topic, so it goes and it grabs those addresses.

Now what happens? Now I've got my million names or my half million names. Now what happens?

MR. WALLACE: Well, you then have access to those names and you can also purchase software which will allow you to send your message to all of those people virtually simultaneously, and if you use the software properly you will also give people a legitimate option to be removed from any further mailings, kind of similar to the way the direct postal mail works.

And if you -- we also offer a service that gives people the ability to use our service provider, meaning us, our promotions, to receive their removal requests and all their responses and they won't lose their account, so that they have no reason to forge E-mail addresses or to relay mail off of third parties because they are now given the opportunity to do it the legitimate, right way.

COMMISSIONER VARNEY: So, does your company actually send mass mail or you merely sell the software that allows individual companies to do it or do you do both depending on the relationship with the client?

MR. WALLACE: Well, our original business model was to send out our own mail on behalf of our clients and on behalf of ourselves. We still use that practice and that's actually not very controversial, we get very few complaints on that particular practice. But we do offer primarily right now the opportunity for other people to get E-mail addresses, sell -- I'm sorry -- get E-mail messages, send messages, relay mail off of our servers --

COMMISSIONER VARNEY: Right.

MR. WALLACE: -- essentially give them everything that they need to do it themselves.

COMMISSIONER VARNEY: Okay. And when --

MR. MEDINE: For those consumers who choose to remove themselves from a particular list, do you maintain a central repository for consumers who don't want to receive unsolicited E-mail, or is that basically a list-by-list basis, which means that they go out then and harvest another 100,000 names which may even include the consumer who will sign up for another site, the removal doesn't end up getting them off of a mailing list?

MR. WALLACE: Well, as far as Cyberpromotions' own mail list, we maintain one remove list and we utilize that for our own mailings. Now, one of the problems that we have dealt with recently is exactly what you mentioned, and that is since there are different mailers using different mailing lists, there were people who would get removed from one list and then continue to get mail from another thinking that their remove request was ignored.

And I think that's one of the reasons why it was very important for us to get involved with forming the association, of which the president is here, Internet E-mail Marketing Council, to implement the first true global filtration system that will not only apply to us and our customers, but to 90 percent of the E-mail that's out there currently.

COMMISSIONER VARNEY: Well, then do you have -- so you guys have good business practices. If somebody doesn't want to get any more mail from you, they can send the remove button back to you, they're off your list and they're off any lists that you administer?

MR. WALLACE: Yeah. We're pretty confident about that. There's always technical glitches that we have had to deal with over the years, but we have gotten that practice down pretty accurately at this point, and now our goal is to have a global filtration system as accurate as what we use currently.

COMMISSIONER VARNEY: When you sell your software to individuals to do their -- or to companies to do their only mass mailing, do you have any restrictions, covenants, contractual agreements that you would encourage or require them to also do this kind of mailing under what might be called best practices that would be clear header identification of who the mail is coming from, clear instructions on how to remove yourself from the list, that kind of stuff?

MR. WALLACE: Yes. We've continued to develop policies for our customers and we also encourage them to use our own relay service which does not identify their service provider but instead identifies us as the contact point for removal requestions, for responses and for any other complaints.

So, we are trying to -- as a matter of fact, we just implemented a new policy which will now allow people to relay mail off of third parties, so we are continuing to develop that, and along with the associations that we're getting involved in we're pretty confident that that practice is going to become -- the bad practices are going to start slowing down and hopefully more legitimate practices will start being utilized.

COMMISSIONER VARNEY: One final question. The idea that in terrestrial space what you're doing is really no different than the third-class mailing that goes on today, I just wondered if it isn't arguably different because for some people there is a cost to receiving E-mail and there is no cost to receiving third-class mail, and I wondered what you thought about that.

MR. WALLACE: Well, the truth of the matter is that there really is a cost to receiving almost every type of advertising that you see today. For instance, people do have to pay to dispose of their garbage, people do have to pay for the electricity that's used when their television set is on. Now, these are very small costs, granted, but also the costs of receiving E-mail is also extremely small as well. It's just that it's being -- we believe that that argument is being overstated and the senders of E-mail all play by the same rules, unsolicited or solicited.

COMMISSIONER VARNEY: Why is the cost of receiving unsolicited E-mail more like the cost associated with disposing of a third-class piece of mail or the electricity to run the TV? Why is it more like that than like the cost of receiving an unsolicited fax?

MR. WALLACE: There's a very big difference because most people who -- actually everybody who has a fax machine has the machine generally set to print out with their ink on a piece of paper, their resources 100 percent. With E-mail most of the popular online services like America Online give people unlimited Internet access at no extra cost, so they could receive a thousand pieces of E-mail and it won't cost them an extra penny.

So, the difference is that fax is a guaranteed cost to the recipient. E-mail, the cost to the recipient is starting to become nonexistent.

COMMISSIONER VARNEY: And what about the cost to the service providers, the ISPs, the systems that are delivering large volumes of mail?

MR. WALLACE: Well, I think the best way to answer that question is that every single ISP on the Internet pays to receive E-mail. That's just the way the Internet works. For instance, America Online sends out over a million pieces of E-mail a day on behalf of their members to different service providers. Yet, they don't pay anybody to handle that incoming E-mail. What they do is they pay for their own connection.

And that's the same way that it works for spammers or for commercial E-mailers. We all pay for our own connection, and that gives us the implied right to send out E-mail through the Internet, because that's exactly what that connection was intended for.

MR. MEDINE: We're going to focus on the cost benefits in the next panel. Just to fill out the record on -- one question is, are you aware of any efforts by any companies to harvest children's names?

MR. WALLACE: Actually, I am not to this day, and obviously being in the forefront of this industry, I to this day have not seen one advertisement which was targeted towards children.

MR. MEDINE: I want to open it up to some of the other members of the panel who have some expertise in this area. Walt Rines, who's the president of the Internet Mail Marketing Council, and Al Mouyal who's the president of the Internet Marketing Association.

Do you have anything to add to the picture we're getting now of how unsolicited E-mail operates, either of you?

MR. RINES: Well, Sanford touched upon a lot of good points. I think there are admittedly a lot of areas that we need to address and cover with unsolicited E-mail. And the focus of the Internet E-mail Marketing Council is in promoting the ethical use of commercial E-mail to address really all of these issues as they apply to every group involved, the ISPs, the end recipients and the marketers. And so our initiative is really to try to address all of those things. I guess you'd say we'll be talking about the cost situation and whatnot in later panels.

MR. MEDINE: Who are the members of your organization?

MR. RINES: Our founding members are the five largest senders of unsolicited commercial E-mail on the Internet today, and we represent about 90 percent of the actual spam being sent on the Internet today. I do have lists of the member companies; for example, Sanford Wallace with Cyberpromotions is a founding member, as is another company I run, Quantum Communications.

MR. MEDINE: Ms. Varney.

COMMISSIONER VARNEY: And how old is your association? When was it formed?

MR. RINES: We were formed in April of this year.

COMMISSIONER VARNEY: Is there any intention or thought to putting together some sort of best practices policies or guidelines for sending unsolicited E-mail?

MR. RINES: Yes. We actually have a Web site. The

URL is www.iemmc.org, and we do have a code of ethics and a group of guidelines which we intend to very actively utilize.

COMMISSIONER VARNEY: Do we have a copy of those, David?

MR. MEDINE: Yes. Al Mouyal, would you tell us about your organization and when you were formed and who your members are.

MR. MOUYAL: Okay. Well, just for the record I started in the E-mail marketing business back in September of 1996. Before I really launched the business I listened to a lot of people that objected to receiving these messages and I solicited these people to call me on an 800 number that I sent out over a course of two months. And the purpose for that was to understand the concerns of these people that did not appreciate receiving these messages, and they have a right to say that.

However, by talking to all these people I was able to create a series of guidelines that is on our Web site, edmarketing.com, that was reviewed by a series of attorneys and reviewed by a series of attorneys who understand the privacy issues and all the other issues that are involved with advertising.

All of the practices that people have been saying that are unethical we do not support, we do not do. Every one of our messages is presented as a commercial message in the subject field. Every one of our messages has an 800 number if people prefer to call to be removed. Our association --

MR. MEDINE: Just along those lines, do you have a policy of putting accurate information as to who's sending it and also how to respond to it?

MR. MOUYAL: Absolutely. As a matter of fact, when you ask to be removed from any one of our targeted data bases you will receive a confirmation saying that you've been removed from the data base. And if anybody can prove to me that they've received a message again from us, they've got something to stick in my face. And I mean obviously we want to try to make it as convenient for people as possible.

COMMISSIONER VARNEY: Well, if your messages are clearly labeled as commercial messages, what would you think about technological developments that allowed a software, a consumer could purchase software that would block any unsolicited commercial messages?

MR. MOUYAL: 150 percent supportive of that. I believe that just like the advertiser has a right to advertise, a recipient has a right not to be a victim of the advertising.

COMMISSIONER VARNEY: Do you think there would be any interest on the part of your industry in working for creating technological tools and standards in your industry that would require mailers to clearly label their mail so that a software could work off of it and block?

MR. MOUYAL: I think it's a great idea, I really do. The other thing is when someone receives a message, when someone receives a message in their box, a commercial message, and it's identified as a commercial message in the subject line and they clearly can see how to remove themselves and they clearly can see that when they do remove themselves they know that they've been removed by getting a confirmation, I think that's pretty responsible, and those are the approaches that I would like to see the industry take. And that's why we felt a real need to create an association that can promote these types of practices.

COMMISSIONER VARNEY: Let me go back to my car thing for a minute. Right now my husband is looking for a car and we would happily opt into a car offer mailing list right now, particularly if we could then get off of it easily and it wasn't going to be sold when we bought a car. Is there anybody that does that? Is there any such thing as opt-in mailing lists where consumers can come to you and say I am interested in hearing about these things?

MR. MOUYAL: Sure. As a matter of fact, my belief is if anybody has a Web site with commercial content that is providing products or services or good viable information, if they're not asking people to opt into a list to provide them with additional information, I think they're missing the boat big time.

MR. MEDINE: Since we're going to address that with the next panel, we only have two additional members before the next panel. Why don't we invite them up, Bob Wientzen and Colleen Kehoe. I think as we're really moving in -- without taking a break, but we're moving into them -- this is a good chance to move into the whole area of costs and benefits of the practice.

PANEL VI: UNSOLICITED COMMERCIAL E-MAIL: IMPACT

"Economic imperatives driving unsolicited e-mail, costs and benefits for consumers and industry, implications for consumer privacy, and consumer and ISP views."

Jason Catlett, Chief Executive Officer, Junkbusters Corp.

Raymond B. Everett

Colleen M. Kehoe, Graduate Student, Graphics, Visualization and Usability Center, Georgia Institute of Technology

Jill A. Lesser, Deputy Director, Law and Public Policy, America Online, Inc.

Simona Nass, Panix/Public Access Networks Corp.

George F. Nemeyer, Tigerden Internet Services, Internet Service Providers Consortium

Shabbir J. Safdar, Founder, Voters Telecommunications Watch

Sanford Wallace, President, Cyber Promotions, Inc.

H. Robert Wientzen, President and Chief Executive Officer, The Direct Marketing Association

***

We've heard now from some of the companies that engage in the practice. It might be useful to turn now to an Internet service provider online company to give their perspective on it.

And I would like to introduce Jill Lesser, who's the deputy director of law and public policy and senior counsel of America Online. Before she gets into this subject, a number of issues were raised yesterday about America Online. I think it's only fair that she have a chance on the record to respond.

So you've asked for this, if you want to take just a minute or two to respond and then maybe get into the whole question of how unsolicited commercial E-mail affects America Online.

MS. LESSER: Sure. Thanks a lot, David, and I appreciate the opportunity to comment on the statements that were made in the record yesterday. Let me first say I am responding to the comments that were made during a panel yesterday afternoon by Evan Hendricks, and they were both reflective of an article that he recently wrote as well as some additional comments that he made yesterday.

I think it's important to first say that in order for industry self-regulation in the area of information collection, use and disclosure to work it is necessary for companies, AOL and other companies, to be responsive to concerns expressed by consumers and the media. So I think that the practices that Evan and other people have engaged in in examining our practices and whether they are appropriate, whether we're appropriately communicating and, in fact, what they are is an important practice and it is not one that we have any problem with and, in fact, we would be happy to answer the question.

I think there are a couple of inaccuracies that Evan's statements indicate yesterday. And the first is that we feel very strongly at America Online that we've taken a lot of initiative to make our policies, both privacy policies, marketing preferences, and the way we relate to our members known to our members. We make those preferences and marketing practices known in the registration process.

Every single time you sign on to AOL there's a button called My AOL which gives you the opportunity to set up all of your preferences, whether they're marketing preferences or other preferences about the way you engage in behavior on our system, and finally it is in our terms of service.

Now, our terms of service, while it does not come up on the screen every single time you sign on, it is an absolutely well-known area in America Online, and we know that for a number of reasons. We know that first of all because members, hundreds if not thousands of members on a daily basis enforce our terms of service against each other. They say, you know, Hey, we think that somebody has violated AOL's terms of service in communications with me, so can you please kick them off, take the posting down, tell them that they've done something wrong, so we do know that our members are well acquainted with our terms of service.

And we do also know I think from the presentation that Alan Westin gave yesterday in addition to some other information that people are concerned about their privacy. So we do assume that when they go into the terms of service, if they're concerned about their privacy and our information practices, that they've looked at those services. So I think that it's inaccurate to say that our members are, A, unaware or, B, have no opportunity to find out about our practices.

The second inaccuracy was a statement made that we have lists of children. We will get into that discussion later this afternoon about AOL's practices with respect to children. I think it is critical to say firmly and absolutely that we have no lists of children. Number one, we only have adult account holders, we do not know who's a child on our system, we do not ask who's a child, and we have no lists.

Evan brought up the issue of overlay data. We disclose to our members that we make our mailing lists available. It is standard industry practice to combine that kind of information with publicly available demographic information, and so you can get information about whether a particular household has a kid -- has a child within an age range.

In addition, you get information about range of income levels, a variety of different pieces of information. We are looking, because we think again the trust relationship with our members is crucial, whether or not we should be more specific in our privacy policy, and we've indicated that we will make another submission to the record if we think -- and again this is an examination process, we have not fully -- you know, that we -- it's incumbent upon us because this is a new industry, and it's built on trust, to say it's standard industry practice in the marketing area to use overlay data when you sell your lists, but here's what you need to know about the way recipients of this information will see the information.

And finally there was an area that Evan identified which identified a list of members who had purchased during the course of whenever they've been on AOL from the AOL store, and there's no information about what was purchased, how much was spent, nothing that indicated transaction or navigational data, but we did think that that was on the line. The list was offered for about six weeks, it was pulled, it was pulled as a result of the article.

We appreciate Evan showing that to us. We don't think it was a violation of the policy, but we do think that it might have violated the spirit of the policy, and that's not what we're trying to accomplish, so the list was pulled, it was never sold, and that's the best -- that's the best I can tell you.

COMMISSIONER VARNEY: Do you have an opt-out, Jill?

MS. LESSER: Um-hmm.

COMMISSIONER VARNEY: You've got eight million members. How many have opted out?

MS. LESSER: Well, the number is fairly low, and it's a bad number because we have a number that's about a half a million over the history of AOL, which means these are not current members, and as people know, we have a lot of turnover, so it's a bad number.

COMMISSIONER VARNEY: There's been some criticism that it's very difficult to find both the policy on the sale of information and the opt-out. Do you --

MS. LESSER: Well, again, I think that it is not difficult to find at all. First of all, it's in the registration process. When you go through the registration process and you're asked to make a set of choices, one of those preferences is marketing preferences, which clearly indicates that we make mailing lists available, and says if you don't want to have your name made available, please check a box.

There -- as I said, every time you sign on to AOL, there's -- there are several buttons on your --

COMMISSIONER VARNEY: To activate your AOL account --

MS. LESSER: Um-hmm.

COMMISSIONER VARNEY: -- you have to go through a registration form --

MS. LESSER: Um-hmm.

COMMISSIONER VARNEY: -- and on the registration form it says, "Mailing lists are occasionally made available to -- so-and-so -- click here if you don't want your name made available."

MS. LESSER: Right.

COMMISSIONER VARNEY: And you can't get your account started unless you --

MS. LESSER: Well, the registration form is probably a little bit of a -- of a misdescription, because it's several screens that you go through. So, you -- you do not have to make that choice, but you do see that screen during the registration process. And then when you pull down My AOL at any time, which -- which is, you know, AOL for me. How do I want my entire system to operate, how do I want my mail to operate, how do I want marketing to operate, what do I want my preferences to be. As I go around the system, it is on every time you sign on.

And thirdly, and -- and, again, it is in our terms of service and it is in a separate area called Privacy Policy that's been revamped several times and moved around to be in as clear as possible area. So, for example, we know that people read our terms of service -- we had a terms of service and a rules of the road. It is now in the terms of service rather than the rules of the road because it was an -- it was an area we knew our members were well acquainted with.

MR. MEDINE: Okay, thanks. Turning back to the subject --

MS. LESSER: Okay, sure.

MR. MEDINE: One issue -- one issue that was raised here earlier is that, at least in the past, it was possible to harvest --

MS. LESSER: Um-hmm --

MR. MEDINE: -- unsolicited E-mail address lists from AOL because of the member profiles --

MS. LESSER: Okay.

MR. MEDINE: -- but is that still true, did that occur in the past and is that consistent with your terms of service?

MS. LESSER: Okay. Let me -- let me answer about harvesting and then digress for a moment on economics of spamming and then --

MR. MEDINE: We want to turn to that afterwards.

MS. LESSER: Harvesting is absolutely against AOL's terms of service. Again, it's in our terms of service, it's against our policy.

Harvesting -- I need to take issue with one thing that -- that Sanford Wallace said, and that is that AOL's system is not a public data base. It is a proprietary system and the member lists are for AOL members. So, the way to get access to those lists is if I am an AOL member, I can go and get access to a member directory if a person wants to register. For example, I am not in that member directory and you cannot find me anywhere in AOL unless you know my screen name.

So, it is totally voluntary and there are several members, because the medium is about engaging in conversation and meeting people who do, in fact, put their information in those member directories. But they are not to be used for harvesting E-mail. And, again, when you go in -- when you purchase a mail order account for 1995 and you use it to collect E-mail that is, A, a violation of our privacy and I think a violation of a proprietary network, it is not a public database at all.

If you --

MR. MEDINE: What steps do you -- do you take if you find out that that type of practice is occurring?

MS. LESSER: We terminate the account.

COMMISSIONER VARNEY: At that point they already have the list.

MS. LESSER: Correct, correct. Now, you know -- and, again, you know, AOL members do go out onto the Internet and they do post their names on public bulletin boards and they do converse, because they-- they E-mail just like on any other Internet service provider. So, what to do. So, we cannot and we don't tell them where to go or what to do. So, AOL's with probably about 30 percent of the Internet market in this country, our screen names are everywhere, and so we get an incredible amount of unsolicited E-mail. And I think that -- that what's really critical is you started to talk about the economics of -- of unsolicited E-mail. I think --

MR. MEDINE: I know you're anxious to get to that subject --

MS. LESSER: Sure.

MR. MEDINE: -- but one more point on this.

MS. LESSER: Sure.

MR. MEDINE: Have you considered seeding your -- you've heard about this practice of seeding earlier in these workshops, of seeding your membership lists so that if you get unsolicited E-mail with a seeded name, you know that someone has violated your terms of service.

MS. LESSER: I don't know the answer to that question --

COMMISSIONER VARNEY: But it sounds like you already have ways -- you have ways of finding out who -- who took your lists.

MS. LESSER: Well, I mean, that's a complicated question because of the dynamics of spam. If a message comes to let's say a million AOL members, it is very, very highly likely that it was collected through harvesting or a lot of it was collected through harvesting because of our member activities and how much hosting goes on and the dynamics of spam.

However, because there is so much dynamism really in spam activity. I mean, Mr. Wallace talked about some of the better practices, because what we are seeing are several different kinds of unsolicited mail coming into our system that are relayed off numerous different sites, that are relayed off of foreign sites, that use dynamic addresses, that means that every three or four messages or possibly every one message the sender's addresses change, so we do not know if -- to fool us from it being a bulk mailing. They forge Internet domains. So, all of those practices make it virtually impossible for us to know who the sender is.

When we had a dispute with Cyberpromotions, we could see where it was coming from, we could say, you know, this is a problem, this is what you're doing. You know, we need to make -- to enter into some agreement about what you're doing and have certain of those practices stopped, but we had no ability to do that.

COMMISSIONER VARNEY: Did you ask Mr. Wallace to stop?

MS. LESSER: We were engaged in litigation with

Mr. Wallace, and we have settled, and litigation and --

COMMISSIONER VARNEY: Can you discuss the terms of settlement or no?

MS. LESSER: I would prefer not to discuss the terms of settlement, but, you know, it has settled. We have required -- and -- and Mr. Wallace and his company are abiding by the terms of that settlement. I do think that when you look at the dynamics and the economics of unsolicited E-mail, however, I don't know how anybody can represent -- for example, with respect to the Internet E-mail Marketing Council that they represent 90 percent of the spammers -- of the spammers on the Internet because we have absolutely no idea who's spamming.

And when you see a Web site like this which is selling software which says, How to mail up a million messages per hour, no kidding, fully functioning -- free ten day, fully functioning software, download here, AOL Stealth features. It's called the AOL -- it's called the Stealth Mailer. It costs about $400.00 and it says the following:

"Here are just a few features of the Stealth Mass Mailer. Forge the header, message ID, ISPs will spin their wheels, add a bogus, authenticated sender to the header, add a complete bogus received from, received by line with realtime date stamp and recipient to the header; does not require that a valid property account be entered in order to send your mailings; easy to use, easy to operate."

There is no cost -- Sanford talked about investing hundreds of dollars -- hundreds of thousands of dollars in an E-mail system. I get a $19.95 account with an ISP, I download this software and I'm in business.

COMMISSIONER VARNEY: Do you think it works?

MS. LESSER: Absolutely, because we get -- we get 15 million, approximately 15 million incoming messages from the Internet to different AOL recipients, anywhere from 5 and closer to usually 30 percent of those messages are unsolicited.

COMMISSIONER VARNEY: I think you should take the copy that you have there and submit it to the staff with a petition to investigate for the deceptive practices alleged in the advertising and the forging --

MS. LESSER: And interestingly, George and I were talking before, George Nemeyer has several other Web sites here as an example with the same kinds of software available. So, you know, this kind of software, which we do think -- we started this process in looking at spam from a technological perspective, but what we have found out more and more is that it is really about fraud.

It is not about questioning whether marketing on the E-mail -- excuse me, on the Internet is a viable practice or an appropriate practice. It is really about fraud and about a system where there is total anonymity, where there is no incentive from an economic basis with a $19.95 account to do anything but send four million messages a day. If I get two responses, then my product was purchased, I'm in business, I've made money. So, there are no incentives to stop.

MR. LANDESBERG: I've got a question, you just mentioned that you received 15 million incoming messages from the Internet, in what time period?

MS. LESSER: A day.

COMMISSIONER VARNEY: A day?

MS. LESSER: Two -- let me clarify, to different AOL recipients, so those may be the same message coming in to -- so, it's 15 million different AOL recipients.

COMMISSIONER VARNEY: That hit your server a day?

MS. LESSER: Absolutely.

COMMISSIONER VARNEY: And what percentage of those, if you know, are unsolicited merchant mailers?

MS. LESSER: The number varies from between 5 and 30 percent. I know that's a big variation, but it depends on the day of the week, but I will tell you that it hovers closer to 30 percent, but it varies.

MR. MEDINE: And what's the cost to AOL of having to process that percentage of unsolicited E-mails?

MS. LESSER: The cost is in a word huge, but let me back up for a second. There has been a huge increase given

AOL's increase in membership and just an increase in usage of the online medium in E-mail traffic. And so over the past several months when we have had a lot of problems with unsolicited mail, we've also had to process many, many more valid electronic messages.

What that means is I can't give you precise costs, I don't even mean in dollars, but even precise percentages because E-mail is expensive. It puts burden on our servers, but what we have found is that the servers slow down. And so we have seen several hours of delay in incoming messages, and the only way to alleviate those problems is to keep purchasing more servers. Those are extremely expensive machines.

Not only that, but when you look at the dynamics, the changing dynamics of unsolicited E-mail, and we have committed -- and this is a company policy, so it's obviously not what everybody does -- to try to block or filter for our members unsolicited commercial E-mail.

In doing that, we have devoted hundreds and hundreds of hours of manpower or womanpower to figuring out the dynamics of spam and to implementing those filters and playing that cat and mouse game.

COMMISSIONER VARNEY: Jill, I have another question. My colleagues and I were just talking about the fraudulent aspects of this. If I got software from Mr. Wallace and went to more public space, Usenet group space, and pulled down anybody on the Usenet group space who had put their E-mail address up there, and let's say I got a million names and that, you know, most of them were AOL subscribers, and I then got software, whether it's that one or not, but not that one, I got software that clearly identified who I was and said I have written this magnificent, you know, piece about how to lose -- how I lost 20 pounds in three minutes, okay, and send me $5 and I'll E-mail it back to you.

And it's true, I wrote it, and whether or not, you know, we won't get into I lost five pounds in a week and here's how I did it, let me tell you how I did it and it's true, I did it, I really did. And I then send that out, I send it to a million people on your system. Is there anything fraudulent about that?

MS. LESSER: No. There's nothing fraudulent about it, and if you -- I mean, except if you were going to send another message and someone requests that you don't send messages to them, you should provide a recipient with a way not to receive those messages. Now --

COMMISSIONER VARNEY: So, if the header information is deceptive, there might be fraud there. If the text of the message itself is deceptive, there's fraud there. If there is a message at the bottom that says click here to remove your name from the list and, in fact, it doesn't remove you from the list or you get instructions on how to be removed from the list and that's just flat out not routed to anything, that would be fraudulent or deceptive.

MS. LESSER: Right. Now, it is -- your first scenario would be against AOL policy and we could terminate accounts, but I wouldn't want to posit that it is fraud under, you know, legal analysis.

MR. MEDINE: Where does unsolicited E-mail rank on the list of complaints by AOL subscribers?

MS. LESSER: It's the number one complaint.

MR. MEDINE: By far?

MS. LESSER: By far.

MR. MEDINE: You introduced George Nemeyer next to you who operates Tigernet Internet Services, a small not-for-profit Internet service provider in Dayton, Ohio. He's here representing the Internet Service Providers Consortium, a nonprofit trade association of ISPs which promotes responsible use of the Internet.

You've heard what the impact is on a fairly large Internet access provider. What's the impact on smaller Internet access providers of unsolicited E-mail?

MR. NEMEYER: In some cases the impact is significantly greater because the small provider doesn't necessarily have the resources to deal with the ramifications of what happens to them. Let me give you a quick example.

We received one single mailing which went to two of our subscribers, a typical MLM scheme for an Internet marketing kit which in turn advertised more spam software plus thousands of names on a list. The two people that received this message attempted to follow the remove request, and I did not -- I was unaware of this as it occurred.

However five days later I get a message to the administrator account that says there's a problem with mail. And what we got back, this goes on and on for over 1,000 lines of data over a five-day period, and these are just the log entries of the attempt of our system to sense that unresponsive return address.

So, you can imagine something like this multiplied by the millions that AOL sees, and this is not a small cost to the provider. This particular attempt clearly did not work to remove. We expect probably to get more mailings along the same lines.

I would also like to point out that in a message earlier Mr. Catlett talked about the reasons why spammers may put someone's true address in a return message. One of those reasons is flat-out retaliation.

Let me quote to you a passage which appeared on one of the spams that we received which basically says that they do not want to hear from you in return. This message, if I can find it quickly here, this message indicates the kind of attitudes that many of the spammers have toward those on the network and trying to emphasize their right to jam their mail in your mailbox.

The quote is, "Note to flamers, don't do it. We will comply with all and respect all remove requests, but if we are flamed, we will flame you 1,000 times as much and we will E-mail three million people with a questionable item with your return E-mail address. We want respect as much as anyone else. So if you give it, you shall receive it."

So, these are the kind of things that we face. In some cases the spammer community that we are attempting to deal with has indeed taken down providers intentionally by putting those providers' names in the return addresses and letting them reap the return of a spammed mail.

MR. MEDINE: Are you comfortable revealing the author of that message?

MR. NEMEYER: The author of that particular message was a customer of Mr. Wallace, according to what Mr. Wallace said. At the time the customer was supposedly removed from his system, but there was another mailing from that customer a short time later. It had to do with a hair restorer offer as I recall, which ironically had it not been fraudulent, I probably would have been interested in.

COMMISSIONER VARNEY: Mr. Sanford I'm sure has no ongoing relationship with the individual who threatened to flame him to death?

MR. WALLACE: No, I just wanted to comment that that was reason for immediate termination of that account. The fact that they may have sent another piece of E-mail would not reflect the fact that we didn't terminate their account. We don't authorize that type of activity.

MR. NEMEYER: Along the lines of cost as well, clearly this is a cost to the consumer as far as the utility of the E-mail system. What we are starting to see is a number of customers indicating that if E-mail is going to be totally useless because of the flood of junk mail that they receive, that they're going to give up on the Internet altogether, number one. Or number two, they switch providers or at least switch accounts in terms of trying to start fresh.

This is becoming a significant situation for some of the larger providers. Compuserve in their case, for example, mentioned the number of folks that had just discontinued their service. Clearly as a small provider, we're trying to offer a positive service to our subscribers and if they don't view what we're offering because of something we can't control, you know, that's clearly harmful.

MR. MEDINE: We have another Internet access provider with us as well, Simona Nass, who is responsible for determining policy at Panix/Public Access Networks

Corporation. To what extent are your experiences similar to what we've heard or different from what we've heard?

MS. NASS: Our experiences are fairly similar. The difference primarily is our approach to it. Panix maintains spam filters that staff administrators -- we have Panix staff administering spam filters for our customers. And what we do is we try to develop technical solutions to a problem that is plaguing all of our customers and taking up a significant amount of our resources also in terms of staff time and machine resources and so forth.

COMMISSIONER VARNEY: Do you think that's an effective solution or optimal solution or what would help that solution?

MS. NASS: It's not optimal for sure. But on the other hand, it is making headway into the problem and the difference between not receiving, you know, 50 percent of the spam that you otherwise would have gotten or whatever percentage is still significant when you're logging in by calling long distance from the other coast and are trying to quickly check your mail for anything important that you need to get over that night.

COMMISSIONER VARNEY: And do all of your -- do people come to you because you have this feature of trying to block unsolicited E-mail?

MS. NASS: It works both ways. People come to us because we have this feature. We also developed this feature because we tend to have the sort of customers to whom this sort of thing is important.

COMMISSIONER VARNEY: And do you have anybody who wants unsolicited E-mail, who says no, don't filter that, or do they just go to another company?

MS. NASS: We do have customers, our approach is opt-in, meaning that you get all the mail that's addressed to you unless you take action to filter it.

COMMISSIONER VARNEY: And how many of your customers -- what percentage of your customers sign up for the filter?

MS. NASS: Several hundred of our customers, about 300, I believe, have signed up for the filters. Additionally, we assist them with building their own if they don't want to use ours.

MR. MEDINE: So, 300 out of how many?

MS. NASS: We have 6,500 individual customers, over 6,500, over 1,000 corporate customers. Anybody who's doing their own solution on their own IP connection, they have a PPP account with us, we don't know what's happening on their end. And we also make tools available to people so they can they can mix and match recipes either that our staff had created for addresses of known spam senders or they can look to their own mail and see who they don't want to get mail from again or whatever system, or if they don't want to get mail that says make money fast ever again, they can make sure they don't get it.

COMMISSIONER STAREK: Tell me some more about these filters. They're 100 percent effective when they're employed?

MS. NASS: No, they're not 100 percent effective. They can't be because they can only filter for things that we can predict, and that's historical information, either for addresses that we know have sent spam in the past, or for common strings that occur in the messages, such as if a particular spam sender is using a P.O. Box, even if they're changing their header information, if they always say call this 800 number or write to this P.O. box or whatever, we can still catch them on that. But if they change it, then it's very adaptive. It's sort of like an arms race, you know, how fast the techniques mutate and how fast can the solutions be made.

COMMISSIONER STAREK: Are you the only Internet service provider that has this capability or employs these filters?

MS. NASS: No, we're not. In fact, we know of other ISPs who have asked us to send them our information and they subscribe essentially to our lists. We also know of other ISPs who filter on behalf of their customers either because -- with or without their customers' permission just as a utility issue. And we also know of ISPs who advertise themselves as we filter your spam, so they use that as a draw to get customers.

MS. LESSER: David, can I add one thing to answer your question. AOL does have a filtering system which is called Preferred Mail. It works differently from Panix's system. Theirs is an opt-in, ours is an opt-out. We made that decision because as I said it is the number one complaint on AOL, and we've been getting so many complaints that what we did as we decided that it was more likely than not that people did not want to receive unsolicited commercial E-mail particularly from the people on this list, which were people about whom we got complaints and who we then went to and tried to get to stop and who refused to stop. That list grows, but again, it's a cat and mouse game, but members can turn it off. If they turn it off, they receive mail from those senders.

COMMISSIONER STAREK: And how much more does it -- will your subscribers pay for this service?

MS. NASS: We offer it at no additional charge. What we found was that we were spending so much time on the issue anyway that, you know, people saying I have this mail, how can I make it stop, that sort of thing. We get working with users to educate them about how to use the filtering tools we have available in our system. We're a UNIX-based system and we offer prop mail and various other filtering software tools.

And so even without our filtering system we were spending so much time talking to them either dealing with complaints about spam that they got from off site or about how to filter stuff and so forth that it's largely equivalent to do this and just point them to the help system and say, you know, we have a system already built for your use, if you want to use it, take a look at what's in the help system, it's really simple to use, contact us if you have additional questions or want to have our help in customizing it.

COMMISSIONER STAREK: As far as you know, are technicians working to, you know, improve the system so at some point these filters will be 100 percent effective?

MS. NASS: There's ongoing research into it. The way we're doing it is not likely to work, because it's going to continue to be an arms race, and it's going to continue to require ongoing maintenance in a proportionately increasing way.

COMMISSIONER VARNEY: Can I follow up on that question? We talked -- we had a brief exchange earlier where we talked about technological solutions and if the industry that's represented here today would think about how to work on technological solutions. One of the things that's been kicked around in the Congress is some sort of header information that unsolicited E-mailers would use and absolutely identify that it was a piece of unsolicited E-mail up front, and then technology software can be written that people can choose what they want to receive or don't receive. Would that work?

MS. NASS: The problem with that is that you're asking the offenders to basically police themselves. And so the problem is not so much spammers who send mail with legitimate information and so forth, because you can just filter those out. The problem is people who would never comply with that sort of requirement. And so --

COMMISSIONER VARNEY: We have sort of a similar historical experience here with the telephone fraud, and Congress passed a law saying telephone fraud is illegal. Now, FTC, go to write the regs to make sure it's illegal. And what we found was that the legitimate business industry came to the table and said, Okay, we'll help you write the rules, but you're not going to put the telemarketers out of business for fraudulent activity. And we said we agreed with that, but what it did was it gave us a framework within which to determine what was legitimate and not legitimate and it also gave us additional tools to go after the people that were fraudulent.

So, although, you know, no law, no regulation is ever going to stop the bad actors, sometimes it's helpful, and I don't know if it would be in this context, to create the safe harbor that says these are the legitimate practices, these are the best practices, and if you're not in this harbor, you're not in it --

MS. NASS: There are some differences between E-mail and telephone solicitations. Namely with telephone solicitations, you can verify if a call was placed from a particular number to a particular number. With E-mail, you can just get a $10 a month or even free E-mail account, use it, burn it up, have everybody directed to your P.O. Box, so it doesn't matter if you burn your bridges behind you and then there's no way to trace it.

With regard to telephone solicitations, it takes longer to establish a phone number. It can be verified, and you can't have those same problems with E-mail.

COMMISSIONER VARNEY: So, what's the answer?

MS. NASS: We don't know for sure. There are people researching technical solutions, there are a variety of approaches being pursued that I have outlined in my written submission. Among the options are a P-filtering, which is also a sort of mutating problem, setting up software to do the filtering itself, or to put in the headers itself rather than letting the person who would probably want to get around it do it.

Like for example, the Pegasus mailer said that -- has implemented a feature that puts in a header that's not user configurable where if more than a certain number of copies are being sent to the same mail, it puts in a header distribution bulk or whatever. If -- I mean, people can obviously get around that by sending, you know, 50 or fewer messages at a time. There are people who are researching things like opt-in E-mail where you give out your address only to people that you want to reach you and you can establish various variants of your address and so they have different priorities.

For example, the people that you know you want to get mail from just get your priority one or whatever. People, like if you post to Newsgroup, say you're a researcher and you're posting for solicitation, you know, soliciting information about the field that you're researching. You don't want to have your mailbox clogged with everything, you know, every offer under the sun.

And so what you can do is set up a certain variant of your address so that you at least know that everything that you receive in response to that is related to your posting. So that it's not the -- you know, your father is in the hospital now and you can prioritize between those things. So that the hundreds of responses you get say to use a posting can be differentiated from mail from your boss, to your colleagues, from your family, et cetera.

Other approaches that have been floated include legislation criminalizing or providing civil remedies. There are problems with that, too. Primarily it's the enforcement issues and also there are risks of it showing expression and so forth, but in terms of enforcement, how would you verify a complaint? If there were a law that said you are entitled to such and such a remedy, if you can document that you received a spam, how would you do that? It's going to turn out being war of logs, your system's log against the system logs that the sender, maybe if that particular piece of mail routed through hops, you know, various other hops on the Internet before reaching your site, maybe there's a record of it in the logs of some intermediate site.

At that point you would probably need a class action suit or the equivalent of several plaintiffs to prove that you had even gotten this E-mail because you're going to say I got this E-mail and the sender is going to say, No, you didn't.

MR. MEDINE: I'm going to hold that discussion which is really just the remedies portion and turn to Shabbir Safdar, founder of Voters Telecommunications Watch, which is a three year old, grass-roots Internet advocacy group based in New York. Talk to us about what your study learned from ISPs about the cost of unsolicited E-mail as well as the impact of it on consumers.

MR. SAFDAR: Let me thank the FTC for hosting what is probably the most heated discussion in what's probably the coldest room in Washington that I have been in the last three days, it's got to be 90 degrees outside.

VTWW over the past two and a half months, in response to the FTC's call for information, ran a survey of Internet users and Internet providers asking them what they think. And as we cited in the survey, we think this is really the best information from ISPs, it comes from folks like AOL and Panix.

We learned some interesting data, but what was more interesting was what we get from Internet users and what Internet users told us bears and gives some spin on what we heard from Jill, which is that for about a third of our respondents, and this is a nonrepresentative sample of Internet users, if you can find me a representative sample I would like to see it, is that about a quarter of their mail was spam as of the last two months.

And we did a broad survey asking people what they thought, and then we also did an in-depth single survey where we took an individual who was a part of our survey from EFF Austin and he for some bizarre reason has saved every bit of spam he's received since last July. And so we did a little statistical analysis, and all this is in our findings, which is in our FTC filings. And he found that starting last July he was getting about one piece of mail, junk mail, junk E-mail, every two days. As of this May, he was receiving about six every day. And it doesn't take a lot of mathematical knowledge for him to do a simple linear growth projection and realize that by the end of '97 he will have received 753 pieces of junk E-mail.

This does not seem to be an unreasonable statistic, this jibes with what people told us, that about a quarter of their mail was spam. And on a system like AOL or Panix, that can be a significant amount of delivery resources to process this information.

What's worse is that we found that a lot of people actually pay for reading their mail and it's not a small amount. If you look at Senator Murkowski's office from Alaska, the motivation for introducing the bill was that they -- his constituents live in areas where they don't have a lot of local dial-up connections, and so they pay toll charges. And we talked about the economic impact, which maybe we've already bought into.

You'll see in our filings there are about four to five places where an individual can pay for receiving spam multiple times, and I'm not saying that we're talking about $5 for a spam, but there is a significant cost associated with it.

MR. MEDINE: Can you just tell us what those -- where in the system these costs would be imposed on the consumer.

MR. SAFDAR: Sure. There are hard costs and soft costs. I mean, soft costs are costs of extra staff time needed to process and handle problems associated with mail which get passed on to the consumer through higher ISP prices. Very simple hard costs are things like disk spaces, ISPs, including my own. Panix is my ISP, so this is a bit incestuous, but -- you can get charged on ISPs per the amount of disk space you consume. And in an ISP where your mail is delivered into your own disk space, you'll be paying for spam over a certain allotment of your disk space even before you've read it.

Now, if you pay for connect time charges where you're connected to their system, you know, at $2.95 per hour if you don't have a flat rate ISP, while you're downloading or reading your E-mail, including spam, you'll be paying for that as well. If you're downloading your mail over a line with a toll charge, perhaps because you don't have a local pop or because for whatever reason you don't have a flat rate per-call service, or you're calling an 800 number or long distance, you'll be paying there as well.

And so it turns out that if you have a really bad pricing plan with an Internet provider, you can pay a lot of different ways. Now the response that most people have in this and I think it's a reasonable one is you should probably change ISPs. And I would agree, but it is undeniable that at some point the costs do get passed on to the consumer even if it's in a flat rate market, because the plan, so to speak, has to be built out to account for it.

And once again I'm not saying that we're talking about adding $5, $10 a month for the customers, but for some people this could be significant. And for some people who don't have a wide choice of ISPs in rural areas, they don't have a lot of market and accessibility. They can't move around in a lot of different ISPs without incurring some charges.

As a proof of sort of the beauty of this medium, Internet users who are right now discussing, whether they're listening to you on the democracy or on the chat, were just polled about 20 minutes ago about how many pieces of spam they receive per 12-hour period and the answer is about eight. And this is going to increase.

We're looking at a number of about 161 that our single sample person received in May, and it only grows to increase. And I think that what George said is very important, the amount of mail people are getting is very high and you lose information in there. And the filtering tools that are present are good, and I think Panix is quite a leader in doing that, I think that's one of the reasons they and AOL preferred mail is such a good example. They're not 100 percent and they never will be.

It's sort of like cryptography where the folks that make the codes are always going to be better than the folks who break them. In this case the folks that need to enter the market to send unsolicited mail are always going to have an easier time than the folks who are trying to block it.

MR. MEDINE: Is there a risk that at some point it's going to kill the golden goose or whatever and that is that people will stop using E-mail or the future utility of E-mail will decrease because of the large number of unsolicited pieces of E-mail these people receive?

MR. SAFDAR: I actually don't think we'll get to that point. I think the risk is that we'll see very ill informed policy, of course not of the FTC, as to how to deal with this problem. There's a great concern among the folks that work on Internet user issues from the Internet user point of view about the proposals for labeling, for example. They carry very grave free speech concerns. I mean, we're in court right now talking about why you -- it's very problematic to label concepts on the Internet to turn around and say well you can't label indecency but you know what you can label ads. People don't see that distinction very well and you come back and find that you're setting a very bad precedent.

COMMISSIONER VARNEY: So what's the answer?

MR. SAFDAR: I think the answer is twofold. One is to let the Internet community come up with some technical solutions, some of which are already out there, and then give them some teeth. Today, people post, ironically enough, to the spam newsgroup, quite often with altered E-mail addresses. For example, my E-mail address, and please don't send me any more junk E-mail, is Shabbir@vtw.org. Well, if I posted it at Newsgroup and I was using the sort of de facto standard it would be Shabbir.nospam@vtw.org.

If you tried to send mail by harvesting my address from that Newsgroup, it wouldn't work because that address doesn't exist. Now, if I were to use that or if I were to use some other Internet-based standard and somewhere to go around it, there's no penalty for that. There's nothing that says that if a bad actor is to abuse that preference that I am going to -- that I have any recourse. I think that's what's needed. I think the Internet community needs to sort of codify some of its standards in a way that is consistent with the Internet culture and the first amendment and then the regulators, be it Congress or the FTC, needs to put some teeth into it so that it means something.

COMMISSIONER VARNEY: Well, let's ask Mr. Wallace or anybody else here, it seems to me that there is some common interest here. I think, Mr. Wallace, when I read your bio you have some background with telephones and telemarketing, or am I wrong? Because it seems -- no, I'm only asking in the sense that it seems to me that there's a possible analogy that David is alluding to in the 900 number industry where everybody thought 900 numbers were going to change the fundamental economics of the way we did business in this country. And what happened is they went zap immediately and they still haven't recovered.

So, it seems to me that there's got to be some common ground for people who want to engage in unsolicited mass mail but want to do it by a set of ethical rules with the people who also say Well, there's some first amendment right here but we've got to clean this up and we've got to do it in a way that gives consumers choice. I mean, is there -- you know, the last thing that most of the people at this table want is government regulation, but the last thing the government wants is to see the system crash.

MR. WALLACE: I agree with you 100 percent and that's exactly the reason why we made it such a top priority to form an association to enforce ethical standards and guidelines. I think that we need to have the opportunity to test those new standards and new guidelines before the government comes in and regulates the whole industry, because this is something that is literally just occurring this month.

COMMISSIONER VARNEY: And do you all talk to each other outside of court? I mean, do you -- I mean, is there a dialogue here that can start?

MR. WALLACE: Well, maybe Walt can answer that better than I can.

MR. RINES: The question being talk to who, the ISPs?

COMMISSIONER VARNEY: The ISPs, the consumer groups, the various kinds of people at this table.

MR. RINES: Well, we do talk, of course amongst the spam industry we talk. Of course in setting up this association, we've talked about common issues, common complaints and addressing those complaints. We haven't had a tremendous amount of communication with other ISPs because they seem to be at odds a lot of times, obviously.

We have seen the importance of putting a global spin on a solution, and one of the things that we've developed as the Internet E-mail Marketing Council is a global filtration system that filters unsolicited E-mail at the source. So before the message travels onto the Internet. And that in all the tests and all the studying that we've done really addresses a great deal of the concerns; in fact, just about all the concerns of cost shifting. Because if the E-mail is never delivered or delivery is never attempted, then it does not require any resources on the recipient side. And that means no long distance charge is being used up, no disk space is being used up, in fact no processor time or reduced space on the ISP on the receiving end.

So, a global filtration system we have seen as a real priority. The development and testing of that system at IMAC is going on right now and we actually have a target date of being up and running with that system the 5th of June, we're running a little bit behind because it's a tremendous undertaking as you might expect.

COMMISSIONER VARNEY: And have you talked to any or have any of the ISPs worked with you on this?

MR. RINES: Well, one of the founding members of IMAC is our backbone provider, one of the six major backbones in the country. And they have been very supportive, in fact were instrumental in helping us get together to form the association to address these issues and take care of these issues before things get out of hand.

COMMISSIONER VARNEY: Maybe Mr. Wallace can comment on this. Sometimes it is extremely useful to when you're solving the problem to sit down with people that are experiencing the problem and even before you beta test see what their thoughts are. I mean, I can't strongly enough -- I mean, it seems to me there's a lot of common ground here and let's at least start talking about it.

MR. MOUYAL: Can I say, one of the solutions we're proposing and we're developing right now is turning the spam or the commercial E-mail into "gem mail" and what we would like to do is we would like to pay people to read commercial E-mail --

COMMISSIONER VARNEY: I'll sign my kids up.

MR. MOUYAL: And the way we would like to do it is through a point system where people can read the advice and what have you.

COMMISSIONER VARNEY: Like frequent fliers. Change the economics.

MR. MOUYAL: Absolutely, and they can go back to an online catalogue and purchase all kinds of Internet services. And if they choose not to use the points for goods and services, at the end of a 12-month period we'll give them back ISP dollars while helping them offset their monthly fee.

I mean, I think that would really work, and I would like to say something about some of the technology that has been developed to forge headers and to do all these nasty things, in my opinion. And I have to put the blame strictly on the ISPs and the AOLs of the world because instead of dealing with the issues with good positive decisions and addressing these people, by talking to them, they have forced them to create these type of products.

MR. MEDINE: Let's keep the gallery quiet. One of the advantages here today is the opportunity for all of us to sit at the same table and discuss these problems. I'm going to be somewhat of a curmudgeon and stick to the agenda and during the next half hour stick to what are the cost issues and then from 11:00 to 12:00 we can really work on solutions among ourselves.

Colleen Kehoe is a Ph.D. student in the Graphics, Visualization, and Usability Center at the College of Computing of the Georgia Institute of Technology. Maybe she can enlighten us further about some of the impact of these practices on consumers.

MS. KEHOE: First I want to mention that I'll only be able to cover a few of the data points from our survey that we've conducted and we have more information available both online as well as hand-outs in the lobby. Our survey that we conducted through Georgia Tech is conducted online and therefore it's self selected, and this is the seventh survey that we've conducted over the past three years.

This survey, which was completed in April, had about 19,000 respondents which gives us a total of almost 100,000 respondents over our seven surveys. And what I'll do is run through basically some of the data points that we have that relate to spam.

First, 80 percent of our respondents report that they have received spam. We asked a variety of questions on direct marketing in general and asked people if they agree or disagree with various statements and to what extent. One of those statements is that they like receiving mass postal mailings. And we get a moderate disagreement with that statement. We also ask do people like receiving mass E-mailings and we have a much stronger disagreement with that statement.

What we've done recently is do a longitudinal analysis of a particular set of people who answered both our most recent survey and a previous survey to see how their experience in being online has changed their opinions over time.

In general, we find that those opinions haven't changed very much except in the area of receiving spam. The percentage of respondents who disagreed strongly that they liked receiving mass E-mailings increased from 63 percent in our sixth survey to 74 percent in the seventh survey. Part of that is that in being online, people have more of an opportunity to receive spam.

So, in our -- in the sixth survey a lot of those people had not yet received spam. We feel it's both reflective of a general increase in spam and also just the longer that you tend to be online the more likely it is that your E-mail address is out there to be collected and used for these purposes.

We also asked what do you do when you receive spam, and the percentage of users who reported that they simply delete these E-mail messages rose slightly from 59 percent in the sixth survey to 61 percent in the seventh. And that is across all our respondents, not just that particular set who answered both surveys.

The percentage that actually read the message decreased from 13 percent in the sixth to 11 percent in the seventh. So it's only a small amount of people who actually report that they're reading these messages. When we look at again that group of users that responded to both this survey and the previous survey we show that they are more likely to simply delete the E-mailings when they get it. Partially because they're just more able to recognize it without having to read the entire message.

Another question that we ask is what do you propose should be done about these mass E-mailings. And the number one response for both this survey and the previous survey was that people would like to see an opt-out registry created. And that is 38 percent of our respondents. The next most popular option is that there should be a blacklist of known spammers created. That was a new option for this most recent survey and that actually came in number two.

Government regulation is favored by eight percent of our respondents which is a slight increase from a previous survey, but that only by 2 percent outweighs doing nothing about the problem. In our most -- in our sixth survey, which was conducted about six months ago, doing nothing actually overrode having any sort of government regulation as it relates to spam.

And I think it's also worthwhile to note that these -- these preferences of first a registry and then a blacklist of spammers are favored by both our U.S. respondents and those in Europe. So, I think it's been mentioned previously that some of these issues unfortunately don't end at the boundaries of the U.S. and that it's worthwhile looking at how other countries might respond to these issues as well.

MR. MEDINE: Thank you. Now we have had a chance to look at the consumers' perspective and ISP's, but there's another component of this, the Internet's infrastructure, and Raymond Everett who is a consultant to AOL and Compuserve will address it.

MR. EVERETT: Well, I think there's an excellent analogy that's been made in other discussions yesterday to the problem of pollution in the environment and in some ways the cost to the Internet is similar to the cost of say toxic waste or other pollutants being released into the environment. It's a cost savings for the producers in order to -- they save money by transmitting this stuff into the environment and shift that cost on to recipients.

And as Ronald Coase in his Nobel prize winning work outlined, this distribution across an ever-widening base makes it much more difficult for those people being impacted to ever recoup those losses. There's a real problem of transactional costs. You're starting to see organizations like the Coalition Against Unsolicited Commercial E-mail who come together on an ad hoc and voluntary basis to try and come up with some solutions.

The coalition that I am involved with is primarily made up of Internet service providers, administrators and technologists on the front lines of the problem. And we have seen that the technological answers have not been very effective. For every block we put up there are a dozen ways around it.

The Internet is an incredibly resilient technology. If you look at its origins, it was designed to reliably transmit data during difficult and spotty connections mostly in wartime situations, but that underlying open standard on the Internet makes it incredibly easy for people to circumvent blocks that Internet service providers put in place and that's -- and that's why filtering mechanisms, like AOL and Panix have wonderful filtering systems, aren't completely effective. I -- I barricade myself behind many layers of filters and still manage to receive a -- a fair number of spam messages every day that -- that slip right through those systems.

MR. MEDINE: Turning to the infrastructure, what is the cost to the Internet? Are messages going through more slowly? Do companies lose backbone? Do providers have to invest more resources in bandwidth? How does this impact the system overall?

MR. EVERETT: Oh, the system at various points in the transmission process suffers from clogging of those backbone transmission systems. Also the routers that select the path to distribute and relay the messages can become very easily clogged and slowed down.

A lot of people have a -- have a hard time getting to Web sites that they want to because the Internet connection that their service provider purchases is oftentimes clogged up with incoming mail and -- and both systems are spending time processing those messages whereas, you know, a -- a piece of equipment can only process a -- a finite number of transactions in a matter of seconds, though it does it fairly quickly.

But if you've got you know, tens of thousands or hundreds of thousands of pieces of E-mail, as in a case like AOL, coming into these machines, that's taking up the fixed amount of bandwidth of the -- of the pipe connecting in and if your pipe is full of stuff coming at you, you can't get things out, whether it's your own E-mail or your own clients and customers trying to surf the Web.

MR. MEDINE: Mr. Catlett, do you have anything to add to that in terms of the impact on the infrastructure of unsolicited E-mail?

MR. CATLETT: I'm not an expert on that topic.

MR. MEDINE: Okay, good. Let's --

COMMISSIONER STAREK: David?

MR. MEDINE: Yes.

COMMISSIONER STAREK: I find your analogy of people engaging in commercial -- even if it's commercial spamming -- to industrial polluters to be somewhat strained. However, I'm curious about the nature of these messages. We've been talking this morning mostly about commercial messages, but are there other kinds of messages which are being spammed? For example, political-type messages?

MR. EVERETT: Yes, there are political and -- and religious and -- and news announcement type messages that are -- that are being put out there.

COMMISSIONER STAREK: And what's the percentage of somebody who engages in several chat groups and stuff -- what's the percentage of the messages that are spammed to that person that would be of this nature rather than commercial opportunities?

MR. EVERETT: I have no hard numbers on that but -- but anecdotally and -- and in my -- in my personal experience, I've received very few in the way of political or religious communications. They're -- they're easily outnumbered, probably 40 to 1 or more in my own personal experience.

I -- I think that our approach, the -- the coalition that I work with, is dealing specifically with unsolicited commercial messages because we certainly recognize the -- the great First Amendment tradition of sending out messages of political and religious and social nature that -- that must be protected, and we are mostly concerned with commercial entities who are shifting their costs onto other people in -- in hopes of making a profit at those -- at those recipients' expense.

MR. MEDINE: Commissioner Varney?

COMMISSIONER VARNEY: He's still --

MR. MEDINE: Oh, I'm sorry.

COMMISSIONER STAREK: But the filtration systems would go throughout all these kinds of messages I would think.

MR. EVERETT: Well, it -- it -- it depends on how you operate your filtration system or where -- or where you base your -- your message operations from. We are not -- the proposals that my coalition is putting forward do not put forward a filtering system. They simply say that commercial -- unsolicited commercial messages -- must be on an opt-in basis. If you wish to receive these sorts of communications, you certainly may.

I -- I personally am on probably a dozen commercial mailing lists that are -- are marketing and advertising and industry update lists, and -- and they're a wonderful resource to me, but I didn't start receiving them until I asked for it.

And that's what we're seeing the largest number of large marketing and commercial organizations doing. They have opt-in systems. The types of spam that we've been talking about here today are largely not those with more legitimate offers but are the multi-level marketing, the pyramid schemes, the -- the quack medical remedies, et cetera.

My analogy to pollution was not meant to characterize the -- the quality of the content of the message but simply the fact that the costs are being shifted off of the -- the profitmaker onto the consumers and the recipients in much the same way that a -- a chemical producer or anyone else involved in a chemical process might move those costs out and -- and -- and save those costs on their end by pushing them onto someone else.

MR. MEDINE: Commissioner Varney?

COMMISSIONER VARNEY: I wonder if Mr. Sanford (sic) has any anecdotal or other analogy of your client, is it almost all commercial? Is there a small percentage that's religious or political messaging? Do you have any insights on this for us?

MR. WALLACE: By the way, it's Mr. Wallace.

COMMISSIONER VARNEY: I'm sorry, Mr. Wallace.

MR. WALLACE: Most of the messages that come from our system are of a commercial nature, but we're also a commercial E-mail company. So, I know that as this practice becomes more widespread you're going to see a drastic increase in political and religious speech being sent through E-mail. It's just that we're not in that business, not at this time.

MR. MOUYAL: Let me ask you a question: We've -- we've done for a state tax department to put up a download of tax returns online, and we sent a lot of people from that state to that site through an E-mail campaign and it worked fairly well for them.

The problem is a lot of people don't want to touch it because people that are against it are calling them and threatening them and telling them that I'm going to boycott your company, I'm going to sell off my stocks that I have in your company. So these, you know, major companies don't want to touch it and I don't want to blame them because they don't want to have that stigma.

However, they are very intrigued and very interested in using this as a viable way to move products and services.

And the reason that you're seeing all the so-called garbage advertising in E-mail is because that's the only people that are willing to try it, you know. And I think we need to give the bigger institutions and the bigger companies and the politicians and the charitable organizations good reasons to try E-mail, you know, rather than stigmatizing them with, Hey, if you do that you're a spammer and you're no good and I'm not going to want this and I don't want anything to do with your company, and I'm going to yell as loud as I can to tell everybody that you're a no good heathen. And I don't think that's right.

MR. MEDINE: I appreciate that, but in transition we spent a lot of time talking about the cost of unsolicited E-mail, but maybe we can shift a little bit to the benefits, and Bob Wientzen, who has been patiently sitting here, he's the president and chief executive officer of the Direct Marketing Association, we appreciate having you back again today, and we appreciate your views on the role that unsolicited E-mail can play for marketers.

MR. WIENTZEN: Thank you. I think the first point I would make is that I believe that the cost of spam as we've been talking about it today is absolutely enormous. It's -- it goes away beyond the cost of the technical side. It really goes to the issue of the cost of missed opportunity and the cost that -- that amounts to a reduction in the potential of this tool to represent a -- a new and exciting medium for communicating to consumers and for conducting electronic commerce.

Now, as evidence of that, I would suggest that most legitimate marketers, in fact, the vast majority, are afraid to be associated with it because of its reputation, as the point was previously made. We recently conducted a survey among our members, a representative one, and found that slightly under 10 percent of our members used E-mail at all even though 86 percent of them actively used the Internet and the Worldwide Web. So, the vast majority of them are avoiding it.

Of the 10 percent that use commercial E-mail, 85 percent only use it in the targeted sense and the vast majority of those to their existing customers. So, in effect, what we have is a tool that is being avoided by legitimate marketers because of some of the concerns.

Seventy-five percent of those folks who are using it at all, in terms of commerce, are only going to their existing customers. And they would like very much to be able to offer their goods and services to other people. However, they are concerned about the public's perception. In a way, spam has left a very bad taste in the mouth of the legitimate markets. Not to play too heavily on an analogy, but I think, in fact, that's what we need to correct.

I think the tools are there to correct it. The first one is we already have stated principles in the marketing guidelines that have been worked out by the DMA and ISA, and they do include principles dealing with unsolicited E-mail. I don't think it would take much energy or effort for the existing spammers to adopt those principles, and I would challenge the existing community that's using unsolicited E-mail to look hard at adopting those principles quickly, before it's too late, before the public really does turn itself off to the regular use of this vehicle.

I think if the standards are followed, and if -- that is if people are identified, if people are given a legitimate opportunity to opt-out where it's easily found, easily implemented and absolutely respected, that we might be able to recover public trust in this -- in this vehicle.

The fact of the matter is that E-mail, as we currently know it, is not what should survive. The E-mail of the future could be an exciting marketing tool. It could present consumers with video, it could present them with audio, it could present them with opportunities to seemlessly make choices and gather information.

It could be a great targeting vehicle, and it could do so at very significantly reduced costs. The fact is it will never get there if we don't find a way to self-regulate and do it quickly.

I would suggest that the community of spammers could join with us and regulate themselves now. I think we could, in fact, save this if we move quickly, and I certainly would hope that they would take up our challenge to look at our principles, our guidelines and adopt them right now.

COMMISSIONER VARNEY: Bob, what are -- what would you do about the outliers? I mean, if everybody at this table said, okay or whatever, what would you do about the -- the people that aren't at the table, that apparently represent a significant portion of the mail that's going through the system?

MR. WIENTZEN: Well, honestly, Commissioner Varney, I don't know what I would do about all of the -- of the outliers, but I know that given the volume that's represented by the significant players that we could significantly reduce the volume of questionable mail if the high volume players were to participate quickly.

When that happens, those outriders would be much more easily identified. I think that's the issue. If the top five or top 10 spammers were to quote "clean up their act," then I think those that were not doing so would be much more easily identified.

MR. MOUYAL: I would like to add something. There's, you know, a lot of people that are creating their own operations off the Web Sites, which I think -- I encourage that -- I've spoken to numerous people who have created these and that they use them an a monthly basis and every month that they send out their opt-in list they get accused of being a spammer by somebody, okay?

MR. WIENTZEN: How do you address that?

MR. MEDINE: Well, why don't we -- why don't we leave that as a lingering question. We're going to take a break and then we're going to come back and then the subject on the table will be where do we go from here.

(A brief recess was taken.)

PANEL VII: UNSOLICITED COMMERCIAL E-MAIL: RESPONSES

"Filtering opinion, self-regulatory efforts,"opt-in" and"opt-out" marketing models, application of current law, and government responses."

Ram Avrahami

Jason Catlett, Chief Executive Officer, Junkbusters

Julie DeFalco, National Consumer Coalition

Raymond B. Everett

Jill A. Lesser, Deputy Director, Law and Public Policy, America Online, Inc.

Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology

Simona Nass, Panix/Public Access Networks Corp.

Rosalind Resnick, President, NetCreations, Inc.

Shabbir J. Safdar, Founder, Voters Telecommunications Watch

David E. Sorkin, Assistant Professor and Associate Director, Center for Information Technology and Privacy Law, The John Marshall Law School

Sanford Wallace, President, Cyber Promotions, Inc.

Eric Wenger, Assistant Attorney General, New York Department of Law, National Association of Attorneys General

H. Robert Wientzen, President and Chief Executive Officer, The Direct Marketing Association

***

MR. MEDINE: We're now going to turn to what we do about unsolicited E-mail to basically prevent those who don't want to receive it and as Bob Wientzen said just before the break, turn that into a positive communication. We'll work through some of the possibilities, starting with self-help on one end to government regulation on the other end, and Shabbir maybe can talk to us a little about this.

MR. SAFDAR: Well, I think what we -- what we've found in our survey was somewhat significant. We found a very high number of people who told us how they address the junk E-mail problem. And I do want to point out that one of the responses which I put in our filings but which I would not give too much credence to is bodily harm.

Seventy-eight people out of up to 2,700 said bodily harm for -- and 30 more for jail sentences -- for spammers would be an appropriate thing.   In fact, I have a bodyguard service. (Laughter.)

For the most part, out of up to 2,750 people that responded, about -- about 360 they just read it. I've actually found that to be a higher -- a higher instance than what most people would manage is that they actually read the junk E-mail, you know, because occasionally they find something useful.

I don't know if I should take this lightly with my wife who's reading her -- I picked up her E-mail the other day and discovered a spouse investigation service. And so I'm going to keep that.

Fifteen hundred of the 25 -- 2,700 said that they read it and delete it based upon the subject line. Which means that really the subject lines are obviously text in this industry. Only 315 said that they -- that they have their mail -- their mail reader filtering it. And as users of Eudora that's an interesting and fun exercise to do, as well as for Panix users, there's a lot of maintenance.

And then a very, very few people said they use things like intelligent agents. But far and away the most popular response to -- to junk E-mail, 883 people fell into this category, said that what they enjoy doing and what gives them the most satisfaction is simply responding to the ISP if they could find them and complaining and that there's no better satisfaction than receiving a letter saying that the account has been cut off.

That's -- that's what we've found so far, and I think what we -- what we conclude after talking to a number of ISPs is that these technical solutions that I talked about, that are bandied about here, are really in need of an -- of an adjunct piece: teeth.

MR. MEDINE: So in some sense are consumers acting like cops on the beat reporting people to the ISPs and then relying on the ISP to cut them off?

MR. SAFDAR: Right. And there's some -- there are some aspects of this problem that are becoming interesting once -- once unsolicited E-mail has come from their own ISPs. And we're seeing this drama play out with upstream providers like -- like Mr. Wallace is, where then the complaints get directed at their upstream providers.

As of today, you know, it's not clear that this is how we want the Internet to function based upon greatest account numbers.

MR. MEDINE: Are upstream providers responsive to those kinds of concerns?

MR. SAFDAR: Sometimes, yes. I -- I think actually, you know, without -- without judging, I think that Mr. Wallace could tell us more about this. As of today, I think AGIS is still your provider?

MR. WALLACE: Right.

MR. SAFDAR: And they have been under a lot of complaints for quite awhile.

MR. WALLACE: AGIS is the -- is really the catalyst that has made us form this association and expedite it. So they have taken a proactive position on the issue as well.

MR. MEDINE: Colleen, do you have anything to add to the self-help issue?

MS. KEHOE: As I mentioned before, we find that our most popular response is for people to simply delete the

E-mail. And that is 60, 70 percent say that they do that. We find a much lower rate of people actually retaliating. And I'm not sure how you would define that exactly, but that's what we find.

MR. MEDINE: Okay. I don't know if you have any thoughts.

MS. NASS: I'd like to address that. A lot of people complain about spam and when our customers send it out-- or worse, when our customers don't send it out and people don't read the headers correctly and think that that came from our site, it really puts pressure on the ISP. Just in terms of the time responding to that mail -- if the ISP stands for that. Some providers say the account has been terminated and just create a new log-in ID for that customer.

It's very important that cooperative ISPs not be unduly burdened by people who are complaining to everyone in sight, everybody mentioning it. Even the person that the mail was ostensibly addressed from because people -- people put header information in -- so consumer education is very important as well.

MR. WALLACE: I would also like to comment that I think there are technological solutions that have already been implemented that work quite well. I'll use America Online as an sample. Recently they have implemented a filtering technique that essentially rejects all mail that comes from a forged, nonexistent return path. And not only did they come up with that technology but they distributed the code publicly so that other service providers can eliminate this same technology. That in itself can alleviate the whole problem of forged return paths. I think that's a perfect example of how technology can help -- this is a recent development, I think within the last month. But technology of that sort will continue to be created as the demand increases.

MR. MEDINE: Does that only work if the forged path is a nonexistent one as opposed to just using someone else's path?

MR. WALLACE: Absolutely, but that's just a sign though that you can eliminate one whole problem.

MS. LESSER: It doesn't -- it only works in certain circumstances. For example, it works with a forged or in our case unregistered domain, which means we have to check whether the domain is forged and then we can block from that domain. But with respect to forged header information and footer information, we don't -- they -- there are dynamics of that information that change, so that is very, very difficult. There is no snap solution to that.

So, while we have obviously made our filtering tools better and will continue to do so and continue to spend a lot of resources doing so, again we are still every day finding new problems. So, we implement a filter, it works for about two weeks, let's say, and we need to try to find something else.

MR. EVERETT: And, David, there are -- there's a growing problem with people using a valid domain but invalid account information, so they may create a -- a bogus at aol.com E-mail address in what they send out, and what happens then is that sets up various bouncing error messages back and forth which wind up filling the administrative accounts of the service providers, and I -- I know AOL in some of their litigation has -- has talked and dealt with the high cost to them and to other Internet service providers of receiving and storing and dealing with those administrative accounts that get bombarded in this way.

COMMISSIONER VARNEY: I have a question here. It seems to me that it might be useful for a moment to think about those mass E-mailers that do things like that, that have either forged domain names or forged domain accounts and why not ask the people in the room and at the table if, generally, the kinds of E-mailers who do that are transmitting what most of us would agree are fraudulent content. They're the people transmitting the get-rich-schemes. Is there a correlation between the people that are engaged in the kinds of practices you've all just described and the degree of veracity in the messages they're sending?

Then my next question is, if that's true, then one solution has got to be -- this is absolutely within our fraud and deception jurisdiction and we ought to be prosecuting those people and the question is how hard is it to get to those people?

MR. MEDINE: Eric Wenger from the New York Attorney General's Office has had some experience in this area.

MR. WAYNE: I think that you're 100 percent right that we're seeing a lot of deception, not only in how the messages are sent, the header information and so forth, but the messages themselves. And we brought suit against Kevin J. Lipschultz (phonetic) which -- he is a blacklisted and notorious spammer, and the -- the point is that not only was the -- the return E-mail addresses were always fake, not only the account fake but the domain used didn't exist, and --

COMMISSIONER VARNEY: And the content of the messages --

MR. WENGER: And the content of the message was -- it was constructed to look as if it was a testimonial from the happy customer, when in fact he was sending notes and generating fake names to go along with it to make it -- it appear that these people were happy with his magazine subscription service, when, in fact, it was just him disguising, you know, disguising the origin.

COMMISSIONER VARNEY: These are the fraudsters, right?

MR. WENGER: Right.

COMMISSIONER VARNEY: And the State Attorneys General and maybe the FTC and other places already have authority if we can find them to prosecute them, right? Now --

MR. WENGER: Clearly, I mean, when messages are deceptive and I would also argue that when the messages are -- are, you know, the subject lines and the headers and things like that are -- are disguised as well.

COMMISSIONER VARNEY: Okay.   Now let's take for a moment the companies -- maybe Cyberpromotions that say, you know, you may not like, maybe get their mail. But they say who they are, they have their message. Do you do anything to check the veracity of the content or when people are buying their software for -- I mean, do you have any way to do auditing or checking that people are engaging in fraud in software?

MR. WALLACE: I think that our relationship with our customers is very similar to a telephone company is with their customers that we can't predict what they're going to do. If they do -- if they -- if they send out an illegal fraudulent mailing and we receive note of it, then it's our responsibility to do something about it, but we can't eliminate it before it happens.

MR. MEDINE: Can I just clarify -- aren't some of the mailings that you send out almost like multiple offers where you basically provide the -- the package that those offers go out in?

MR. WALLACE: Yes, we do. We -- that's part of our own mailing service.

MR. MEDINE: And in the context of your own mailing service, do you check out all those offers to make sure that they are not fraudulent?

MR. WALLACE: We do the same thing a newspaper would do. We -- we have guidelines, we don't allow adult ads, if we see something that looks outright fraudulent, we'll investigate it to a degree. But we're really not in the direct business of checking every single advertisement that comes in. But if someone's breaking the law, there are remedies out there -- there are remedies out there available currently.

And like Mr. Everett said in his statement, there are lawsuits that are also dealing with these issues that are defining laws as well. So I think there are proper remedies already in place to address that issue.

COMMISSIONER VARNEY: It seems to me, then, that, you know, one of the things that we are kind of circling around this morning is that there are really bad actors and nothing anybody can do to get to the bad actors. Well, let's take the bad actors and put them aside for a moment. Now let's look and deal with everybody else.

We have massive amounts of unsolicited E-mail moving through the system. Some people like it. Some people don't. It seems to me what -- what's got to happen now is we've got to -- you've got to work with us, being law enforcement, State Attorneys General, on how we can go after, effectively and quickly, the people that are perpetrators. But then it seems to me that there's a whole other realm here, and that is you've got to work with each other to figure out what are the right rules for the -- what I'll say are the legitimate free speech, commercial free speech, that's going on within it.

MR. MEDINE: Well, let me pose that to Jay McCrensky who is the -- who has joined us as the executive director of the Internet Marketing Association.

MR. MCCRENSKY: Thank you very much. We're a new association, a new marketing association that's been -- that's formed actually to solve these sorts of problems and to address these self-regulatory issues. And what we've come up with is a -- sort of a -- an innovative solution to the problem and that is to certify E-mail and to -- and to undertake major public relations and public education effort to educate people on the logo that they will be looking for on commercial E-mail.

We're an association -- not just of the E-mail marketing companies but of advertisers who are interested in developing E-mail as a viable communications tool, of -- of ad agencies, law firms and Internet service providers -- that's our potential members. So we really represent all of the players, and what we've come up with is a five-part program that we call certified E-mail.

The first is that the applicant who uses the logo on their masthead would -- would have to maintain very strict standards. Everything that we're talking about and more, with regard to ethical practices, with regard to content. Something that we actually can enforce.

Secondly, we want to -- as Al Mouyal our president mentioned, we want to turn junk mail into gift mail or gem mail. We want to provide -- one requirement is that any certified E-mail must provide some sort of specific benefit, a tangible benefit to the recipient, in terms of a major discount, a coupon, 25 percent off if you come to our Web site and buy it, a free gift -- something very tangible that turns it into gift mail.

Third, the recipient will receive points towards free gifts or free access, free AOL or free ISP access. And this really ties into the traditional role of -- of advertising in the economy that really enables the free media -- and can do so on the Internet also. We can create that framework.

And fourth we plan to provide revenue to the Internet service providers that are members and that work with us and provide opt-in lists of their members who can be marketed to.

MR. MEDINE: Do you have any current ISPs as members?

MR. MCCRENSKY: We're talking to AGIS, the backbone company, who is very excited about this, and has said that they will bring us their 700 ISP members and clients.   We're also talking about a combination with the association -- that's in discussion as well, and we're hoping to really combine forces here.

MR. MEDINE: Were there any other points of the program or is that -- does that pretty much set it out?

MR. MCCRENSKY: Did I cover five?

UNIDENTIFIED SPEAKER: Um-hmm.

MR. MCCRENSKY: Okay. Oh, also, the fifth point is that we will -- as with all of the applicants and users of certified E-mail must provide a direct opt-out specifically along the lines that I would suggest is very easy to opt-out and -- and you get a confirmation back and that would be enforced.

MR. MEDINE: George Nemeyer, does that -- do you rest now assured that the specific E-mail problem has been solved?

MR. NEMEYER: Not really. (Laughter).

Well, the problem that we see from the provider community is that as long as the situation is an opt-out one, we face a flood of incoming mail and if the DMA's projection, which I fully expect will happen, that people start sending video and audio clips along, the quality of traffic that this is going to cause on the receiving end is huge, because of the fact that these things are orders of magnitude larger than an average piece of text mail.

The other problem that we see is the fact that you've already heard the testimony regarding the amount of administrative time that it's taking at the receiving end. Basically what we're concerned about is the fact that the receiving end is bearing the brunt of the cost. Now he mentioned some -- some revenue sharing or something with the receiver -- I'd like to hear more in detail about that from his side.

We've heard of one from Mr. Rines' organization which largely makes you forfeit your membership list in order to qualify for that, plus you have to negotiate with them to figure out what they might pay you, so that is the offer they're extending. It is seen as more -- as more smoke screen than -- than real.

So from our perspective I don't see that as long as it remains opt-out as the primary basis that it's really benefiting the receiver or the consumer.

MR. MEDINE: Mr. Avrahami, do you have some views about opt-out as a way to go to try to address this problem?

MR. AVRAHAMI: I run an operation that actually provides global accounts for any consumer who wants to use it or who wants to register. They don't need to be specific to Panix or AOL or anyone else. It's also not limited to any specific spammer-like promotions or AGIS or anyone else.

Our notion is that technology can only go that far and as long as we want to have Internet as an open communications medium you will have companies who will use that to send commercial messages and there are going to be consumers who will be annoyed with it.

So, we try to communicate between those consumers and that question from Commissioner Varney about trying to communicate or to try to talk between the spammers and the consumers who get that, and what we do is we allow consumers to register their interest in not receiving any commercial solicitations that's on our Web site of www.cd.cd.com. And we also ask them to forward to us the -- the spam that they receive.

And what we do is we go to the spammers and tell them, you know, it's really beneficial for you from a business perspective to honor the request of those consumers and remove them from your mailing list. I mean, those are not the ones that you want to receive the E-mail.

And if you do that, you will not be flamed, you will adhere to some kind of ethical guidelines and -- and it will -- we also hint to them, you know, it's going to help you prevent any regulation on your business.

A company that -- that adheres to our request is Cyberpromotions and I will fully state for the record I have not found them violating our request. And any consumer that asks us not to be spammed by them, they have complied and I have not found any real violation of that.

Having said that, out of the hundreds of requests that we have sent to spammers, over 80 percent of them would not respond at all. I mean, we --

COMMISSIONER VARNEY: How many companies are you talking about, roughly?

MR. AVRAHAMI: I know that I have sent our message, our request, to almost 1,000 spammers and some of them are hard to get to, because some of them open an account, spam, close it, start again. I have a data base of over 2,000 spam messages and, by the way, answering -- I do have answers to staff questions before now. About 2 percent of solicitations are political, religious and I have more detailed figures saying how many are in essence sex messages, computers, Internet, all that information is available. I have submitted it in my comment and I have a more updated list with me today.

COMMISSIONER VARNEY: Would you submit the updated list also for the record?

MR. AVRAHAMI: I will be happy to.

COMMISSIONER VARNEY: Thank you.

Okay, so you've got 2,000, a database of 2,000, can you break that out for us a little bit? How many would you put in the Cyberpromotion category -- companies, enterprises, corporate -- that are responsive to your requests and how many are repeat offender individuals that you're not getting the responses from? Sort of give us the landscape of what you're seeing.

MR. AVRAHAMI: When we're talking about how many Cyberpromotions, it's very difficult to know from the name of the company exactly how big it is. I can tell you that I see almost no known name. So, when we -- when we hear from the Direct Marketing Association about their interest to provide ethical guidelines or from the Internet Marketing Association, we need to understand that has almost nothing to do with the current phenomenon of spam.

I mean, the problem is not with DMA members, the problem is with all those individuals and small businesses. And I am corresponding with them and I understand why they are there and, in a way, I have some sympathy for them because they have heard about the great riches on the

Internet in which you finally don't really need to be a big company in order to make money. And they say, Well, let's go and do that and, you know, it's fairly cheap we have only a few hundred dollars and you can -- you can reach a vast market. And they do believe they have a product that they want to sell, and, well, in a way they are like any direct marketer. They try to reach as many as they can at the cheapest cost and make sure that they cover their costs.

So, those individuals, those home businesses, those people who want to live the American entrepreneurship dream, they are the ones who go there, not necessary with that intention, but with the tools that they have and they try to reach the market. So, here we have the problem with that First Amendment and wanting to provide commercial space and -- and allow them to reach their consumers.

COMMISSIONER VARNEY: Where do they get the tools?

MR. AVRAHAMI: We have heard about the software and we need to understand usually three steps in -- in getting the spam.

The first one is to be able to get the E-mail address of the recipient. And we have fairly cheap software that will do that. Sometimes -- and that is not mentioned here, you don't really need the software, you can just buy the mailing list. Those lists are offered now for as cheap as $11 for a million addresses, which is really negligible. I have some statistics here that averages about $40 dollars, which is 1,000 times cheaper than mailing lists in the real physical world.

And we see the cost of both the software and the mailing lists going down because there's actually no barrier and no cost associated with duplicating those lists. So, we don't see that going -- going higher or blocking. And, again, we, you know, in a sense want to help those small entrepreneurs get, you know, get the tools that they can at cost rather than at some artificial barrier, and the problem is -- the problem is what is the consequence for consumers.

MR. MEDINE: On that point, we also have with us Roslyn Resnick, who is the president of NetCreations, an Internet marketing company, and appropriately co-author of a book called The Internet Business Guide, Riding the Information Super Highway to Profit. Can you tell us why it is maybe that market structure currently on unsolicited E-mail makes opt-out not work, if that's the case, or why you think that there's an opportunity, if you would like to comment.

MS. RESNICK: Can you hear me?

UNIDENTIFIED SPEAKER: Yes.

MS. RESNICK: Okay. Thank you, David. As you know our company is NetCreations and we operate a 100 percent opt-in E-mail service on the Internet, it's called Post Master Direct Response, and what we do -- I can tell you first of all we oppose both unsolicited commercial E-mail as practiced by the firms such as Sanford Wallace's -- we also oppose the DMA's opt-out principles. We believe that they just won't work on the Internet.

MR. MEDINE: Why not?

MS. RESNICK: Well, let me talk about both of them. As far as opt-out, opt-out, the whole centerpiece of opt-out is what they call in the postal world a mail preference service -- run the Internet to try to create an E-mail preference service. And the reason why mail orders would use that in the real world is because if somebody doesn't want to receive the postal mail you're going to waste a dollar or two dollars reaching the person. There's an economic incentive. On the Internet-- I mean, where you can get a list of a million names for $11 bucks, obviously there's no economic incentive. So, you know, that's opt-out.

Unsolicited commercial E-mail, I can tell you from our own experience, you know, despite the fine words we've heard here today by Sanford Wallace and other admitted spammers, I can tell you that spammers bounce their E-mail off our SMT server, you know, all day long -- you know, every day, every week, all year long. And basically what they're doing is they're stealing our service. You know, they're stealing our bandwidth, they're forging their message headers to make it look like their spam is coming from us, and our belief is that these spammers should not be regulated, they should be prosecuted, and I think the laws exist to do that today.

Now as far as what we do. We do not spam people to get them to our site to opt-in. We have a number of partnership programs with other sites, we have about 10,000 other Web sites pointing traffic our way. And as a result we get a lot of traffic to our site. When people come to our site, they're given an opportunity to click on an icon and go to a sign-up page where we fully disclose what information we're going to send them, and then they can opt-in to any of 3,000 different mailing lists on topics as diverse as Web design, gardening, scuba, whatever the case may be.

So, we allow people to opt-in. After they have opted-in, they get an automated message from our server that says, Hey, you've opted-in into this or that list, if somebody signed you up in error, if you've changed your mind and you want to get off, simply opt-out now by pointing this E-mail message to delete via PostMasterDirect.com. And that way they opt-out before they get commercial message one.

If they decide to stay on the list, what happens then is a marketer can come to our site, because essentially we act as a manager and broker and list owner, similar to what a list brokerage would do in the real world, a marketer would come to our site and pick out, say, the Web design list to mail to.

Well, what would happen then is the marketer would send us a copy of the E-mail message that it wanted to send out. We send that E-mail message to the people who are on that list, but at no time do we ever disclose the name or E-mail address or any other information about the person on our list.

And, you know, you can say I know that there's a lot of people in the marketing community who think that our approach is a little too pure, a little too rarified, something that would never catch on in a big way. But let me tell you that we have over three million E-mail addresses under management in 3,000 different categories. And we had -- despite -- you know, despite the statistics presented by Bob Wientzen from the DMA, I mean, the truth is the most legitimate marketers would not even use a service like ours.

You know, but despite all of the bad publicity created by spammers, the fact is that Smith-Davis is our biggest client. We've had CMP, Eye Chat-- lots of major software and high tech companies use our service and get response rates on the order of two to three times what they would get from postal mail at a cost that's two to three times less expensive.

So, what I'm saying is that opt-in does work and I hope that before the FTC gives its blessing to spammers, I hope that it will consider opt-in.

MR. MEDINE: I don't think we're blessing anybody today, we're hearing -- (laughter).

One question for you this morning was or assertion was that even opt-in E-mail senders suffer from the reputation of unsolicited E-mail senders, and do you get complaints back about your messages because people think they are unsolicited?

MS. RESNICK: Well, I -- I can tell you that the other piece of puzzle here, which I didn't mention, is that once somebody opts into our list and stays on our list, after getting a confirmation message, every piece of E-mail that that person receives contains a header, right at the top, that says this is a Post Master Direct list, this is not a spam, to get off the list forward it to Delete @ NetCreations.com. You know, that's what we do so that every one of our message is identified.

Now, having said that, it sometimes happens that someone signs up for a list of ours today and then three weeks from today gets an E-mail message and forgets that he signed up for a list. And that person flames us, sends us an angry E-mail saying why did you spam me, blah, blah, blah -- and we answer all of those messages individually.

We point out that this individual really did sign up for a data base and at such and such a day and such and such a time. Sometimes we can even locate the IP address. And then usually the person apologizes and says, God, I've just been hit by 10 other spams today and I thought you were one of them.

So, what I'm saying is these are marketers like Smith-Davis who work with us, understand that when they send out mail to 30,000 people they might get a couple of flames, but this is the Internet and they are willing to deal with it.

COMMISSIONER VARNEY: What happens -- talk a little bit more about people who use your server so that the mail looks like it's coming from you when it's not.

MS. RESNICK: Well, I can tell you that -- yeah, people -- other people on the panel have talked about this already, but what typically happens is we get mail -- and I can tell you Sanford -- and maybe this was before you changed your policy to anti-relay -- but we have gotten mail from AnswerMe.com, which I believe is one of your domains. You know, people have used that domain as well as many other domains, like SaveTrees.com -- they're pretty notorious as well. What they do is bounce off our SMT server and they forge our message header to make it look like their mail is coming from us.

So not only does that waste our bandwidth, that's really the -- the least of the problem. The worst of the problem --

COMMISSIONER VARNEY: Has anybody who's doing that been prosecuted under state or federal law?

MS. RESNICK: Not that I know of. I could tell you that it's very difficult to track these people down. I mean, we ourselves have E-mailed these people, called these people, threatened to sue them, and they're just nowhere to be found. I mean, we would love to get our hands on these people and file a lawsuit, but it is just very difficult to track them.

COMMISSIONER VARNEY: So what's the solution?

MS. RESNICK: Well, let me say this. You know, my view is that, you know, even though it's difficult to track these people down and prosecute them, I think it needs to happen. And I think that the day the first spammer goes to jail, the rest of them are going to run for cover. And we're not going to have this problem.

I mean, I think that if Sanford Wallace and other spammers are willing to act in a legitimate way, like I know that Sanford just recently started an opt-in E-mail service that apparently has, what, 38,000 people on it?

MR. WALLACE: Yes.

MS. RESNICK: I think that's a very, very good step in the right direction. And I don't think that unsolicited E-mail is necessary to foster commerce on the Internet. I think that there are other options and that the bad guys should be prosecuted and the good guys should adhere to a set of principles and create a win-win situation for marketers and consumers alike.

COMMISSIONER VARNEY: Let me just ask Sanford a followup. You're not doing -- what is the practice called? Relay?

MS. RESNICK: It's called relay.

COMMISSIONER VARNEY: Do you -- you don't do relay from your opt?

MR. WALLACE: No, we don't it from our office and we just -- really it's a strict policy that we adopted last week (laughter) to -- to address that issue.

COMMISSIONER VARNEY: Good!

MR. WALLACE: I would like to make two comments, if I could. First of all, not to keep bringing up AOL, but they have implemented an anti-relay code in Send Mail, which -- which eliminates the ability for people to relay E-mail off of their servers. So there is technology available also to stop people from having the ability to do that exact practice. That's -- that's one of two comments.

COMMISSIONER VARNEY: Can Jill comment on this? Is that right, Jill?

MS. LESSER: Yes, actually it is right, but one of the things I want to comment on is, just in terms of the way the Internet works and the way that we've developed in terms of open standards, the SMTP Mail Protocol was developed as an open protocol, and one of the reasons why the relay function or systems are open is because when the Internet started it was thought that, you know, it -- that was a productive way of trafficking E-mail. So if your server couldn't handle particular E-mails, it should be able to be gone, you know, through other services.

And I think, you know, when you -- when AOL has to harden -- it's called hardening its system, or other services have to harden their systems so that their service cannot be used for relaying, it is sort of a fundamental change in the

Internet. Because where you say, Okay, fraudulent behavior is now governing the way the system, built on open standards, is working.

So, I mean, I think that it's important to note that we -- we have in fact tried to prevent relay from AOL so that our customers, because what would happen when you relay off of AOL is our customers think that we are spamming. So, from a relationship from our customers point of view that was absolutely a practice we had to prohibit as quickly as possible.

COMMISSIONER VARNEY: David, I think that this is really, really an important point. Jill, let me say it back to you and see if I've got it right.

When I send E-mail and I type in my little address and I hit my send button my E-mail goes out and I try to bounce this around the Internet system until it finds a free server and then it goes to wherever I'm sending it.

MS. LESSER: Well, when you send it, it's going to go through your ISP as SMTP server --

COMMISSIONER VARNEY: Okay.

MS. LESSER: -- unless you redirect it.

COMMISSIONER VARNEY: Okay.

MS. LESSER: So, if I have an ISP account and I just send mail --

COMMISSIONER VARNEY: Un-huh.

MS. LESSER: -- it's not going to -- it's not going to bounce around.

COMMISSIONER VARNEY: Okay.

MS. LESSER: But it -- it can be bounced around.

COMMISSIONER VARNEY: Okay. So the ideas is that as packets of data move through the Internet they find the appropriate server and if that server is full or engaged it goes to the next server and goes on. And the whole concept of Internet was that all these servers have to be able to talk to each other and everything has to move freely without restriction.

Now what you're saying is that in order to prevent the fraudulent use of somebody's server, you're doing something called "hardening your system," which is in some way kind of putting a choke on the system.

MS. LESSER: Um-hmm.

MR. WALLACE: The bottom line is that most people agree that the open nature of SMTP is a security hole more than an infrastructure of the Internet. Everything can function just perfectly fine without the ability for people to hijack a third party SMTP gateway, and it can be configured in a way so that the people who do want to leave that port open can selectively -- they can select who can relay through that port. So, there really is no threat to the backbone of the Internet by closing up an inherent security hole.

COMMISSIONER VARNEY: Does somebody want to comment on that?

MS. NASS: The problem with shutting off relaying is not just that it prevents fraudulent use of your port, but it also prevents legitimate use of your port. For example, we -- in talking to administrators of other spam sites said, Why don't you turn off relaying? And they said we host virtual domains, we can't do that.

Basically, the way relaying works for send mail, which I think is the most popular E-mail for ease of use, et cetera, is that it relays by default and the -- the manager of -- of the send mail codes has posted to his Web site a two line fix -- I think it's a two or three line fix -- to set up relaying, but the problem is that only works for really simple systems.

If you're doing anything complicated, you need to know the internals of send mail in order to not, you know, bounce your customers' mail who have virtual domains. For example, one of the things about the Internet is that anybody can register my company .com and even if they're a one-man operation or a one-woman operation or whatever, they can have a presence on the Net that makes them as much of a player as anybody else.

MR. MEDINE: Is that what you meant by virtual domain?

MS. NASS: Yeah. Where they -- they don't actually have their own server but they have their own domain to appear like it does.

MR. EVERETT: For small ISPs, going into -- delving into the guts of their mail systems can be very dangerous and can violate service contracts that they have with their hardware and software vendors, so I talked to a number of small ISPs for whom disabling relaying not only in case of virtual domains but simply in the cost to their system administration makes it an unworkable situation.

MR. CATLETT: Could I add that one of the causes of the major outages that we've seen, you know, has been attempts to thwart spam and to put into place provisions such as these.

MR. MEDINE: I would like to return to the question of opt-out, because of the questions and I would like to pose it to Bob Wientzen, what about opt-in?

MR. WIENTZEN: Well, I think that opt-in provides a very, very limited opportunity for the market to go out and prospect. It does not deal with the issue that direct marketers are always concerned about, which is how do I make new concepts, new products available to people. And historically it has been found to be ineffective in dealing with the kinds of numbers that are really necessary to make most businesses viable.

On the other hand, opt-out does provide for people to express a desire not to receive marketing information and it has, in fact, worked in other areas. The key thing to keep in mind is it doesn't have to be an absolute kind of event. I'm perfectly comfortable with having a worldwide opt-out system, which we're in the process of developing, and I want to update the Commission on that, but that doesn't mean that there can't be selective opt-in systems that are commercial enterprises -- Roslyn and others -- can, in fact, I think operate quite effectively with targeting opportunities for people that are opt-in.

But I believe that -- that what we're hearing from the public is that many people simply want to say, I don't want to participate in this process. There are -- much of the discussion today clearly is among a very, very small community. It's a small community made up of people who are very actively involved in -- in using the Internet in a lot of different ways. In many cases the general public simply want to say, Don't count me in. And I think we should give them that opportunity.

I'm pleased to report that we're in the final stages of implementing a worldwide opt-out system that will give consumers the ability to say, I simply don't want to participate. While we recognize that there will be some challenges to that, we think that we can make it work. It will have the feature of saying to consumers that if they get on the -- on the Internet and give us the information, we'll go back to them and confirm so that we know that they are, in fact, so that we know that they are, in fact, being identified correctly.

We'll have a national system that will be in operation within six months, and we're confident that we'll able be able to expand that globally within a year. We've already, basically, talked to 27 countries -- direct marketers in 27 countries who have signed on with the concept, and I'm comfortable with -- we're going to have a way for reducing very significantly the amount of unsolicited E-mail.

Now, that won't eliminate it, I know that, and we've never made that claim. But I think we can get the agreement of a lot of the people sitting around this table, I've already had preliminary discussions with a number of them who have said, Fine, if you have an opt-out register, we'll participate. And that will, I believe, very significantly reduce the amount of -- the extent of this problem.

MR. SAFDAR: Can I address that, please? I hope that, you know, with due respect to the DMA and these others and hoping this will result in some good. We all appreciate the irony of being at this Privacy Workshop for four days and hearing about a global data base (laughter) of E-mail addresses, which is, so far as I appraise, not going to have any official Government oversight, especially since it's going to be international in nature, and I think we have to look a little harder for other solutions. I think that's part of it, but I'm not -- I'm not convinced that that is the end all, be all of what's going to get us there. I'm not sure that the solution isn't worse than the problem in some cases.

MR. WIENTZEN: Can I comment on that? I mean, it's one thing to say that there's -- there's not going to be a global data base. The fact of the matter is it will be comprised of people who have voluntarily participated, number one, and number two, when we give them full information about exactly what will become of the system.

So, I mean, it is not a de facto assumption that I think we can accept that there's something wrong with that. Nor do we want you to believe that it is the ultimate solution. We think it's part of the solution. We think that a lot of the things that have been discussed here today need to go forward. We're going forward with one part. I would not suggest that others proceeding should stop and -- and just hang on this one solution, but I think it is part of what will be a worldwide solution.

MR. MEDINE: Deirdre Mulligan -- you want to speak,

Ms. Mulligan?

MS. MULLIGAN: Yeah. I think we've clearly found that there are outliers and I think we've also found that there are things to be done about that. And that clearly the market is having a tough time responding. We've heard from ISPs, from DMA, and from the consumer side that there are real costs here that can be identified and that the market feels as though it is engaged in a technological race.

I think there is clearly some room for government here, if anywhere. And, that said, I think there is some easy answer and then there are a number of answers I want to say I think we should proceed with very, very cautious small steps. I think the easy answers are the fraud, the accuracy of the information, acknowledging that there is a right in this country to speak anonymously, at least in the political context, and that we should be sure that any solution remains -- keeps that kind of core privacy value.

I think the harder questions -- I would -- I would like to start with just saying that this is a little anecdote. People talk about spam and think all the world's talking about the same thing, and I think possibly we may not all be.

I walked into an office of a staffer on the Hill the other day who led a discussion by saying, I came to the office this morning and I had 500 E-mail messages that said, "stop abortion now," and I need to stop that. And I said well you're not talking to the right person. I said that may be spam to you. I said, you're in a political office, there's a vote on the partial birth abortion bill tomorrow, you're -- I said, this is political speech. I said, You may not ban this.

I don't care what else you want to do, that was spam to him. And I want to caution that what we think is bad speech here -- be it commercial speech or advertising, may not be what they think in Europe, may not be what they think if this bill gets to the floor of the House or the Senate. And then I think labeling or starting with a presumption that when there is a problem, be it a market problem or another problem, that where we start just banning speech is a bad idea.

Similarly, labeling -- you know, I think that there are some serious questions whether or not we can force mandatory labels on speech. I think that also raises some very, very scary, scary questions of where we're going, especially if you want to look at where we are right now with regard to the Communications Decency Act, and I think where that leads me to is that mapping old solutions onto a new medium is problematic.

I think we run the risk -- we are arguing in the CDA that the Web is more like print than broadcast. Well, I will argue that E-mail is not fax, it is not phone, and it is not our post office. It is really unique and I think that while I agree that opt-out is problematic, I think that requiring the creation of a list in order not to receive mail is problematic.

I do not believe that when we have Aristotle taking voting registration lists and setting up mailboxes for every resident in the State of California, we don't get a receipt -- we're receiving their government and commercial mail that they choose.

But opt-in might raise some series questions too. Do I have to put my name on a list if I want to get speech? I'm not so sure that's a good idea. I think that what this does tell us is that we need to give the people who are operating in this medium a chance to think about how to structure a system that actually fits with E-mail. And I think that some of the ways to go, you know, should be pointed out. There are ways with filtering, with how we do that more effectively.

I think there are also some interesting ideas about how do we create a decentralized global solution that allows people to control mail coming in and out, recognizing that I may not want to receive mail from NetCreations and I may want to receive mail from Cyberpromotions, but not right now (laughter).

So, you know, I think that the closer we can get the control back to the level of the individual probably the better off we are, especially because of the global nature of this medium. I think what I would propose is that there aren't any easy answers, and I would urge both the Commission and people who are looking at this in Congress to take those easy steps.

I would encourage that we try to set up a process -- I would prefer that it was an Internet-focused process that had representatives from the technical community, because I think we saw yesterday that they have a lot to show us. Representatives from the public interest community, I think you will often find that privacy and fraud sit on opposite sides.

I would sit with National Consumers League and sometimes I'm concerned about anonymity. They really don't care about anonymity and we need to be in the same room so that we have kind of a full picture of how we deal with consumer issues and civil liberties.

And the marketing community -- I think you guys have a lot to lose, as Bob Wientzen pointed out. You need to find a solution that works on this medium and I think it's going to require us all to take steps forward in our thinking.

COMMISSIONER VARNEY: Well, you're from the Center for Democracy and Technology, are you willing to commit your organization to following this up and maybe working with Bob and Walt and our friends from the Internet Marketing Council as well as the individual groups here? I mean, can we and will you all do that? I mean, can we expect that there can be a dialogue and maybe you can come back to us in six months and tell us kind of what you figured out?   Are there other possibilities?

MS. MULLIGAN: We have been brainstorming, we have been talking with other people and I think we really are interested in sitting down with everybody and figuring out the possible solutions. I don't know that we're going to come up with any solution. I think that one of the things we've learned from the Internet is sometimes --

COMMISSIONER VARNEY: Multiple competitive solutions.

MS. MULLIGAN: Are the best way to go, but yet --

COMMISSIONER VARNEY: How about other people at the table? I mean, would you-- would you all do that? Is that something that interests you?

MR. WALLACE: Absolutely.

COMMISSIONER VARNEY: And could you make a commitment that you could come back to us and tell us kind of where you are and what you found? I mean, I want to emphasize something, I don't think -- although I really like what the Internet E-Mail Marketing Council is proposing, I don't think it's the only solution. As in privacy we've got P-3, we've got Truste, I think there can be a multitude of solutions. And I don't know that this issue, the E-mail issue, is as susceptible to multiple solutions, but I think you all ought to tell us. We probably shouldn't tell you.

MR. AVRAHAMI: I think the question is really how do you force a solution on the wide market. With all due respect to the global lists, how can you reduce the problem of spam if none of the companies who are going to use this list is now spamming?   And what about all those companies that the industry cannot force, you know, cannot force to use that list? How would they --

COMMISSIONER VARNEY: But you know what I think the people at this table need to sit down and talk to each other and tell us how we can do that. I don't think anybody at this table knows the answer to that.

MR. RINES: Well, that's one of the key issues in self-regulation and it's one of the reasons why participation in an industry group is so important. I know that IEMMC, for example, really sort of mandates inclusion in our global filtration system because the only Internet backbone provider that allows commercial E-mail is AGIS, and AGIS only allows it with the mandate that you are a member if IEMMC and therefore your mail has to be relayed through a filtration system.

MS. NASS: Commercial, unsolicited?

MR. RINES: Right, unsolicited, right. And while we agree that opt-in does have a place in the marketing spectrum, we would also argue that so does opt-out given the right control and the right respect to the recipient.

MR. MEDINE: I want to second Commissioner Varney's request for you all to work together and if we could facilitate that process along the way we'd be happy to do that. There's, of course, another process going on down the street with a number of proposals pending on this very subject and David Sorkin, who teachers courses in cyberspace law, information law, and policy and consumer protection at the John Marshal Law School, has agreed to give us an overview of what some of the ideas are on the Hill to address these concerns.

MR. SORKIN: Thanks, David. I want to talk about some pending legislation both at the state level and the federal level. I'm not aware right now of any legislative proposals in any other countries, although I think that's certainly something that could happen, is likely to happen if we see some legislation passed here, and something that we really need to be thinking about as we talk about drafting potential solutions.

There are three bills currently pending in Congress, two in the Senate and one in the House. There are also relevant bills pending in about half a dozen states. I'm going to go through them topically rather than by jurisdiction.

There's currently one federal and three state bills pending that would make some -- most or all unsolicited commercial E-mail illegal. Representative Smith's bill, House Bill 1748, at the federal level, there are similar bills in Connecticut, Nevada and Rhode Island. There is also one in Colorado, although all the provisions relating to E-mail were deleted from it before it was passed. I think at least two of the bills on the state level have passed one chamber of the state legislature.

There are a couple of bills pending that would, as I view it, destigmatize unsolicited commercial E-mail. I think these -- to editorialize quickly -- I think these are the biggest danger of all because these could dramatically increase the volume of unsolicited E-mail. Instead of getting one or 10 or 100 or 1,000 pieces every day, we could be talking about millions or billions or trillions of pieces of mail.

Those bills are Senator Murkowski's bill in its present state, which is Senate Bill 771, which is basically a tagging or labeling bill. It would require unsolicited commercial E-mail messages to be labeled "advertisement." So they would still be transmitted over the Internet, they would be received by the end ISP. ISPs would have some burdens in the bill to block them out at that point if the recipient requested it; otherwise, the recipient would have the option of deleting it or actually reading it, which fewer and fewer would do.

There are a couple of bills pending in both houses of the legislature in New York State that would also require labeling. The Direct Marketing Association's proposal in some ways relates, I think, to this in that it also would destigmatize unsolicited commercial E-mail.

There's a product out on the market -- I don't know if many of you have purchased it -- I personally don't buy spam very often, but it's a product called Spam Light. It has fewer calories and less fat than Spam, and I take it the major advantage of it is that you can eat a lot more of it (laughter).   And this isn't advertising for Spam Light -- it's the DMA guidelines.

So that proposal -- and on the legislative side I'm talking about Senator Murkowski's bill in its present state and the New York bills -- as I view it, it would destigmatize unsolicited commercial E-mail. On their face those bills would help consumers by helping them filter it out, but I think they would also cause major problems.

By the way, pretty much all of the bills would require companies to honor individual opt-out requests. I don't think there is any controversy about that at all. In fact, it may well be that under existing harassment laws in many jurisdictions that's already in place, that if you ask not to receive further contacts from somebody they can't contact you anymore. I think that's pretty meaningless on the Internet where it's so easy to create a virtual presence. But in any case, that's not really very controversial.

The final bill that's pending now was just introduced within the last couple of days by Senator Torrecelli, it's Senate Bill 875. On its face, it appears like the second category in that it will destigmatize unsolicited commercial E-mail. It doesn't have any labelling requirements in it, although it would require senders to honor individual opt-out requests.

It does open the door, I think, to a somewhat more effective solution by incorporating an Internet standard provision. I know that most people here probably have not seen the bill, so I would encourage you to read through it to find this. But, basically, what it says is that any standards adopted by an Internet standard organization, and it gives a couple of examples, including the IETF, the Internet Engineering Task Force, which traditionally has been more of an engineering and technical community than a policy group, although it does -- it is involved to some extent in policy, that any standards adopted by a group like that would also have the effect of -- of law, in that a civil action could be brought based on violations of those standards.

Depending on how that bill is interpreted, and I think it's going to have to be changed in some instances, that could end up enforcing an opt-in rather than an opt-out system. Which, as you've probably been able to tell so far, I think is the only effective solution to this problem.

The chances of these bills passing are pretty hard to tell. I suspect that the destigmatization bills, the labeling, the companies that specifically opt-out, are going to be viewed initially as compromise bills. I'm hoping that the Internet community will make it clear that those aren't compromises, those are worst case, because they're going to bring a lot more marketers in and they're really going to increase the magnitude of the problem, and what we may end up with is -- is no legislation at all.

So, we may have some time to develop an effective solution to the problem before we get a bad law imposed.

MR. MEDINE: Thank you very much. Eric, why don't you reflect on any proposals, particularly First Amendment implications.

MR. WENGER: Well, I don't think we should start with the position that all legislation is bad. I think that -- first, I did want to start off with the question of free speech and what is spam.

If the speech is not commercial, it's not spam. If it is sent to existing customers, then it's not spam. What we're talking about is unsolicited commercial E-mail, and as such it is commercial speech. And commercial speech enjoys the protections of the First Amendment insofar as it is not deceptive. So that's what we were discussing before, the deceptive nature of much of the content of the advertisement as well as to what's in the package.

I think that many of the proposals that have been brought out here are very well founded and thought out. I think the idea of technology that will help to screen out unsolicited commercial E-mail messages is great. However, unless there is some sort of uniformity to the way the subject is labeled, it's going to be constantly an arms race where the messages change and then you're going to have to reconfigure your software to make it so that you can catch that new iteration of what the unsolicited commercial E-mail becomes.

And that's going to result in a position that makes it impossible for consumers to really exercise choices in technology. If you expect the consumers to exercise that level of expertise and knowledge and interest, then it's very unrealistic.

So I would think that before any sort of technology could be issued, you would need to have some sort of uniformity as to how the stuff is labeled. And I think that that also goes to the perception issue. When unsolicited commercial E-mail messages are labeled as something other than an advertisement, then it's my feeling that that is something that is actually unacceptable.

The other topic that was brought up here was self-regulation. Sanford Wallace and the Internet Marketing Association, which is represented here, maintain that they represent 90 percent of the people that are engaged in the business of sending unsolicited commercial E-mail. I find that to be very unrealistic.

The barriers to entry in this market are extremely low, unheard of. I mean, the idea that for $11 you can purchase a million E-mail messages and for $19 you can get a month's worth of access. And for a few hundred dollars you can buy an old computer that would be capable of sending out the stuff.

And so that means that it's very unrealistic to expect that the -- that, you know, there are going to be major players in this industry that will control the industry itself and, therefore, be subject to self-regulation.

I think that the ideas that have been proposed and, once again -- although I'm here on behalf of the state and also as a representative of the National Association of Attorneys General -- I, in general, represent my opinions and not necessarily theirs.

The standard and code of ethics that were proposed by the Internet E-mail Marketing Council to me seem very reasonable, just as the idea of self -- of the technology seems very reasonable. But the application seems -- it seems to me unrealistic to expect that these guides can be adhered to. And, so, what our bill did, the bill that was proposed by the Attorney General of New York and it has been adopted, you know, it's been introduced in both the State Senate and the House of Representatives -- the assembly, I'm sorry, in New York.

It helps implement a self-regulatory -- I'm sorry, it helps implement the standard of codes and ethics. It's very similar to this, but it applies it to everybody, not just to those who volunteer. It helps promote the growth of technology that will screen out unsolicited commercial E-mail for people that don't want to receive it, because it would provide for a uniformity, which would allow greater -- a greater ability to screen this stuff out.

And it also helps to address the deception issue, because it requires the real identity and address of the person who is sending it as well as information about how you can avoid receiving such messages in the future. The problem is obvious: It is that you still have to receive the first initial message and respond to it before you can avoid receiving further messages. And in that I would very much encourage the idea of global opt-out lists that would exist for consumers to join.

There are many problems with any sort of solution, but I think that the ideas that have been proposed that in a sense would take place through self-regulation and technology would be much more successful if there were some sort of baseline standard that was established through some reasonable and narrowly targeted legislation.

MR. MEDINE: Why don't we open it up to including people's views on the various legislative proposals that have been put out on the table to see if they endorse them, have concerns about them, answer questions, maybe the ISPs -- can it solve the consumers' problem but not ISPs' problem?

MR. NEMEYER: Yes, I would say that's true. Right now the Internet Service Providers Consortium supports the Smith approach, which basically stops unsolicited E-mail based on the extension of the Junk Fax Law, basically enforcing an opt-in approach.

The problem that we see in a labeling approach is multiple. One is, technically it causes perturbations in the way mail operates. You've got to get in and actually deal with it at a system level in order to be able to trap it and so forth. And exactly how this is done can be either efficient or inefficient depending on technical factors and when you -- honestly when you get into legislating those kinds of things in a vacuum, as it were, without talking to the technical community, you run the risk of coming up with some schemes that don't work.

I would recommend that folks that are looking at legislative approaches like that, at least bring in technical folks like the Internet Engineering Task Force, to be able to assess the impact of those. Additionally, the cost that it would put on the receiving end is a problem.

From Senator Murkowski's bill's standpoint, it's the same issue, it's an unfunded mandate on the receiving end to implement filters. It puts reporting requirements on the receiving end to respond to complaints and provide the -- whatever the FTC or the FCC or whoever would be the ultimate designated enforcer, to respond to that within X hours.

That becomes an administrative burden on the receiving end. Again, my thrust would be, please, in any of these considerations, let's put the onus where it needs to be -- on the guy that's trying to stuff the stuff into your mailbox and not on the unwilling recipient.

MR. MEDINE: Jill?

MS. LESSER: I can say at this time AOL is sort of looking at a couple of different approaches. First is that we are extremely uncomfortable with approaches that focus on banning a particular kind of speech, whether it's a ban on unsolicited commercial E-mail or coming up with a labeling function. And that is because we have seen, as people have mentioned, through the Communications Decency Act and through traveling around the world and seeing what other governments are doing globally, that single government-based regulation in this area focused on content, and the flow of content over the Internet, is extremely dangerous and it is one that I think we are more concerned about really globally.

So that in this country, if the U.S. government decides that commercially unsolicited E-mail is particularly egregious, it is very inconsistent to then look at the German Government, who focuses on hate speech and say, Well, yeah but, you know, that kind of speech is actually, you know, protected by the First Amendment. Of course, we'd say we think it is irrelevant.

So, we -- our initial reaction is that legislation that focuses on speech is not the best road to go down initially, particular because we are, I think, at the beginning phase of trying to deal with this.

The two ways we would like to focus on at least now are number one continuing to look for technological approaches, and I think that the suggestions that Commissioner Varney has brought up and you as well, David, about getting together and working with the community -- despite the fact that we have often fought with members of this community -- is a productive suggestion because we do not know, since we are not talking at this point, whether there are ideas that we have not yet come up with where we can all cooperatively work.

I think we have worked with Senator Torrecelli in looking at his approach, which I think from our perspective, is number one, not perfect, but what it does do is focus on some of the things I talked about earlier, which is fraud on the system. Some of which may be an extension of or actually an explanation of frankly pre-existing FTC authority. And some of that authority may not yet exist because or -- it may exist, but you folks have not focused particularly from an enforcement point of view on the Internet.

The one thing that is not in any of these bills that I would just like to bring up and one thing that I can say that AOL has not necessarily -- doesn't necessarily endorse but is something that I think should be talked about, and that is the notion of the degree of the sanction for fraudulent behavior, whether it should be criminal or very serious civil penalties because what we really need here and what we heard earlier is an economic deterrent where some sort of a serious deterrent, so if it's criminal penalties under pre-existing laws or very, very significant civil penalties, that takes one really egregious spammer if you will, and says you are going to be an example.

And maybe it's more than one, maybe it's two or maybe it's five, but I think that that kind of an investment is an investment that you will see deterring at least some of this behavior because I do not think that these are all bad people out there. I think that what, you know, exactly what Ron said, small business people who say, Gee, there are low barriers to entry, I can finally make money pretty easily, I am selling a legitimate product -- let's assume there is a subset of people who are indeed selling legitimate products -- and -- and it looks like they're great opportunities. So, I think we have to -- we have to figure out all of those elements.

COMMISSIONER VARNEY: But if you all are going to talk amongst yourself for the next few months and come back to us with some ideas, on the very long list of things that you're going to talk about, there are two things that I think might be helpful: One is exactly what Ron talked about that you've got all of these small entrepreneurs who aren't necessarily consciously evading ethical standards. How are you going to reach -- how can we reach them?

The other thing, Jill, is that I don't know -- maybe, David, we need some kind of technical assistance here, because I think we would be very interested in aggressively going after the most egregious fraudsters in the E-mail space. But I think part of the problem, as I understand it, is we can't find them. So I think we need some help on figuring out how we can move very quickly into getting the people that are perpetrating the worse kind of the problems.

MR. MEDINE: Folks at this table who want to volunteer their help in helping us catch the bad guys, we would very much appreciate your help.

MR. RINES: That's one of the reason why self-regulation is such an important part of this process, because those of us involved in -- in self-regulatory efforts do have the resources. Most of these people are our customers. Even the ones who admittedly are the rogue element are our customers. And so we do know who they are and it serves, definitely, everyone's interest to have a self-regulatory environment in which we have the opportunity to police this stuff and help ourselves.

COMMISSIONER VARNEY: And I think what we need to do in looking at NAAG is the FTC and NAAG may need to set up a special working group who can work exactly at this issue. Because you know some states have a very different ability to sanction behavior, and depending on where the behavior -- obviously those states also have perpetrators -- we can certainly work with a couple of states and we have on a lot of issues on fraud in the past. And by state, federal through both sting efforts and then enforcement effort. And so I think that's maybe something we want to bring up in the next session.

MR. NEMEYER: Let me emphasize from the standpoint of the providers to touch on something. We also don't believe in trying to curb speech, but we do look at what's going on now as a behavior. It's a behavior that's destructive to the network and as far as the ISPC is concerned, we would welcome an FTC investigation into exactly all that is going on and what's behind it and how it operates and putting a stop to it.

MR. WENGER: If I could just quickly address the issue of free speech. This test -- I mean this issue has been put to the test with the Junk Fax Law and the Ninth Circuit found that the cost shifting was a reasonable reason for -- a rationale reason for the Congress to try to legislate in that area, and found that the law was Constitutional.

So I think that from a straight Constitutional point of view, it would be permissible to -- to have a law that banned unsolicited commercial E-mail. Do I think that's the best approach? Personally I do not and the reason that we looked at other approaches was because of -- of the power of the technology to screen out unsolicited commercial E-mail and to empower consumers to make these kinds of decisions and that's why we felt that legislating some basic standards about the information that would be included would help facilitate the development of technology.

MR. EVERETT: And I think those of us who support the Smith bill would really like to see if there could be a way to address the cost shifting element without addressing a flavor or variety of speech. I think that would be ideal. It's been very difficult for us to do that. I've had some preliminary discussions with folks like Cybercash about some payment transfer method or bulk E-mail postage stamp concept which is technically available now that might provide a non-speech-limiting method, but the cost shifting element really must be addressed.

MR. MEDINE: Deirdre for just a few quick comments, and then we'll come back and close out the session, but

Deirdre first.

MS. MULLIGAN: I'm actually very happy to hear Raymond say that he's interested in looking at an approach that will focus on cost shifting rather than speech, because I think it's been very problematic for some of us who care very deeply about this issue, both how to keep the Internet viable, how do we maximize the First Amendment and privacy in a useful way.

To be in the position where I can say I think there are some approaches out there that raise some serious questions. Like Jill said, I am most comfortable with the position the Torrecelli bill has started, but part of that is because it hasn't tried to come up with the complete solution yet. And so its strength is also its weakness.

And what I would like to say is I would very much like to sit down with all of you and try to figure out how we address it both in the standard dealing with the fraud issues and in a more proactive way because I think that is what we've seen the Internet is uniquely able to do. And I would, you know, like to accept your challenge and hope that other people will too and set up a process by which we can all sit down and come back in some timeframe that you set up and hopefully have some answers or at least be closer to one.

MR. WIENTZEN: We would certainly welcome the participation and I think the Commissioner's got a great idea. I think we can look today -- look back at today as the beginning of a major part of the solution if not the solution. I think clearly it's too early for legislation, I think that some of the technical solutions that have been discussed today will evolve. But beyond that I think that just having the participation of some of the individuals who are involved, I certainly commend the Commission for making that happen today. That's what's going to make this a solvable problem and preserve the medium for commerce in the future.

MR. MEDINE: Maybe that's a good note to end on, which is a good chance for us all to come back and resolve this issue.

COMMISSIONER VARNEY: Before everybody breaks up, I just want to say one thing: I think that it took a tremendous amount of courage and commitment for the commercial E-mailers who are here to come, because there's been a lot of criticism of them and a lot of criticism of their industry. The fact that they are here and that they have evidenced a commitment to work with everybody at this table, I want to echo what Bob said, it represents a fundamental shift in this paradigm and I know you guys are going to come back here and you're going to have at least the beginnings of so worked out. So we salute you and we thank you and good day to you.

MR. MEDINE: I want again to thank Martha Landesberg and Lisa Rosenthal for really helping put this sesthis together. This concludes session two of our workshop, and at 1:45 session three will begin.   (Applause.)

(Whereupon, there was a pause in the proceedings at 12:40 for lunch.)

SESSION THREE: CHILDREN'S ONLINE PRIVACY

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

Lee Peeler, Associate Director, Division of Advertising Practices

Commissioner Steiger

Commissioner Starek

Commissioner Varney

Toby Levin, Attorney

Michelle Rusk, Attorney

Caroline Curtin, Attorney

Jodie Bernstein, Director, Bureau of Consumer Protection

AFTERNOON SESSION

(1:50 p.m.)

SESSION THREE: CHILDREN'S ONLINE PRIVACY

PANEL I: PARENTS' PERCEPTIONS AND ATTITUDES ON ONLINE INFORMATION COLLECTION FROM CHILDREN

"Reports on various surveys of parents' and children's attitudes and preferences about information collection from children."

Panel 1A: Representative National Society

Alan Westin, Editor and Published, Privacy and American Business

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

Stanley B. Greenberg, Greenberg Research Inc.

Sharon Strover, Director, Texas Telecommunications Policy Institute, University of Texas at Austin.

Charlotte Baker, Director of Education Services, Consumers Union

***

MR. PEELER: Good afternoon. I would like to welcome everyone to today's third and final session. This session will focus on children's online privacy and we'll begin the session with opening remarks from Commissioner Janet Steiger.

COMMISSIONER STEIGER: Good afternoon and thank you all for being here. This afternoon we're going to focus on the special concerns raised by the collection and use of information about children online. The question of how to protect the privacy of children in cyberspace is a complex one, but it's clearly important for this agency to examine.

The Internet is both a valuable educational instrument and a powerful marketing tool. Through this medium children can find instant and infinite resources for homework assignments, take virtual tours of the world's museums and communicate with other children anywhere in the world. It's estimated that in the next few years there will be 10 million children online and that children will soon be spending more time surfing the Net than they will be watching television. Our challenge is to ensure that children are protected from deceptive and unfair practices on the Internet.

This isn't the first time that the Commission has addressed this subject. Our June 5, 1996 workshop examined the collection and use of children's information on the Internet. One year later we continue our examination of this subject with many areas of consensus already defined and much more information to fill in the gaps of our understanding. Yesterday morning Dr. Alan Westin gave us the preliminary results of his survey noting that there are over 14 million Net parents and that between 50 and 97 percent of those parents say they don't find it acceptable for business to collect information on children for statistical purposes, for product improvement or even for internal company use. And, Doctor, we look forward this afternoon to hearing a more detailed analysis of those results.

There seems to be a consensus that information collection from children raises special concerns, that there is a need for some degree of notice to parents of a Web site's privacy policies, and that parents must be given some measure of control over the collection of information from their children and its subsequent use. The task for the rest of today, on into tomorrow morning, is to attempt to identify what combination of technology, self-regulation, consumer education, and law enforcement will provide the best solution to children's privacy concerns.

This afternoon we have a very exciting agenda. We're going to hear presentations and the results of a number of surveys and focus group studies that will give us extremely valuable information about what parents and children know about the collection and use of information online and what it is that they want. We'll also hear from the FBI and the Department of Justice about the most terrifying aspect of this issue, the use of children's information online by child predators.

Two other panels this afternoon will be devoted to reviewing the current state of information collection practices on the children's Web sites.

I would like to take this opportunity on behalf of the Commission to thank CME, the Center for Media Education, for their valuable efforts in bringing a number of practices to our attention during the past year. And also to thank those industry members who have been willing to come here today and engage in an informative discussion of their policies and practices regarding privacy.

Thank you and, Lee, on to you.

MR. PEELER: Thank you, Commissioner Steiger.

Our first panel today is going to focus on surveys of parents' and children's attitudes and perceptions about information collection online. The research, of course, regarding these perceptions is very important to the Commission in its general analysis of these issues, and we're particularly happy to have that. Our first presenter today is Dr. Alan Westin, who is returning for his second stint in Privacy Week. Professor Westin is Professor Emeritus of Public Law and Government at Columbia University, where he has taught for the past 37 years. He presented his survey findings about general online privacy yesterday, and today he's going to report his findings regarding consumers' views on the collection of information from children. To our knowledge, this is the first such survey that's ever been conducted, and such research, as I said before, will represent an important part of our analysis here. Dr. Westin.

DR. WESTIN: Thank you. As Lee mentioned, this is, as far as I know, the first representative national survey statistically valid that gives us a picture of what 14 million parents who say they have children 16 years of age and younger surfing the Net think about all of the critical issues involved in collection of information about children.

Just to give you the statistics about the statistics, this was a 25 minute telephone survey done by Louis Harris and Associates, who served as the academic advisor, of 1,009 adults 18 years of age and older, who say that they use a computer at home, school, work, library or other place, and represents approximately 100 million adults who are the computer users in the United States, and that was our base sample. We had four sub-samples for analysis. Forty-two million of the computer users say that they are on the Net at least once a month, 33 million say they are using online services, 49 million of the computer users are not yet either online or using Web sites, and 14 million parents told us that they had children under 16 using the Net.

We started by focusing on whether parents and the whole sample saw the collection of information about children online as being dramatically different, significantly different, from the collection of information traditionally in the off-line environment. Let me read you our question so you can hear exactly the way we put it.

"Many advertisers collect personal information from children for marketing purposes through sources like comic books, magazines and kids clubs. Do you think there is or is not a significant difference between collecting information that way and collecting similar information from children using the Internet?"

And just to be extra careful, we split the sample in half and asked that question of half the sample before we went into 12 questions that dealt with children's privacy, and then we asked the other half of the sample the same question after they had been led through and obviously to some extent imprinted by the questions that were put to them about children's privacy issues.

It turns out that the sample, the total sample, split about equally. There were 46 percent of the total samples that thought there was a significant difference between online information collection about children, 45 percent thought there was not a significant difference, and 9 percent were not sure, and between the persons who were asked the question before all the other children's privacy questions and those that were asked afterwards, there was only a two percentage point difference. So, it really tells us there was a stability of viewpoint that came through and that the asking of the specifics about children did not create a major difference in terms of the attitudes people have on that issue.

What I thought was a kind of interesting and high figure, three quarters of the parents of children on the Net, 73 percent, said they were aware of what sites their children visit. Perhaps they felt that a dutiful parent should answer that way and there may have been some skewing effect of people not willing to be heard to admit the fact that they didn't know what the children were doing, but when asked, at least three quarters of the sample said that they were aware of the site visiting that children were doing.

The survey asked respondents a really key question about marketing and children's information collection, a question which asked them to assume that an Internet company that was advertising or promoting products for children collected information from children in one of four ways that we were going to indicate and it would be used only for the purpose that we asked about. When I give you these figures, therefore, my own sense is that if we had not put that in, if we hadn't said please assume that it would be used only for that purpose, we would have gotten even higher negative readings from people because of what I'll go into, the lack of confidence that the respondents who were Net parents have in companies that are operating on the Internet.

Sixty-four percent of Net parents say it is not acceptable to ask children to provide their E-mail names to gather statistics on how many children visit a site and what they do there. Fifty-six percent of Net parents say it's not acceptable to ask children to provide their E-mail name along with their interest and activities in order to gather information on product improvement. Those two again surprised me. In both cases, the assumption is that the uses were only statistical or product improvement, no judgments about children, no circulation of information with any identity outside the collecting organization -- I'll come back to that in just a minute.

The third use we asked about, 72 percent of Net parents said it is not acceptable to ask children to provide their real names and addresses when they purchase products or register to use a site and use this information only within that company.

Finally, a whopping 97 percent of parents say it is not acceptable to ask children to provide their real names and addresses when they purchase products on a registered use site and then rent or sell those names to other companies.

So, you have majorities, at the low end 56 percent and high end 97 percent, of Net parents rejecting all of the kinds of marketing using collection of children's information, the obvious question is what explains that since that is not the pattern you normally get when you deal with off-line advertising activities. My guess is even if we had asked that about children, we wouldn't have gotten that kind of figure.

I think the central finding of our survey is that this is directly related to a lack of confidence on the part of Net parents, as with the whole sample of computer users, in the way in which online companies are seen to collect and use information.

The way we tested that is that we gave a list of 10 industries to respondents and asked them how much trust they had in each one of those industries to use the personal information they collect about their customers in a proper manner. And both Net parents and the whole group of computer users, 77 to 80 percent, reported high to medium confidence in employers, hospitals and banks.

On the other hand, when asked about how online service providers, direct Internet providers and companies marketing on the Net were trusted, we dropped down to between 40 percent and 48 percent, and as far as Net parents are concerned, they drop down even further. Only 31 percent of Net parents say they have confidence in companies offering products on the Internet. That put them below, in terms of trust, direct marketers in the off-line world and credit reporting agencies. We didn't ask about members of Congress or used car salesmen, but my guess is there would have been a stellar capacity for the Net companies even there.

We asked another question dealing with the confidence level. All respondents were asked how confident they would be that companies that stated on their computer screen how they would use the personal information collected from children who visited their sites would follow the policies that they officially put on the screen. Seventy-five percent of all computer users said they would not be confident, and that percentage went up to 82 percent of Net parents who said they would not be confident that companies marketing -- collecting children's information would follow the policy they declared.

We then turned to how much parents knew and were willing to use the new technology tools by which parents could control what kind of information their children gave or what kind of sites they visited. A majority of the parents, 55 percent, said they were aware of software programs that enable them to limit the Web sites their children can visit and the personal information that their children can provide on the Internet. That's about 7.7 million parents, and I think it's a pretty high figure given general levels of knowledge about things, technological or public affairs in our country, and so on.

However, when we asked how many of the parents that were aware of this kind of software program were using them today, only one in four parents said that they were using such software at the present time. That's the kind of a half-full/half-empty glass situation, it seems to me. It represents approximately two million Net parents and given the recency of the development of the filtering and control of software, the fact that two million parents -- people who we know barely can program their VCRs -- are saying that they're using filtering and control software, can be seen as a very important and interesting move into parental control through this technological tool. If one assumes that growth has been taking place really across two years and parents, if they were interested, would have many, many more alternatives and a lot of experience, you can view that hopefully.

I think one statistic that we collected should lead you more or less to adopt that conclusion. Eighty-five percent of all of the 14 million parents represented in the survey said that they would use such software to control what their children see or do on the Internet, if the software were inexpensive and easy to use.

So, while one always has to be careful asking in a survey about interest of people in buying a product or using a service, if you compare the intensity of concern on the part of the parents with the way information is being collected about their children, with their readiness to use these filtering and control technologies, it seems to me you have a very, very clear indicator that the great majority of the Net parents would be interested and are interested in that kind of technique to empower themselves to set the parameters of whether their children give up this information and what information is collected about them.

When you turn to what it is that Net parents would like to see happen, 96 percent of parents said that companies collecting information from children should be made legally liable for violations of their stated policy, and this coincides with the discussions here about the potential jurisdiction of the Federal Trade Commission over organizations that state policies as to their information collection and use, and then violate those policies. And incidentally, 94 percent of all computer users have the same view, so you have two very high numbers. In this case, parents are even two percent higher than all the rest of computer users.

When it comes to general choice as to whether government should pass laws now dealing with the collection of information on the Internet or whether this should be left to voluntary groups, it's interesting that Net parents even though they were obviously quite intense in their concerns about the collection of information about children, were lower than the rest of the sample in terms of their attitude on government passing laws now. Fifty-three percent of Net parents believe that governments should pass laws now compared to 58 percent of the total sample. However, obviously that still represents a small majority of Net parents who feel that passing laws now is important. Let me make clear that that was not passing laws specifically about children; that was the general question about passing laws to protect the collection of personal information on the Internet.

What kind of conclusions are we to draw or think about in terms of the survey's findings? It seems to me that the heart of protecting the privacy of children and families on the Net is clearly based on all the other things in our survey. First, by every site that wants to have children participating, informing both children and parents what personal information is being collected, how it will used, and having some kind of appropriate authentication system so that parents can be identified and verified when they set the parameters and when they enroll their children, or when they have to give the specific consent for particular activities on the part of children.

Secondly, I think the survey is very clear in suggesting that parents want tools with which they themselves can monitor and control the uses that their children make of the Internet and the collection of information from their children.

Third, the way I read the confidence figures, the online industries have an uphill, but not impossible task, that is they've got to recapture the confidence of parents that the companies that are collecting information about children can be trusted to do what they say they're going to do and to carry out the kind of policies that the parents would like to see followed.

Finally, it seems to me that government needs to monitor and watch this issue very closely. But I don't myself believe that one could or should draft some kind of children's privacy protection legislation that would define which content is acceptable or not, which marketing practices are acceptable or not. I think we have to try to understand and give the parents the choices that technology tools and absolute full disclosure and policy communication on the part of the companies would bring forward.

Thank you very much.

COMMISSIONER STEIGER: Doctor, before you leave, as you yourself said, some of the percentages here are, to put it mildly, surprising. They are very high. It's unusual, I think, to find unanimity or near unanimity on any questions on a survey.

Could you just detail a little bit for us your level of statistical confidence in the results since people always ask that question.

MR. WESTIN: Sure. Nobody from the Louis Harris organization is here and they're the real experts, but what I know is this, that in a sample of about 1,000 respondents you generally would have a confidence factor of plus or minus three percent. What that says to me, of course, is if this were an electoral survey and you could have somebody elected president by half a percent or one percent, you've got to be very nervous about your confidence factor. But when you're dealing here in 97 percent of the respondents saying something and 73 percent of the respondents saying something, that kind of confidence really allows one to put a lot of weight on that kind of very high, very unidirectional finding.

Also, I didn't go into the demographics, but there are a lot of factual opinions in the full report of our survey about how parents divide by education, by income, by region, all the kind of things that are interesting, plus how parents, when you get to some of our factors like concern about privacy or general distrust of government or fear of technology, you get some very interesting patterns, but I didn't go into those here.

MR. PEELER: Ms. Varney.

COMMISSIONER VARNEY: One of the things that I wanted to comment on is that one statistic that 97 percent of Net parents say that it is not acceptable to sell kids' names, but 53 percent of Net parents say the government shouldn't pass laws, and you pointed out -- you didn't specify whether or not they should pass children's laws.

In light of the 97 percent that say under -- I'm paraphrasing, under no circumstances should you sell kids' names -- two questions, did you guys think about asking the regulatory question a slightly different way and that is, should the government regulate children's issues? And is there any correlation there between 97 percent identifying one practice as completely unacceptable?

MR. WESTIN: Yes, but we had this problem -- we had a 25-minute survey, which is already pushing respondents' forbearance to stay on the phone, so our dilemma was there was so much to ask about it and so many facets that we had to hunker down on the things that were key. We would like to do another survey for you in the next year in which we would like to go into these issues in much greater detail where we could spell out what kind of regulatory or legislative approaches might be favored or not and what will have progressed obviously in one year of more technology, more industry guidelines, more things that could be seen as potentially affecting the confidence level on the part of the public.

I really couldn't speculate on how more specific legislative presentations to respondents would come out because you've got a lot of variables -- state or federal legislation, who regulates? Is it a criminal offense to sell children's information to a third party? Et cetera.

COMMISSIONER VARNEY: Can you comment at all -- I mean I've never seen a survey where 97 percent of the people agreed.

MR. WESTIN: It's very high and I think that what it must have tapped was, as Stanley Greenberg said yesterday, there's a great deal of fear on the part of parents about the safety of their children, about what their children can be exposed to that can be distorted or skewing to young children. That must have been triggered by that question, it seems to me. If all of the harm was that the children might get another E-mail message that said come to X's kids' club and have fun, I don't think we'd get 97 percent, so I think that just thinking about all the survey research and the attitude, that must have tapped some very deep-seated sense that children are in the kind of peril that we've been talking about.

COMMISSIONER VARNEY: Thanks.

COMMISSIONER STEIGER: Do you know, Doctor, how difficult it was to get your sample? We have heard in many other surveys that it's sometimes extremely difficult, especially if people are told this is a 25-minute process.

MR. WESTIN: You don't tell them that in advance.

COMMISSIONER VARNEY: Not full disclosure?

COMMISSIONER STEIGER: We might talk about disclosure.

MR. WESTIN: If I may, let me just explain that. We have 20 years of doing privacy surveys so that we can keep people on the line longer than most other surveys because people are very interested in privacy. We've tested that and if it's about tax policy or it's even about race relations and so forth, there are more hang ups it seems, early hang-ups, than we've encountered when we ask questions that people seem to get engaged in.

COMMISSIONER STEIGER: The reason I ask that is if it was relatively easy in terms of other surveys to get your base numbers, that would indicate, at least anecdotally, that that 97 percent does speak of the sincere interest in the issue.

MR. WESTIN: Well, this was done in kind of standard national survey firm technique. It's a random digit telephone dial and we have a thousand respondents who answered the question, do you use a computer at home, school or other place and then the survey unfolds.

If you can pay the money to do the survey, you can get a good sample; and if you have a topic that's interesting, people stay with you 25 minutes. My sense is, as I said yesterday, this survey helps people who are doing self-selected surveys or online sampling to use a question or two from our survey and thereby establish how representative in attitude their sample is or to what extent their sample has characteristics that enable you to say they're more this or more that than a true national cross-section sample.

MR. PEELER: Thank you very much, Dr. Westin.

Today we're also very lucky to have not only this excellent quantitative research but also very good qualitative research, and we have three panelists to come up and join us now.

Stanley Greenberg is Chairman and Chief Executive Officer of Greenberg Research, a national survey and polling firm. He's going to talk to us today about a series of focus groups that he conducted. He will be joined on the panel by Dr. Sharon Strover who's Director of the Texas Telecommunications Policy Institute at the University of Texas at Austin. She's also midway through some qualitative work of her own. And they will also be joined by Charlotte Baecher who is the Director of Education Services for Consumers Union. She is the editor of Zillions magazine, which is mailed out to many young consumers all over the country and she's going to be talking about a survey that was done in connection with Zillions and also some work that they've done on the availability of blocking software. So, Mr. Greenberg.

MR. GREENBERG: Thank you very much, and I reiterate having been here yesterday to discuss this subject for everyone, not just children. I'm delighted to have the opportunity to be here talking about the findings of the research that we've done and also to reflect a bit on the findings that Dr. Westin has presented in this important and timely study of attitudes on privacy on the Internet, particularly with regard to children.

I do want to emphasize what is, I think, the main finding of the focus group research we did, which was a series of nine focus groups about 10 people a day in a session, open-ended discussion, that was with guidelines on a range of issues. Certainly at the beginning of these discussions people talked about their lives and their families and what's happened with their children and then later on in the discussion, an open-ended discussion of the Internet and then a discussion of privacy issues.

It does not, as you appreciate since overall you're talking about 90 respondents, does not have the kind of statistical validity that a national random digit representative sample would have; and I think it's appropriate that you look both at the qualitative research and quantitative together. The quantitative I think for some sense of the scale, and the qualitative I think for a sense of the underlying dynamic that may help to explain why you get these kinds of numbers, particularly the 97 percent.

I think we're dealing with a real issue. I think the Commission is right to explore this subject because you are centered on an area that the American people are quite worried about.

It is situated in a broader set of worries as I indicated yesterday. This doesn't start with the Internet, it starts with the family. It starts with the fact people believe the family is in trouble. They believe that the country is experiencing moral decline, that the children don't learn right and wrong and aren't guided by the kinds of values that they ought to be. The traditional concerns that parents expressed to their children in my day about not talking to strangers takes on a different meaning when you meet strangers in so many different settings and when the family itself lacks the kind of stability that it had in an earlier period. So people are worried about their families, they're worried about their kids, they're worried about the bad influences they will experience.

When they face the Internet, the reaction to the Internet is, in our focus groups, strongly negative, particularly with parents, particularly with non-college graduate parents. It's actually stronger with parents whose kids are not on the Net. The survey did not look to people that did not have computers. I suspect you would find that the level of concern is greater with those people who are not part of that sample, because the popular commentary on the Internet is full of stories about unibombers and terrorists and a range of quite awful things.

I was struck in our research as to how we found people responding to the Internet. Rather than responding with the kind of hopefulness and excitement and positive feeling that I have about the Internet, it does not carry over. It is mixed in with a lot of worry, a lot of anxiety about what's happening on the Net.

Just to read a few of the quotes to give you a sense of this, "It used to be all fun" -- this is from some women, mothers with children who had Internet access in Chicago -- "It used to be all fun and exciting, but then when you hear about all the pornographic and stuff on there now, it's more like oh, God, I'm going up there and I'm going to sit there with them. Don't go there. I think of perverts when I think of it."

Another woman -- "There should be some control over it. You think about people on the Internet they were showing how to make bombs when there was that Unabomber thing. Kids don't need to know those things."

So we come to this issue, as I said yesterday, we come to this issue through the privacy issue, and we come to this within a specific framework in these discussions and hearings which is around corporate practices and privacy. Parents who come to this issue don't operate in those kinds of compartments. They're coming with a genuine concern as parents into an environment which is uncertain to them and some say unknown to them in which they have read many, many stories about the awful things that people can encounter.

So, when they look at what they want to get under control, the areas they look at initially -- and I don't say this with any sense that one should discount the importance of what you're looking at -- but the first concern is the problem of indecent material and kids being exposed to indecent material, and then the worry about being exposed to people on the Internet who will pose dangers to their children, and then they worry about children passing out information that exposes the family and the home to some kind of danger.

Further down that list of worries are companies marketing to children and collecting information, and I'm not saying it isn't a concern, but the top of my concern, the big concerns that they are focused on that have to do with those kinds of safety issues, which the focus of these discussions do not necessarily address. Again, I'm not saying you shouldn't address them. These are genuine issues, but there is enormous anxiety of most people about the Internet. It's broad ranging and it's broader than the question of marketing.

On the question of how to respond to it, there's no doubt that people are open to a regulatory response as part of how to address this issue. But that response is in the context of help -- responsive people saying give me tools, show me, solve this problem. My family shouldn't be subjected to these kinds of dangers. There ought to be some orders, there ought to be some rules, there ought to be limits, there ought to be responsibility, and the parents are calling out for, I think, a variety of changes that will protect their children.

I'm struck by the finding in Dr. Westin's survey, the Harris survey, which shows 53 percent support, which is a small majority, for a legal response to the problem given the scale of worry which I think is real and given the very large number, unanimous number of people saying that data collection on children should not take place. And I think there are a number of reasons for that. And I think it has to do with the fact people want -- they want effective things to address the problem -- ideological -- that is, what's going to work, what's going to protect my kids.

There is an openness to a broad range of responses. I'm struck in Dr. Westin's survey on the overwhelming support, 85 percent support, and I would have thought that was high until I saw some of the others -- but 85 percent would be likely to use parental control software if it were available. Sixty percent saying very likely that they would use parental control software if it's available. We ought to assume this is a dynamic situation where people are learning about what are the different ways in which people can protect the family. Parental control software is coming to be known by about half the population.

Now, we presume with the aggressive activity over the next few years-- I don't know if it'll be universal, but there will be many more aware of that opportunity.

We found in our research on parental control software that there was an enormous sense of relief. In fact, in the research we did in the focus groups, and it's nice to have focus groups along saying that this is very responsive to the problems that people are facing. When we presented the parental control software, what you got from parents was a sense that, you know, thank God for making one.

Just to quote a few. From one of the fathers in Birmingham, "It makes you feel more protected. You know there's limits there. And when the kids start to try to see how much rope they have, you know, how much rope they have."

Another Birmingham mother, "I think it is wonderful because you are in control." And from another Birmingham mother, "Like when you come in and buy a computer. Now you get your Windows or whatever and it's already built in. It should be there."

"I would feel a lot more comfortable with my child on the computer with that," says another Birmingham mother. "It's good, absolutely, but it is also telling my kid that it is adding that reinforcement that it is here because there is stuff out there that is bad. "That goes along with what Mom and Dad have been telling you about what is good and bad, so it continues to build on their mind, the value."

What you're hearing there is, I think, parents saying this is helping me be a parent. This is giving me the tools to succeed to provide the protection, I can teach a lesson through this kind of research.

The reason why I think you're looking at a 53 percent and not a 97 percent technology is I think people are pragmatic; that is, I think they're looking for what works, what enables me to protect my kids, and I think they'll be responsive to the range of initiatives that may take place over the years.

MR. PEELER: Commissioner Starek?

COMMISSIONER STAREK: Thank you. Mr. Greenberg, yesterday you cautioned us to not take completely from Dr. Westin's statistical survey the idea that people wanted regulation or legislation regarding controls on the Net. And

I wonder if you would express the same kind of caution today with respect to the issues that we are discussing with regard to children's privacy on the Net.

MR. GREENBERG: First, let me say that I think people are more interested in some kind of public response in the area of children than they are in other areas. But I think the general point is still true. There is an enormous gap between the 97 percent and the 53 percent. And I think I made this caution yesterday in response to one of the other studies being offered.

When people say a practice is not acceptable, that a practice should not happen, it does not mean that they think therefore that the only way to address that is through a government regulation that bars practicing it.

They want businesses simply to stop doing it. They may want to see self-regulation by the business community, they may want to see more responsibility on the part of individuals, helping themselves, to keep themselves opting out, taking actions that stop the practice from happening. There's just a big gap between wanting something not to be a common practice and assuming that therefore the best way to do it is government regulation. I did specifically mention on the finding yesterday and I would repeat it today on the 53 percent with respect to the Net, is the question did come in the context of questions about people having unauthorized access to your E-mail communications. Those were the questions that preceded the question about whether there should be a law.

I think that that question is partially a response to that; and in the same survey, next page of that survey more broadly when asked whether you want a governmental response or a private sector response, not just private sector, but a good-faith effort by the private sector and a good faith effort to address the problem, they preferred the good-faith sector effort. There's no doubt people want action. I think it's much more of who takes the initial one.

COMMISSIONER VARNEY: I would like to follow up on that. Some of this 52 percent looks like a big majority.

MR. GREENBERG: We went with 49.2.

COMMISSIONER VARNEY: Stu and I were together in 1992. It seems to me though that 97 percent of the parents of the survey of Net parents believing that children's information should not be sold and then we go to those on the Net that aren't parents and then what about the rest of the country. But it does seem to me, that although they might not say if asked that their first instinct to solve the problem would be regulation, it also seems to me that if you've got 97 percent of the people saying that practice should not occur, you would probably find some level of support. And I'm asking you where you would -- some level of support for some government action saying thou shalt not sell children's information, whether it's legislation, regulation or something else.

MR. GREENBERG: I have no doubt in this area that there's openness to government regulation, but I'm not sure on the question when asked about what would you prefer, whether it's a private-sector response or the government response, when they would opt for the government sector. That's taking a leap. I'm not sure how to answer that. We don't have that specific question posed in this context. It's certainly not done in the context of other alternatives, including parental control software which gets overwhelming support in the survey and might well lead people to say, let's give the private sector a chance, let's give people themselves a chance, give them the tools and the education to get the job done.

COMMISSIONER STEIGER: I realize that this is better posed no doubt to industry experts, but what do you think would be the response to parental control tools, if you will, if there was a feeling it would slow communication or that it would in some way diminish the rapidity of the Net, the speed of the access, or do you think that really would not weigh on the minds of the parents?

MR. GREENBERG: I don't think it would weigh very heavily. We did get some response amongst the younger users of the Net, by younger -- I mean, young adult users of the Net, some of whom were parents, and they were very cautious about government getting involved in the Internet for those very reasons. But with parents the issue is achieving safety for their kids. That was a much, much, much higher priority than the speed of information transfer.

COMMISSIONER STEIGER: I should make it clear that I have no reason to say that that would be the result, but that is the typical kind of objection one gets if you are talking about additional controls on any medium that begins to depend upon speed or clarity transmission. I do want to say I'm not suggesting that that would be the result.

MR. GREENBERG: I'm coming at this from a public opinion point of view. I don't know whether it would have that effect, and I don't know what the policy position ought to be on that. What I'm saying is from the point of view of the parents. The issue is how best to achieve safety for their children. That's the primary and almost only question I think when assessing the alternative.

COMMISSIONER STEIGER: It is that strong a response?

MR. GREENBERG: That strong.

MR. PEELER: One of the things you see pretty commonly is people who answer yes to a question because they think they should answer yes to it, but when you actually look at the behavior they don't respond that way. And I guess the question I have for you is, isn't that also a possible explanation for why 85 percent say they would use it if it was available but only 27 percent use it?

MR. GREENBERG: Well, there's no doubt in surveys people probably overstate their intentions. And they are probably overstating their use of the parental control software and probably overstate their intention to use it because they think they ought to use it. But for a variety it is not because they are simply lying to a caller on the phone. It is also because it requires time and effort and commitment that they're not sure they'll be able to do when it comes to the real world, but they would clearly like to be able do it and I think that's reflected in their response.

COMMISSIONER VARNEY: This might not be a public opinion, but it sounds like one, an anecdotal comment you read that when you turn on your computer you've already got Windows there, I think they should put this kind of a thing there also. It might go exactly to that point. We all know that there are several companies out there now selling various versions of blocking software, different kinds of protective software. I think the question goes to the ease with which it can be used, and I'm not sure that the people who are probably most sufficient and prolific at finding the software, downloading it or buying it and installing it and setting all the preferences and who are probably 18 or 19 have the worries yet about their kids. You want to comment on that, Stan?

MR. PEELER: Tomorrow morning at 10:00.

DR. STROVER: I know Texas had legislation that it was considering and I thought it passed that would have required all Internet service providers to post a link -- a hot link to filter into where they can learn more about filtering software. So, there may be some other states that are doing that as well.

I have some black and white slides.

Thanks very much for inviting me to share some of our very preliminary data. I would like to underscore what Mr. Greenberg said about focus groups. They're not based on generalizable samples, small samples. What I am going to talk about today is preliminary findings based on our work. We're still in process. We just started this project in February. It has four components. I'm only going to talk about two of those components today.

First, a content analysis of some children's sites and then secondly, I'll talk about what some of the parents that we spoke with said about their children's use of the Internet. The sample that we're working with is a little bit different from any of the samples that we've heard from so far in that we dealt with parents whose children are using computers at home to access the Internet.

Basically then if I can turn to the Internet site content portion of the study. We have in our sample right now some 84 sites, 51 of which are .COM sites. Those are the sites I'm going to be talking about today.

We coded for a lot of things -- I'm not going to talk about everything today, but we coded for: targeting a parent; target age range, not every site identifies the target age range; the presence of cookies; advertising; the source of information that either might be required or requested by the site, and under what conditions that information might be requested; whether or not the site presents links to other people or links to other sites; whether or not there are clear policy or privacy -- or both -- guidelines; safety tips; and then whether or not these sites have chat rooms.

What we found in our site analysis is that 39 percent of our sites did in fact have advertising. We weren't counting those sites that had strictly self-promotional advertising. Sometimes that's a real judgment call because a lot of the .COM sites are self-promotional. One page of Disney is going to send you to all the Disney products. We didn't code that sort of advertising. So, in any case, we found that 39 percent had advertising of other sorts.

Most sites did not have warnings about ads and that becomes an issue for young children who can't tell the difference between an ad and what is content. I think there will be a presentation later on that's going to present one type of solution to that. But we found that most of the sites did not have any warnings at all.

Twenty percent posted policy guidelines or some sort of usage guidelines. However, in most of those sites, the language was not the kind of language that children would read or perhaps understand. Eighteen percent offered explicit safety tips, but some of these sites had language more directed to parents than to kids. That's not always a bad thing because as I'll mention a little bit later on for younger children oftentimes it would appear that parents are at the site with the child.

We found that about a quarter of the sites that we looked at used cookies, and then 39 percent, almost 40 percent, either requested or required some sort of personal information from the child. These were often presented in the context of giving the child access to chat rooms or Bulletin Board Systems ("BBSs"). Chat rooms were most common for sites that seem to be targeting teenagers, while bulletin board systems were more common for sites for young children and it did seem to be the case that these BBSs often were monitored or screened for the younger children. The most common information requested would be E-mail and name.

Obviously E-mail if they're going to be engaged in live chat. Often times, the BBS would post maybe a first name and perhaps an E-mail address.

In conclusion, we saw a fair amount of sites with ads. I would say generally the ads were more commonly found in sites that had larger, recognizable corporate sponsors. Privacy notices rarely appeared in children's languages. There weren't that many safety tips available, and 40 percent requested explicit information from children. That led us to wonder whether or not the parents knew that their children were being asked this specific information.

If I could turn now to what some of the parents told us about their children's use of the Internet at home. I think it's necessary first of all to contextualize how children are actually using computers to access the Internet at home. This was kind of a surprising thing to us and we hadn't really given much thought to the actual context of children's use.

First of all, children are usually using their parents' computers. They're often using their parents' E-mail accounts, as well. We're not at the stage yet, if we ever will be -- I suspect we will be -- where we have multiple computer households. There's still usually one computer in the household and everybody in the household has to use that computer.

The home setting -- in the sense that there's one computer that the parents are using and the children are using as well-- that home setting actually helps the parents monitor what the children are doing because they get on the computer themselves.

In fact, they often go in and if the kids are using their E-mail account, which we found was the most common way for children to be using the mail, they will read their children's E-mail. They also will often be in the same room where the child is using the computer. And we found that the equipment was often older and very limited in capacity, so a lot of things I think we take for granted -- all the plug-ins, all the JAVA scripts, most people don't have computers that can do that -- and the children aren't quite yet at a stage where they're exposed to the coming generation of ads.

We also have found that parents put themselves in a position to monitor what children were doing as well because many of them only had a single phone line and when kids were on the Internet, they were acutely aware that they could not get them off. It's a very practical consideration.

Consequently, because of this context, most of the parents said they thought they knew what their kids were doing on the Internet at home. Many of them said that they had come and peeked over their children's shoulders when they were on the Internet. Moreover, there was a real age difference in what parents did with their children when they were on the Internet. Younger kids really needed some help with the Internet. They might not be able to type very well. They certainly aren't able to spell very well, and they might not be able to maneuver very well. So younger children usually had their parents sitting with them as they maneuvered around the Internet.

The second thing that we found is that the parents really didn't believe their children had any privacy rights with respect to what they, the parents, should know about their Internet use. They felt this very, very strongly. I don't know if that's a Texas bias or not, but they thought they had a right to look in their kid's E-mail. They thought they had a right to go in and examine the chat files and they did; and frankly, simply in terms of hard drive maintenance, they had to go in and get rid of files routinely. So they thought they really had a handle on what their children were doing.

We found overwhelmingly that parents were more worried about their children's exposure to indecent content, as well as to the opportunities for meeting strangers, for meeting people who might exploit their children, than they were about advertising content. That said, and I'm going to underscore these comments a little later, most of the parents really weren't very aware of what data would be gathered from their children through ads. So, by and large the parents were worried about those two things and that's indeed mainly what they wanted to talk about.

Parents felt quite genuinely caught between the positive aspects of giving their children access to this wonderful tool and the negative potential that could be realized. For example, the parent of a 14-year-old boy and an 8-year-old girl said this: "I think what would help a lot is having -- I don't know, maybe these are out there and I've been oblivious to it or it just caught me off guard, but having guidelines, like, you know, a booklet or pamphlet to sit down and talk to your kids about these things, because I'm fairly computer literate and I work with computers all day and I know a lot about kids' software, but you just don't think. You think you're giving your kids this great advantage, the computer and Internet because they can do homework, they can do research and then all of a sudden the dark side creeps up on you." They really felt very torn.

One area in which they particularly registered some objections had to do with chat rooms. Now, as I said earlier, most of the chat rooms that we saw on the sites were directed to a teenage audience, and as I said before, that's where we saw most of the personal information being requested from children. Parents didn't comment so much on that as they did on the content in the chat rooms. They thought that chat rooms were a forum where children would be exposed to indecent language and also to these untoward interactions with strangers. They really registered a plea for some guidelines of how to achieve safety online. Most parents felt that they just needed to be directed toward more safety guidelines. And I think that if there's one thing that could grow out of this forum it might be that those kinds of safety guidelines appear on home pages of these sites that are targeting children.

With respect to parents' attitudes towards privacy technology, most parents are unaware of privacy technology with respect to filtering. Specifically, while they were somewhat aware of filtering software they had a lot of doubts about its efficiency. And, in fact, they took what I guess I would call the long view. They said that there are many ways in which filtering could work, but they thought that their children could defeat filtering software. And if their kids really want access to the content that a parent might legitimately block their kids from, that if their kids really wanted to get there, they would find a way, like parents getting their own experiences with National Geographic Magazine 20 or 30 years ago. So that led them to look with somewhat jaundiced eyes to the efficacy of filtering software.

They also said that in a way the Internet is very similar to other unfamiliar public places for a child, and as they've been grappling with the dangers that they feel are out there, they more or less said that the Internet is like the mall -- it's like a street corner. The Internet is a place where you have to prepare your child for these occurrences -- these interactions with strangers, and that one very good solution from their standpoint is to drive home to the children that this is what's best -- this is a place and here are some guidelines for you. That said, not many of them had had very explicit conversations with their children. Few had explicit guidelines, but they felt that their children would talk to them when something untoward or unusual happened.

Most parents were unaware of cookies. In fact, in one focus group we ended up having one parent gave a little tutorial on cookies and there was tremendous interest in it. Most parents don't want children divulging personal information beyond the E-mail address. They didn't seem to have as much hostility toward simply registering E-mail addresses as perhaps some of the statistical results suggest. That said, however, they did resent getting junk mail.

For example, when children go to MCA sites or Disney sites or something like that, they might be asked to register, and then promotional information would be pushed out. One parent in particular singled out movie ads and movie information. They didn't particularly appreciate that. But that said, I wouldn't say that this was a top-rated concern.

With respect to some of the other sites that might have responsibility for children's Internet use, the parents that we spoke to were aware that schools and libraries would bear some liability for what their children did on the Internet and they were also aware in part because there had been some front page news coverage locally of the Austin Public Library problems. They were aware that libraries and schools were in fact using filtering software. They assumed and indeed believed that schools should monitor and protect children and they were using the Internet from these public settings.

I would add anecdotally -- this is not based on our parent research work, but I think it behooves us to be aware that across the United States, schools are wiring computers for Internet access. In Texas alone we're spending about $150 million annually in what will be an eight to 10-year program to wire schools specifically for Internet access. So what schools and libraries are going to be doing with respect to children's access and privacy protections, I think is something that has to be extended to that forum and those groups. The institutions really have to be brought into this discussion.

So, in conclusion, parents are concerned about indecent content and about children meeting strangers over the Internet. The chat room and registration vulnerability suggests that some guidelines are in order. This might mean that we need to build more safety features into sites attracting children. Parents' knowledge of cookies and data-gathering practices is extremely limited. If they knew more about it, I might speculate that they might register more concern than we heard in our groups.

MR. PEELER: Thank you very much.

MS. BAECHER: I'm really happy to be here to present these survey findings, but I do want to start out and tell you that this survey was not conducted for these hearings. I'm editor of Zillions, which is a magazine for kids nine to 14, and this survey was conducted to gather information on what kids were doing and kids' experiences in cyberspace for an article that's scheduled for publication this September or October. However, some of the findings that came through in the survey I felt were important enough that they really should be considered in this dialogue for several reasons.

First of all, we heard an awful lot of data about parental concerns and what the parents are doing, but I think we really need to see what's happening at the end of the line that we're really concerned about with the kids themselves. I mean, we've all been kids ourselves -- our parents didn't know everything that was happening in our lives. And I think it's a very important area for us to look at. I also want to give a little bit of information about the survey before I talk about the findings.

The survey was conducted at the beginning of last November. It was what we call a tag-along survey. Zillions is published by Consumers Union, which also publishes Consumer Reports. And the survey research department of Consumer Reports does bimonthly surveys of our readers, and they send these surveys to a random sample of kids. Privacy is totally protected; we don't ask for names, addresses anything like that. We just ask for gender and age. And it's -- I think our survey department would be a little bit upset if we termed this qualitative. They consider it quantitative. But the sample is Zillions subscribers and not all kids in general.

Typically, kids in this age range who are magazine subscribers also tend not to be typical of the population. If anything, there would be more parental attention, they're higher educated families. So this is really a best situation that I'm talking about. But that's really just my hypothesis, but I think it will be upheld.

The survey response was over 50 percent and a little more than half of all of our respondents do go online and were online in the past before they received the survey.

The first finding and the finding that I felt was most important to bring to the attention of this hearing kind of confirms that a lot of the parents worry about what's happening to their kids online may be justified. Nearly one-third of the kids who went online experienced problems with other users. And this was done as an open end. We didn't want to put a whole list of problems and say check here, check there because kids' imaginations can be very, very active. So we just asked them, did you have any problems with other users online, and if yes, what? We just left it as an open end.

We went through every single open end and basically what we have mostly is the experiences in the words of the kids themselves. There were three general areas. There were some problems that we didn't define sorting, but there were three general areas, password stealing, profanity -- that was mostly in chat rooms -- and inappropriate advances to kids. Call it potential predators, whatever, but there were definitely approaches that it may happen to your child.

I'll give you a few examples. Twenty-nine of the 90 kids who reported problems had problems with password stealing, as well as other problems, too. And many of them actually had given up the password. One reported that, "About six months ago someone got a hold of my password and charged around $200." Another said, "I've had a big problem with people trying to get my password." Another child, "Someone got my password somehow and charged $500 in time to my account." That really was a big problem.

As far as the profanity goes, one 13-year-old girl said, "I generally hang out in Christian chat rooms because it's Christian, people come in with porno stuff and use bad language."

The inappropriate advances to kids in that area were particularly disturbing. One kid said, "I had my E-mail address visible in my profile. Someone sent me a lot of pictures of little kids naked or performing sexual acts. I got over 100 pictures! I deleted them, but it was gross!" Another 10-year-old girl said, "An older man tried to ask me on a date." A 12-year-old boy said, "One person was asking me sexual stuff about different sexes and he was also using vulgar language." But there's enough in the kids own words to say that this still is an area for concern.

And I have to say that this was really not an area that we intended to cover in Zillions magazine because we feel that for kids, it should be an upbeat experience. It's a whole new arena for them to explore, and it's not like you want to scare them or turn them off from something that really is their media of the future. And we're still kind of grappling with how to deal with this and what kind of education to give kids and what kind of suggestions we can give kids so they can actually be part of the solution.

Another finding in the survey was that kids are visiting commercial sites. About a third of the kids said that they went to commercial Web sites.

And again, I want to say that we didn't plan this survey for this particular hearing. So we didn't ask about particular kinds of things that we've been looking at, like whether they divulged personal information at these sites and whether they entered contests and whatever. We had some anecdotal things from kids and they actually view it as very positive. One kid gave all kinds of personal information, entered the speed contest and won something -- I don't know, a binder or something. It was great, it was fun. But it is definitely an area that requires a lot more study again from the kids' viewpoint -- from the kids' experience.

We also asked the kids whether there was blocking software on their computer. And then the first thing we did was take the kids who had recorded these problems and did a cross to see if the blocking software played any kind of role in keeping kids from getting -- from experiencing these kinds of problems, and there was no correlation. But we also -- when we asked them, only 20 percent of the kids reported any kind of blocking software on their computers at home. And again, this we see as a best scenario, so our assumption is that the rest of the population is probably using blocking software at a much lower percentage rate.

I find it interesting to compare this with the parental intent reflected in the opinion poll. And I think it underscores the importance of us really trying to find out what really is happening out there. I sort of question the ability of blocking software to be the major part of a solution, because there are so many variables. It's really not even just the using it, whether it's used or not and who's using it. And what about the 80-plus percent of kids whose parents are not using it?

One of the things I should mention is three quarters of the kids who were going online, were going online through an online service provider -- not just an Internet provider, but an online service provider which has lots of blocking ability available for downloading, whatever, and the rates were still just 20 percent, it's rather disturbing.

We also, this peaked our curiosity and we also did a quick market survey for a city, and we had shoppers, where you could normally shop for test samples for Consumer

Reports, go out and try and buy the blocking software, and we gave them four titles to find at 47 stores. They found them in five stores. And where they did find it, it was one kind and really very little help, very little knowledge, very little support, whatever, from the salespeople. It just definitely was not familiar, nor was it obviously in very much demand.

But I think the experience of just doing this survey, and there are many things that have come out of this. Primarily, I think when addressing online privacy protections for kids, we really are talking about a special situation and kids can't be expected to have the experience or maturity to really solve this problem themselves, to deal with it in the way that adults would hope they would. I don't know that the assumption -- it can be validated, that kids will automatically go to their parents if there's a problem. I don't know. But I don't think that we can make the assumption that they will.

I guess I would really like just to end with a real concern that we not over-estimate the ability of blocking software to solve this problem. The problems that came through in this one survey almost by accident and other areas of concern just anecdotally from kids, I think, really pushes the anecdote a little bit. I think we really have to say that because they're children that they need special protection and that the role of the Federal Trade Commission is going to have to be an active one to make sure that children are adequately protected.

MR. PEELER: Thank you, Charlotte.

COMMISSIONER VARNEY: Lee, do we have the results of this survey in our record?

MR. PEELER: Yes, we have the results.

COMMISSIONER VARNEY: Do we have the questionnaire?

MR. BAECHER: I have a copy of it.

MR. PEELER: For everyone, that is for the point David made yesterday, it's very important, especially for this type of research, to have an idea of how the questions were posed and what the environment was so we can understand it. So, if you can submit the questionnaires for the record.

COMMISSIONER VARNEY: I would be interested if anybody, but particularly the previous presenters, have any thoughts on the fact that these kids were out there and responding to the survey and really the astounding level of difficulty that they ran into and the astoundingly low percentages that had blocking technology and then the difficulty when your testers went out to buy it.

COMMISSIONER STEIGER: Before you do that, Charlotte, would you review for us the size of this survey universe, how many questionnaires were sent, and how many were actually received.

MS. BAECHER: We do this every other month. We do a random sampling of 1,200 subscribers to Zillions from our subscribers and our response rate was 53 percent.

COMMISSIONER STEIGER: That's over 600.

MS. BAECHER: Yes.

COMMISSIONER STEIGER: That response rate seems to me, for a survey, to be high.

MS. BAECHER: Yes.

COMMISSIONER STEIGER: Do you routinely get that high a response from the magazine?

MS. BAECHER: Yes, when we do our readership surveys. Basically the way we do the survey is we send a postcard. The week before we mail the survey we send a postcard to the parent telling the parent that the child is getting the survey. And we also include a $1 incentive in the survey and we tell the parent that the kid is going to get it. So they don't think the kid is making up a story when they come up with the dollar bill. And we've been getting -- yes, that's typical for us.

COMMISSIONER STEIGER: Very high -- our experts can tell us.

MS. BAECHER: But again these are children -- these are kids. They love to get mail, and it's not in the same competition as an adult survey.

MS. BERNSTEIN: And the age is seven to 14.

MS. BAECHER: Age is nine to 14.

MR. GREENBERG: Again, I just want to elaborate on a point and there appears to be consistency for all three presentations. I am not sure whether Dr. Westin's survey has a similar finding.

On the question of whether the problem of marketing to children is a problem people are conscious of, was something our group did not come up with on its own. We introduced the subject, but the subject did not come up on its own. It was not a top-of-the-line problem. What people did talk about was above all indecent material and approaches by strangers. That appears to be the most common problem here and as well the most common problem that the kids themselves report. So that there's a genuine problem. The problem of marketing to children is a subset of that which is not on the same part of the radar screen.

COMMISSIONER VARNEY: Well, I think you missed it, sir, because you weren't able to be here this morning. Part of the problem is where are these people who are making these untoward advances to these children getting their address, their E-mail address?   And when we talk about kids' privacy, it doesn't only have a marketing dimension. It does have another dimension because somewhere either these kids e-mails are getting harvested -- there's some preceding event that unless the kids have gone to a chat room and somebody else in the chat room has engaged in some unacceptable behavior, they're getting sent an E-mail, then there's a privacy concern.

DR. STROVER: I would agree. I think, first of all, the parents themselves weren't sufficiently aware of the advertising and privacy content on the Internet. As I said before, they weren't that aware of cookie. I would agree generally with your comments on what the parents were concerned about, but I think that it has to do with their knowledge base, their lack of understanding of their advertising and some of the information gathering practices that explains some of their response.

MS. BAECHER: But I would also like to add to that, I think a lot of the practices of commercial sites by asking kids for information, they get kids in the practice of divulging information in a totally non-critical way. It becomes an accepted procedure and I think that that is a real problem. I'm not saying that's the reason it's happening, but I am sure it's a contributing factor, rather than having there be a caution against -- you do not divulge personal information, it's the opposite at this point.

MR. PEELER: I want to thank all of our panelists. Your research has been very helpful. I would like to ask our second panel this afternoon to come up.

PANEL II: A REVIEW OF CHILDREN'S INFORMATION COLLECTION PRACTICES ON THE WORLD WIDE WEB

"An update on how commercial sites aimed at children collect information."

Kathryn Montgomery, President, Center for Media Education

Shelley Pasnik, Director of Children's Policy, Center for Media Education

Mary Ellen Fise, General Counsel, Consumer Federation of America

Michael Brody, American Academy of Child and Adolescent Psychiatry

***

MR. PEELER: The second panel today is one of two that's going to provide us an overview of how commercial sites are collecting information about children. A panel of representatives from the Center for Media Education and the Consumer Federation of America have reviewed the wide range of practices on children's Web sites and will be illustrating these practices with a few specific examples.

As part of this discussion, we'll also hear from an expert in psychiatry about how children respond to solicitation for personal information on the Web. And finally the Center for Media Education will provide their thoughts about the implications of this review for children's privacy. Later this afternoon, we'll hear from a panel of industry representatives who collect information from children on the Web about their company's practices and privacy policy.

Today's panelists are Kathryn Montgomery who really needs no introduction. She is the President and Founder of the Center for Media Education. She will be joined by Shelley Pasnick who is CME's director for Children's Policy. She is accompanied by Mary Ellen Fise. Mary Ellen is the General Counsel for the Consumer Federation of America. And we're also privileged to have Dr. Michael Brody, who is a practicing child psychologist and CEO at the Psychiatric Center, the District of Columbia's largest provider for the chronically mentally ill. He's appearing today as a representative of the American Academy of Child and Adolescent Psychiatry and also serves on the Board for the Center for Media Education.

MS. MONTGOMERY: I want to thank you very much, Lee. And I want to thank the Commission for taking up this issue and taking it up in a serious way. We are very gratified with the role that the Federal Trade Commission has been playing in this area. In fact two years ago I was not a participant, but I came to hear the public workshop that the FTC held and I believe that it was the first public workshop on online privacy, and at that time was looking into the issues of marketing to children on the Web. I was very interested that I did not hear that mentioned at the workshop two years ago.

We released our report documenting some of the troubled practices that we had identified in online marketing last March, March of 1996. And the purpose really was to sound an early warning signal that parents, policy makers, and the public in general needed to be aware of how this new media was developing. And we were very pleased that the industry took note of that, that the Federal Trade Commission incorporated the issue of online privacy to children or children's online privacy in last year's public workshop. We're very pleased.

We're here today to sort of assess where we are now, where things are going, and to make some recommendations. I'm only going to talk a couple of minutes and then I'm going to let my colleagues make the meat of this presentation. But I will say that from our vantage point, as we've been assessing the way this market is evolving, we can see that there have been some changes. Some companies have changed their practices in response to the concerns that we raised and that the Federal Trade Commission has raised. And certainly, I think, the individual companies that have volunteered to testify here today will tell the Commission this afternoon about how they are acting more responsibly and for the most part these companies are. I think we should be concerned, however, about the companies that have chosen to be absent from this very, very important public process.

The key point here is to assess what the overall trends are. And, as my colleagues will share with you, what we think is that in terms of overall plans, the collection of personally identifiable information from children continues unabated; and it's becoming more widespread and that there's an absence of effective safeguard.

This is a medium in its infancy and as others on the previous panel shared with you, a lot of parents don't even know what's going on. As a colleague of mine said at a recent panel I was on, this is happening under the radar of many parents. They're not aware of these emerging marketing practices.

I was at a presentation a couple of months ago at a workshop on online privacy, and several of us were making presentations to the group and in the middle of it a woman left the room and disappeared, and I didn't see her until the end. She came back at the very end and she said, "I'm sorry, I hope you all will forgive me for walking out in the middle of your presentation. But what you were talking about made me realize that I left my daughter back home in Peoria and she loves to go online and she loves to order catalogs, and I had no idea this might be happening. And so I went to the phone and I called her up and I said, `Don't do anything until I got home.'".

And I think that is the state for a lot of parents. I mean it's a medium and it's in its infancy, and we're still not fully aware of what practices are developing. Our concern is that if there are not effective interventions now, and first off we seem to have to have a major public debate about this, but if we don't have the effective interventions put in place now, at the outset, to really guide the development of this medium, then we run the risk of seeing an out-of-control marketing media develop where we could see a flood of hard sell, direct marketing by E-mail of animated products, by made-up spokes-characters coming into kids' personal computers, which they undoubtedly in the future will have in their own rooms.

We can learn from the surveys that have been shared this week that parents are deeply troubled by the intrusive nature of the online environment into their homes and the dangers that are posed to child and family privacy. They're very concerned about the serious and harmful consequences to privacy for families and children.

Last year when we met, companies promised to develop self-regulations and we have been very heartened by their acknowledgment of this as a major problem. But we found that the self-regulatory rules that have been developed are really meek and unenforceable, despite their good intentions. We're also not convinced, by any means, that the parental control software will in itself be an adequate solution in this area.

By relying on that primarily we give them a green light to market and to develop practices that step over the line of what's appropriate and what is not appropriate. I will say what I said last year, I believe in keeping to rules of the game to guide the development of this new medium. They need to be enforceable rules that ensure that children who are online are protected. And we believe that without such playing cards in place, that parents can really trust -- this could hinder the growth of the digital economy and really parents -- and prevent children and families from reaping the full benefits of the positive aspects of the digital age.

I'd like now to turn this over to my colleague, Shelley.

MR. PEELER: Shelley.

MS. PASNIK: I want to thank the Commission for addressing this important issue, and I want to commend representatives from the industry for participating. I think it's extremely important that you're here, however, perhaps more important are those who aren't here. And so I humbly offer myself as the spokesperson for those who chose not to show up today.

We have done a study, analysis of 38 individual commercial Web sites and I would like to share the findings of that analysis with you today so the subtitle of my comments will then be seven points in 10 minutes. And given that I've probably used one now it will be nine minutes.

Point number one, fully 90 percent of all Web sites that we examined actively collect personally identifiable information from children. The first example that I'd like to show and I'll draw your attention to the overhead, and keep in mind that this is a representation of our exciting and beautifully maintained Web sites online. This, however, is the newly launched Nickelodeon site and, as you'll see, they asked for information from young users.

There also in addition to this registration is a sweepstakes that asks or tells children about all the different prizes that they can win including a big screen PC/television set. So you want to enter the sweepstakes. Well, the first thing you need do is ask your parents for permission, so they do make a note of that, however, this is very rare.

After that, scroll down, it asks for first name, last name, age, gender, street address, city, state, zip code, and then the second half of the form reads, "Want more stuff to fill out? Well, you have to fill out the form to learn about the things you like so we can learn more about what you like." And they ask questions about do you have any pets or animals? Do you play any sports? Do you like to paint or draw? Do you like collecting stamps, comics, coins, et cetera? And it asks again to submit the E-mail address.

Now, if the offer or the chance to win a big screen TV hasn't peaked your interest, then you can go to a glossy online magazine and it is a site that is maintained for targeting young girls. And here is not just a chance to win the sweepstakes, but you get the promise of a glossy compact mirror. What girl wouldn't want to provide personally identifiable information to earn such a prize.

I'd like to point out though that they ask for a great deal of information, including birth dates and when you're not on the glossy site, what other girl magazines do you flip through? Which services do you use to cruise the Net? You are alive with the sound of what type of music? And the survey goes on. However, they don't include any disclosure or a legal statement discussing how this information will be used or who will have access to it.

Point number two. No site obtains verifiable parental consent before collecting personally identifiable information from children. Let me repeat that. No site, out of the 38 commercial sites that we examined, obtained verifiable parental consent from parents before collecting that information.

Point number three. Forty percent of sites use incentives such as free merchandise screen savers and sweepstakes to encourage children to release information about themselves. So again, if the compact mirror wasn't enough and a chance to win the big screen TV wasn't enough, then other companies are sweetening the deal and they're offering free candy. I'll take you to the Jelly Belly site.

Under the heading, Jelly Belly Online Highlights, the home page of the site reads, "Free Jelly Belly Survey." And they go on to explain how they give 500 samples to the first visitors at the site for that day. I'll tell you that they change the time that they offered this survey so I had to repeatedly go back to visit the site, but fortunately I was able to find the survey. And I think Jelly Belly was excited, too, as they found themselves on the cover of a very prominent newspaper earlier this week. And the survey asks everything from favorite candy that the visitor likes, have you already heard of Jelly Belly beans, would you consider purchasing special Jelly Belly bean products, and, of course, they introduced Mr. Jelly Belly, which brings me to the fourth point.

Several sites use product spokes-characters to solicit information from children. Not content to let the companies speak for themselves, they're creating relationships with these characters that are far more appealing to young people. In addition to Mr. Jelly Belly and Ronald McDonald that you can find on the Web you can also find the M&M's characters that are featured prominently on the M&M studio site. Here they've created a very active sweepstakes process that involves the gray imposter candy that can be found in special packages of M&M's candies that you can buy, so it's kind of a cross promotion that's taking place.

But they do something different. They not only ask the child to provide his or her own name and E-mail address, but that of a friend as well. The friend will then receive an unsolicited E-mail message from M&M studio featuring a wanted poster for that gray imposter, M&M.

Which brings my fifth point. One-fourth of the sites that we examined sent an E-mail message to children after their initial visit. A perfect example of this that combines both the use of a product spokes-character and E-mail message was the Colgate site. Here, children after entering the No-Cavities Clubhouse, went to visit the tooth fairy and the tooth fairy was used to by Colgate in collecting the information and asked for names to E-mail messages to submit that put my tooth under the pillow now. After visiting the site, of course, the child received an E-mail message which lovingly was signed, "Keep Smiling, Your Friend The Tooth Fairy."

Point number six. Cookies were used by 40 percent of the sites. Some sites used as many as 12 cookies during a single visit. And nowhere was cookies explained to the visitor nor to the parents.

Point number seven. A third of the sites attempted to describe how the information once collected will be used by the company maintaining the site. So many of these sites were incomplete. More commonly, sites offered no statement about information collection use.

And I would like to point out Nabisco. Their site does offer a very extensive policy statement regarding the use and the collection of children's information and they should be commended for that. However, they too still are not obtaining verifiable parental consent.

Far more common, however, were those disclaimers that either did not exist or that were very clear that the company maintains the right to do whatever they want with that information. So on the last note I provided you a statement, it's number four on Jelly Belly's top 10 rules for cyber-surfers. And let me read it.

"If you don't want the world to know something, don't post it on the site in any survey, form, bulletin board or anything -- anyplace else. That's because anything you disclose to us is ours. That's right, ours. So we can do anything we want with the stuff you post. We can reproduce it, disclose it, transmit it, publish it, broadcast it and post it someplace else. We can even send it to your mother as soon as we find her address."

So you'll see that they are very clear that these companies maintain the right to collect information from children and to do whatever they want with it.

And with that, I'm going to turn it over to Dr. Michael Brody who's going to explain why this should be so troubling.

COMMISSIONER VARNEY: Has Jelly Belly or M&M changed any practices since the Wall Street Journal?

MS. PASNIK: The tooth fairy has been changed. I haven't noted that the M&M site has been changed, nor have I noted that Ronald McDonald, which we haven't talked about, has added one line, but -- and Mary Ellen also mentioned that the Sony Wonder site which was in USA Today on Monday, they've added a statement in their terms of use. But it, too, is quite thin.

COMMISSIONER VARNEY: Okay, thanks.

MS. PASNIK: All of that is detailed in the report.

DR. BRODY: Members of the American Academy of Child and Adolescent Psychiatry, and a child psychiatrist like myself, are quite interested in a person like Dennis Rodman.

They are celebrities/role models with attitudes as they may determine who our children imitate and use these ideals. Role models are important in child development as they help with impulse control, the ability to learn and socialize. In fact, child play which is a part of the continuum on the line to work, is to a large extent adult role play.

While the child's first object of emulation may be parents, other family members, teachers and even therapists, none may be as influential or pervasive as the models offered by the media. Cyberspace with its adoptive interactive capability profoundly promotes the strong bonding with these media figures. And while my six year old may not yet relate to Dennis, comic characters like Batman or the Power Rangers are quite important in his fantasy production and ego structuring of self.

This is why an online children's culture, very much in its infancy, requires great care and sensitivity. Now, licensed comic characters have a long history beginning probably in 1904 at the St. Louis World Fair with Buster Brown selling shoes. Some of us are old enough to remember Captain Midnight on the radio promoting Ovaltine. And Howdy on TV talking about Mounds bars.

Children are now constantly bombarded with images of Hercules and Barney through various commercial context. Placed only in the most positive light, there is trust.

There is also passivity and laziness as brand name comic characters determine what a whole family will buy. That's why Ronald McDonald is so busy in a cyberspace with no child rules. With entertainment and advertising totally merged Ronald exploits children easily. But all a child knows is there's Ronald in color on his Web site interacting with us kids.

The narrators become one big infommercial for MickyD's. No one -- no one can be passive and make believe. No effort required. Like pornography, these stories have no depth. Everything is reduced to the lowest common denominator. This does not promote active thought or play which kids need for development. As research has shown that neural linkage in the brain and muscle maturation is to play activity, studies have also shown that the main effect of play deprivation is increased aggressiveness and violence.

From my view as a physician, the real public health menace on Ronald's Web site is not cholesterol, but the invasion and destruction of the child's fantasy and play life. And commercial interests are not stopping, at comic characters. As mentioned earlier if a child clicked onto Colgate's No-Cavities Clubhouse, there was the tooth fairy who is right up there with Santa Claus and the Easter Bunny as a mythological childhood creation, morphed into yet another enabler character as spokesperson, robbing our children of their souls and turning them into nothing more than super consumers. The tooth fairy is now or was asking for personal information.

For young children there is evidence that commercial interests have not only continued the same inappropriate marketing tactics for children since last year's hearings but now have upped the ante by involving real myths, not just comic characters.

How far will these companies go to gain information from our kids, personal information which will be used in a financial context to target these very children? This is a context which most children do not understand because they have not progressed cognitively from logical thought to the stage of formal operations -- being able to generalize, understanding the nature of advertising and selling.

Kids don't even understand that when they disclose information about themselves, they are giving something away. Not until well into adolescence do children understand what personal information is. As adolescents they may develop a subjective self, an inner voice, a concept of art, and for those of us who have been fortunate as I have to have had teenagers, a strong sense of privacy. Children are not quite connected to their personal self and therefore information about themselves is not valued.

Also imagine a seven or eight year old receiving the E-mail that Shelley put up there. A child who has been raised believing in these magical icons of trust. Receiving personal E-mail from the tooth fairy, no less, saying "Happy Birthday, Billy,", with a "By the Way, have you brushed with Colgate?" This is awesome. The child feels special and certainly wants to please.

The child being in what's called a pre-conventional stage of moral development is quite responsive to cultural labels of good and bad and motivated by punishment and reward. He is going to obey a supreme authority like the tooth fairy.

Now, it may take a whole village to raise a child, but just one big corporation to exploit one. Using the tooth fairy to perhaps gain more authority to extract personal information is an escalation of invasiveness into a child's psychology, a child's psyche, that views missing baby teeth replaced by a fairy/mother figure, who leaves money as compensation for separation, compensation for growing up, the loss of childhood. The tooth fairy collecting personal information for Colgate from children can now be seen as a most alarming metaphor for the giving up of baby teeth, childhood in exchange for commercialism, money and deceit. An invasion not only of privacy but of the child's collective unconscious.

MR. PEELER: Mary Ellen?

MS. FISE: Thank you. I would like to join the Center for Media Education in expressing our appreciation to the Commission for its continued investigation. We know the staff has worked very hard in the last year, and we're most appreciative.

Shelley and Kathryn have described what our review of kid-oriented Web sites found, and I would like to continue that discussion about what we didn't find. I would like to do so in the context of principles or protections that we believe should be practiced in order to protect children's privacy. You will recall, we have submitted guidelines we believe the Federal Trade Commission should issue. So I would like to take up some of those issues in terms of what we found when we visited Web sites.

With respect to disclosure, we found that almost all the Web sites we visited that collect information from kids failed to tell the visitor what is collected or tracked, how it is being collected, how the information will be used, and who is collecting or tracking the information. In some cases one or two and all of those types of information disclosure is included.

With regard to the issue of who will have access to the information and what their commercial interest is in that information, some sites did claim that only their company would have access. Two examples would be Binney and Smith's Jazzy Girls Site and also, as Shelly alluded to earlier, a business site did that. But overwhelmingly, this was the exception rather than the rule.

For a disclosure to be effective, we have said that it must use appropriate language, that being language at a level of vocabulary suitable for children. It must be easily read, meaning visually legible. And it should directly precede and be on the same page as the collection. While a few attempts are being made in this area, for the most part, we found disclosure to be in small print. In many cases, it was written in legalese and it was placed not near the information collection area, but rather was accessible on a link contained on the first page of the site. We had also recommended last year that whenever possible that disclosure be audible to the child and in no case did we ever find that to be the case now.

While we didn't find adequate disclosure for children and their parents, we did find lots of other kinds of disclosure. It is clear that Web site lawyers have been hard at work coming up with disclosures, particularly on limitations on liability. Companies don't want to discuss children's rights, but with respect to their company's rights, these Web sites are pretty verbose. For example, many sites have long sections on the limitations of their liability and their property rights in what they collect from their site. At one site called the Free Zone, they collect personal information, name, age, gender, E-mail address, without adequate disclosure and without parental consent, but Free Zone does includes statements that and I quote, "They are not responsible for any interactions that take place outside of Free Zone's pages."

As a result they may exchange E-mail addresses, Internet addresses or any other information within Free Zone's interactive pages. So not only do they not want to take the responsibility of informing and obtaining consent, but they don't want any responsibility associated with their failure to institute such a safeguard.

On another site, the Sony Wonder site, which also again collects personally identifiable information without parental consent, Sony goes one step further and says, "All personal information provided by you must be accurate to the best of your knowledge at the time of providing the information. Each Station Member --" Station Members are the kids who use play stations -- "each Station Member must provide Sony with accurate, complete information as to his or her name and E-mail address, and must update such information upon any change thereof." So, not only does Sony improperly collect personal information from kids, but they place the burden on the children to keep it updated.

There was a question earlier about changes that have occurred.

COMMISSIONER VARNEY: Before you go on, on the Sony site where it says, "Our commitment to parents," does that outline any of their policies on information collection and disclosure?

MS. FISE: No. These are all described in our report in great detail. The disclosure statement only comes after you've filled out the information.

MS. PASNIK: With respect to the change that took place, you asked, Sony was running a site this year in the USA Today article, and they have -- since June 9th, they have added the statement that the station highly values the privacy of its Station Members. As such the site will not divulge any personal information about a Station Member to anyone outside Sony without that Station Member's explicit consent.

This clause does apply to any advertisements or promotions on the site involving a third-party advertisement or sponsor in which that advertiser or sponsor may request additional information from Station Members. So, it appears that if they're getting paid by a third-party advertiser, then fine, we're going to go ahead and release that information.

Another disturbing practice is telling children that disclosure of their personally identifiable information is optional. At the Nick-at-Night site children are told, "Tell us about you and maybe win a prize." Questions include household income, Web surfing motivations, favorite TV shows, whether the user has cable TV. Name, address, E-mail address and age are also asked but are listed as optional. While there is a limited disclosure statement, parental consent is not required. We believe that telling children that they can win a prize for answering the survey and then saying part is optional is a very confusing message for a child. Most youngsters will not be able to appreciate why disclosure of that particular information is, in fact, optional.

Another concern is on contrary claims. A good site will not have contrary claims that undercut the effectiveness of the disclosure. One example of a site that used contrary claims is McDonald's. On its Write to Ronald page, children are asked to fill in the blanks and write a letter to Ronald. And the blanks include first name, grade, favorite McDonald food item, favorite sports team and favorite book. A note at the top of the Write to Ronald page reads, "Parents, This page is for fun only. The information given is used solely to respond to the participant. The information is not retained by McDonald's."

On the home page, however, there's a link to the fine print that brings you to McDonald's Internet Site Terms and

Conditions, which states, "All remarks, suggestions ideas, graphics or other information communicated to McDonald's through this site will forever be the property of McDonald's. McDonald's will not be required to treat any submission as confidential and McDonald's will be entitled to use a submission for any commercial or other purpose whatsoever."

Another example of a contrary claim is on the KidsCom site. There, the disclosure to kids says, "And don't worry, we don't rent or sell your information to anyone." However, in the letter to the parents, KidsCom admits that their kids questionnaires also help other companies learn about kids. "The results of the surveys we do with kids, whether for ourselves or for others, are always reported in general or aggregate terms." Which makes one wonder what the business relationship or relationship is between the people that enter into an agreement with KidsCom for that information.

On parental consent, we have said that in today's world for that to be valid, it must be in writing. As Shelley had indicated, Nabisco came the closest on the consent issue, however, it was not verifiable consent. And it's clear that obtaining prior parental consent, however, is not foreign to these companies to the sites we visited. For example, Crayola asked for personally identifiable information at its site, name and E-mail address, but did not require parental consent.

However, children who send their mail in by postal mail, their artworks to the Crayola playground, must have parental or guardian signature, so that Crayola will know you have permission to enter the drawing. So in the context of the Crayola playground gallery, they want signed consent from the parents. So we know that they know how to do it.

Finally, a good site will have a correction procedure available, and only a few of the sites we've reviewed -- one example would be Bonus.Com which had a procedure to delete or add to previously collected personally identifiable information. Only a few sites we reviewed indicated that they have a process for preventing further use of personally identifiable information previously collected allowing the parents or child to go back and delete or correct. One example is Kellogg's.

In summary, we believe there's more than ample evidence of the unfair collection of information from children and that enforceable guidelines by the FTC are urgently needed.

Last year we submitted to you very, very detailed guidelines that we believe that the Commission should issue. And we've expanded that just slightly with five initial requirements based on what we've found in our review.

Those five very briefly, and I'll close with this, are that products spokes characters and other mythical fictional figures should not be used to solicit personally identifiable information from children. Unsolicited commercial E-mail should not be sent to children. Children should not be asked to release personally identifiable information about family members and other people they know. Free merchandise or the chance to receive free merchandise should not be promised to children in exchange for personally identifiable information. And finally children should not be asked to change privacy preferences set by their parents.

MR. PEELER: Thank you, Mary Ellen. We would like to get copies of the overhead that you used for the record. We would also like your opinion about whether the number of sites in general are going up, going down, or staying about the same.

MS. FISE: There's no doubt in my mind that it's increased. Last year at this time to do a search and to find a particular company online, often times you wouldn't find that company there. Now, any company that has a presence in kids culture has a presence online. So I definitely think it's increased.

MR. PEELER: Commissioner Starek?

COMMISSIONER STAREK: Yes, Kathryn, in your introductory remarks, you said we needed to take action right now because companies had not gotten better, they had gotten worse and there was a presentation by you and your colleagues on the fact. And also that the blocking or the filtering technologies that were on the market weren't adequate. And I wondered if you would elaborate, why are the technologies that are currently available to block and filter these this kinds of sites and other kinds of objectionable sites to parents not adequate?

MS. MONTGOMERY: I'll tell you my primary concern in the area of online children's marketing. And that is that -- I know that some of the software programs have been adapted so that kids can't give out personal information in some cases. First of all, it's a somewhat prudent mechanism in many ways in that you can't necessarily discern when children can give out that information and when they cannot, but my bigger problem with it is that at this early stage of development of this new medium, if we create a paradigm, if you will, that puts most of the responsibility on the parents to keep these kids from giving out information, personally identifiable information to companies, you really in many ways give the green light to companies to develop many, many manipulative and unfair practices that parents then have all the responsibility of protecting their kids from. And we're talking about really the creation of kids' culture for the 21st century. My concern is that we need at the outset to have some clearly established groundrules for how you market to kids online.

MR. PEELER: Commissioner Steiger?

COMMISSIONER STEIGER: You mentioned that you were able to determine which sites used cookies and which did not. Were you able to determine to what use the cookie was played? We have had several people tell us that the only purpose of the cookies basically is to count the number of hits, that it is too expensive, time-consuming and complicated to link that information or to link other visits to a site, another site and so forth. That is, the cookie is basically to count the number of hits and be able to tell an advertiser or marketer the numbers as to visits on our site and to the quality of the product on the site. Can you tell what use the cookies are being put to on these children's Web pages?

MS. FISE: Commissioner Steiger, if I may, they're not disclosing that so I cannot tell. What I can tell is when they're being placed, and there seems to be a high correlation between sites that solicit personally identifiable information and the placement of a cookie. And so as you move through a particular Web site and visit various pages, it's when submitting the registration form or when providing information that they've asked for that yet another cookie or that pop up window appears.

But, no, that's something that is lacking across the board. No company disclosed that they're using cookies, and so if I had my browser set so I didn't get that prompt, I wouldn't be aware of it. And many users have their system set up in that way. And then also in the disclosure or legal statements not a single word was said about cookies.

COMMISSIONER STEIGER: Can you explain why there might be as many as 12, I believe, is the highest number that you indicated on a single page?

MS. PASNIK: I don't know. The messages tended to vary from window to window when the cookies were being set. Sometimes it was the same window that would appear, but I would answer yes, because I know sometimes if you're asked if a cookie can be sent and you say no that window can appear again and the question is re-asked. But I would always eagerly answer yes and then the cookie prompt would appear again. But, no, it's not clear to me.

COMMISSIONER STEIGER: Thank you.

MR. PEELER: Well, thank you very much for your presentation. We appreciate the materials you've submitted; we will be taking a close look at them. I would like our third panel.

PANEL III: THE POTENTIAL FOR INJURY TO CHILDREN ONLINE BY PREDATORS

Linda Hooper, Supervisory Special Agent Federal Bureau of Investigation.

Judith Schretter, Trial Attorney, Criminal Division, Child Exploitation and Obscenity Section, U.S. Department of Justice

***

MR. PEELER: In addition to all the terrific information we're getting today, we're also running out of time. I think you'll find our next panel to be particularly important. This panel will address the type of most serious potential injuries to children online from both predators and pedophiles. We are very privileged to have with us two representatives from the law enforcement community. Linda Hooper from the Federal Bureau of Investigation. She is the supervisor of "Innocent Images," an undercover operation and the primary objective of this investigation is to identify and develop prosecutable cases on individuals who use computer services, as well as the Internet, to recruit minors for elicit sexual relationships.

In addition, she's joined by Judith Shretter of the U.S. Department of Justice. Judith is a trial attorney in the Child Exploitation and Obscenity Section of the Criminal Division of the United States Department of Justice and she's going to discuss the Department of Justice as well as "Innocent Images" investigations and examples of recent cases. Linda?

MS. HOOPER: First, I would like to thank you very much for inviting me here today, and I'm just going to talk to you for a few minutes about an investigation that the FBI started in July of 1993 and which has evolved into a national initiative. Let me keep in mind that I am a law enforcement officer, I'm not a computer expert. So if you have any questions towards the end, gauge them in that arena.

Because this is an ongoing criminal investigation, there are specific areas that I am not going to be able to talk about, but I'll briefly describe to you exactly what this initiative is and how it got started.

The FBI has developed several initiatives designed to address the emerging trends in utilizing computers to conduct or facilitate criminal activities. In July 1993, the FBI initiated an investigation entitled "Innocent Images". This ongoing initiative focuses on individuals who utilize computers to facilitate the distribution of child pornography, as well as those who use commercial online services and the Internet to recruit minors into illicit sexual relationships. And it was predicated on the disappearance of George Stanley Budinsky, Jr. of Brentwood, Maryland.

While investigating this disappearance, FBI agents and Prince George's County, Maryland police detectives identified two suspects who had sexually exploited numerous juvenile males over a 25-year period. Investigation into the activities of these two suspects determined that both adults and juveniles were routinely utilizing computers to transmit images of minors showing frontal nudity or sexually explicit conduct as well as to lure minors into engaging into illicit sexual activity with the subjects.

Further investigations and discussions with experts, both within the FBI and the private sector, revealed that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques used by pedophiles to identify and recruit minors into illicit sexual relationships as well as to share photographic images of minors.

Let me make this point, it's very important that the FBI does not surf the Net, but we only go into predicated areas. Predication is based upon consumer complaints, service provider complaints, complaints from the National Center for Missing and Exploited Children, and law enforcement. The National Center has actually set up a toll free tip line so consumers can call in any complaint that they have or that their children have encountered online.

The first goal of this undercover operation is to identify and locate individuals who are using computers to arrange meetings and with -- and the sexual molestation of children. As this investigation has shown, the technique of contacting children via computer is being frequently used and with destructive results. Because they are aware of the need to maintain absolute secrecy, these individuals use their computers to interact with children in a covert fashion. Consequently, pedophiles and child molesters use computers which offer a high degree of anonymity to meet others and exchange information about children.

The second goal is to identify and gather evidence against those individuals who are producing original images and introducing those images onto an online service or the Internet.

The third goal is to identify and gather evidence against those individuals who, while not producing child pornography, are major distributors of child pornography. The FBI continues to analyze information obtained from sources, complainants, undercover agents, searches previously conducted during this investigation, and service providers to identify those subscribers. Most of those subscribers identified through this investigation have readily provided child pornography to our undercover agent.

In addition, prosecuting charges in the investigation, a priority is placed on protecting the children who are subjects of child pornography and sexual abuse. This priority is important for the Attorney General Guidelines for Victims and Witness Assistance and reflects the national concern for protecting innocent victims.

MR. PEELER: Thank you. Judith?

MS. SHRETTER: As you heard, I am a Trial Attorney with the Child Exploitation and Obscenity Section in the Criminal Division. My section was formed in 1988 as an outgrowth of the Attorney General's Commission on Pornography, which met in the mid-1980s. The initial focus of the unit was an obscenity issue, but as a couple of years passed, it focused more and more on child pornography and other issues dealing with children.

Our section's name was changed in 1991 to reflect the trends in our office. We are approximately 15 attorneys. We provide assistance to the United States attorneys all over the country who can call us for assistance on the statutes over which we have responsibility, including obscenity, child pornography, travel for purposes of engaging in sexually explicit conduct, child support enforcement, international child abduction -- a whole variety of child-related issues.

I most recently came back from Las Vegas where I helped try a case coming out of the "Innocent Images" project where we convicted two brothers who were subjects of the

"Innocent Images" project. They were distributing, receiving and possessing child pornography which they had received online. In that particular case, we were not able to identify any of the particular victims. The images that were involved with the case are many of the same images we're seeing in a lot of different cases around the country.

I did bring with me today a couple of samples of cases in which we provided assistance to the United States attorneys in which actual children were victims of somebody online. And I would like to share a couple of them with you.

There is one case in which we've been providing assistance in which a child, a young teen, was online in a teen chat room. An individual representing himself as a kid was also in the chat room. At some point after he had established a relationship with the teen, he then said to him I have a friend, an older friend, who would very much like to meet you. In his new persona, he then got online with the same teen in the chat room as the adult.

The child that was targeted was typical of the kinds of cases we see that pedophiles or molesters target off the computer as well. A teen who may be very unhappy, may have poor peer relationships, may have a poor relationship with their parents. They're craving attention. People get on with them and develop and manipulate, and develop a bond with the child. He made arrangements to meet in the child's hometown. The adult traveled from his home to the child's hometown. Then they left on a bus and traveled. They were on their way back to the adult's home. The child's mother found evidence of what was going on, notified the police and they were able to intercept them en route. When they did a search warrant of the adult's home, they did find out that he had engaged in the same kind of conduct with other children.

Another example, there were a couple of cases involving adults who again meet children in chat rooms. They lie about their ages. In these particular cases, they were targeting young teenage females. They said they were about 20. Fortunately, in one particular case, one of the people they ended up talking to in the chat room was an undercover agent. And they made arrangements to meet that agent and was arrested, but they did learn that the same adult had done this with several young women and had engaged in sexual relationships with about six young women. These girls, again, not quite the same personalities perhaps as the child in the first example, but they were very flattered that a 20 year old liked them and was showing an interest in them.

There is one other case I would like to share. A teenager on the East Coast meets someone, an adult male from the West Coast, and tells her girlfriends at some point she's got a boyfriend online and he loves her and so on and so forth. At some point the child travels with her mother to a swim meet in another state and has made arrangements with her boyfriend to meet at the hotel where the swim team is staying and they do actually meet. The girl's friends though do tell her mother what's going on and the mother was able to intercede and rescue the child from this situation.

So children can be very vulnerable and we see that in these kinds of cases. Agent Hooper mentioned the National Center for Missing and Exploited Children. They have a child pornography tip line which they began with the customs service many years ago, and I work closely with the FBI, Postal Service, as well as with the Customs Service. They are accessible at 1-800-843-4678. The information they receive, they do pass on to appropriate law enforcement agencies for appropriate follow up.

Another item that the National Center publishes is the booklet "Child Safety on the Information Highway," and that can be found online at www.missingkids.com. It has tips for parents as well as children, and they've done some targeting of young teens. They created some mouse pads in cooperation with law enforcement agencies and we're distributing them through some of the junior high schools with some of the safety tips for children to have next to them right at the machine. So I hope the message is getting out.

COMMISSIONER VARNEY: What do either of you see as the correlation between information gathering for minors and children without their parents' consent and the vulnerability of these kids to predation? I'm not really talking about kids that go into chat rooms and meet somebody in the chat rooms who deceives them, but how much do you see of the kinds of people that you've talked, the pedophiles and the sexual molesters harvesting data, using cookies, using the kind of technologies that we've been looking at today to find kids?

MS. HOOPER: Well, we do see that. And actually what we've termed them is the lazy pedophiles.

And those are the ones that will go into an online service and will look up profiles of children. They'll put in what their desire is, and it will bring up all the profiles of children that live in a certain geographic area. That way they don't have to travel very far. So, if your children are putting in true information in that profile they be contacted by a child molester or pedophile online.

COMMISSIONER VARNEY: Can you elaborate on that? My colleagues are astounded. How could somebody do that?

MS. HOOPER: If you enter a profile --

COMMISSIONER VARNEY: Where?

MS. HOOPER: With a service provider. You have the option as a member to put in information about yourself that is accessible to anybody in that service. Now you are the only one who can enter that information and the only one who can change that information, but that is accessible to anyone who is on that service, and you can enter any information you want.

If you're an adult, you can enter that you're a 15 year old boy for example under one of your screen names, and if you go into a chat room and you're carrying on a conversation with what you believe to be other 15 year olds, you can pull up their profile and you can see who they are. And when they pull up your profile, they think that you're a 15 year old.

COMMISSIONER VARNEY: How about some of the sites we saw that collect a lot of personally identifiable information from kids, are they vulnerable to the wrong element getting into their databases or intercepting their information?

MS. SHRETTER: I don't know that.

MS. HOOPER: I don't know that either and that's a violation that would not be worked off of what I am working now.

COMMISSIONER STEIGER: You mentioned that you are looking or following, of course, complaints throughout the Net as you used the word, where there could be a problem. Would you say that if the material goes through a service provider, there is some protection to the extent that the service provider can track this individual or tell you the individual's address? Is that easier as you are trying to bring a law enforcement action than simply being on the Net or does it really make any difference?

MS. SHRETTER: We would have to serve a search warrant on the service provider to get specific subscriber information. The service providers are sort of like a collection point, the message is passed through this service. But I believe unless they receive a complaint, they may not necessarily know what's passing through.

MR. PEELER: What advice would you give to parents in terms of disclosure of personal information about their kids on the Internet?

MS. SHRETTER: Certainly on the profiles I would not have my child filling out a profile.

MR. PEELER: What about identifiable information in chat rooms?

MS. SHRETTER: I certainly would be circumspect about what I would provide. I think parents certainly have a responsibility to know about chat rooms and what their children are doing online.

COMMISSIONER VARNEY: What about these sites that we saw that aren't necessarily chat rooms that are collecting information from kids maybe for marketing purposes, maybe for other purposes? What would you tell your kid about that?

MS. SHRETTER: Fortunately, I don't have little children anymore, I don't have to confront this, but I certainly would be very careful about the information I permitted my child to put out there.

MR. PEELER: Thank you, very much. We appreciate your coming, and we certainly would like to get a copy of the brochure for our records.

We're now about a half hour behind. We would like a 15-minute break by, I think, a unanimous vote of the Commissioners.

We know it's been a long day for everyone.

(A brief recess was taken.)

PANEL IV: THE PRIVACY PRACTICES OF COMMERCIAL WEB SITES

"Do commercial Web sites provide parents with notice and control regarding the collection and use of information collected from children? What are the costs and benefits of creating privacy policies?

Jorian Clarke, President, KidsCom

William W. Burrington, Assistant General Counsel, America Online, Inc.

Robert McHugh, Senior Producer, Yahooligans!

Arthur B. Sackler, Vice President Law and Public Policy, Time Warner Inc.

Craig Stevens, Director Research Services, Digital Marketing Services

***

MR. PEELER: Now we will hear from some Web site operators about their approaches and perspectives to children's privacy. In particular, we will be interested in hearing more about things that are not readily apparent from just visiting the Web site, for example, what type of information is collected, what is it used for, what do the different sites do to provide parental control when the information is being collected? Is the information retained in an individually identifiable form in the site? And is it given out to third parties?

We have a very good panel today to discuss these issues. First Jorian Clarke, who is the Founder and President of KidsCom, an educational and entertainment Web site. KidsCom is geared for children four to 15 years old. Second, Bill Burrington, who has been a fixture at most of these hearings -- almost doesn't need an introduction again. Bill is the Assistant General Counsel at America Online. He's joined by Robert McHugh; Robert McHugh is the Senior Producer for Yahooligans!, a comprehensive Web site for kids. His sites are selected and individually reviewed for appropriateness for children. Rob also has many years of with such companies as Claris Spinnaker Software, an Educational Development Center and Computer Curriculum Corporation.

In addition we are joined by Arthur B. Sackler. He is Vice President, Law and Public Policy with Time Warner, and he's here for his second day. And we appreciate you joining us.

And finally we're joined by Craig Stevens, who is with Digital Marketing Services and is the Director of their Research Services. Digital Marketing Services conducted over 150 online research studies on behalf of a number of companies, including marketers of children's products. They've established a methodology for conducting research involving children and Craig will describe how DSM obtains parental consent before collecting from children and has adopted policies on collecting information on an aggregate anonymous basis.

So with that, I would like to start by asking each of the panelists to spend about five minutes just addressing the general question of what their site does, what information they collect, what do they do with it. So, can we start with Jorian Clarke.

MS. CLARKE: Thank you. I'd like to start by thanking the Commission. It really is an honor to be here because of what we have learned. We attended last year as an attendee, and we're pleased this year to come forward and talk about the practices that we've done. We're also pleased to hear this because yesterday we heard a lot from people that there were theories, but we now are going to actually be able to talk about practices, what we've been doing in the past 12 months in self-regulating based on our knowledge of privacy, safety and advertising standards.

The KidsCom site has now been live since February of 1995 and during the course of two years and four months, in working with kids, parents and educators from 81 different countries, we've experienced a lot. As a site dedicated to shrinking the world, we are continuing our leadership tradition by bringing forward our creativity and offering these practices that work to address these issues. In a moment I'll detail these practices and then we'll go online briefly to show them.

We would also like to thank the people that helped us understand these issues -- our kids, educators, parents, KidsCom, our advisory panel including several of the advocacy groups that have talked earlier the last few days, including the Children's Advertising and Review Unit (CARU) of the Better Business Bureau and the professionals at the FTC. As a result of these changes, CARU now calls us one of the kids' sites leading the industry and using creative solutions for addressing concerns about child safety, privacy and the development of online advertising standards. While these efforts have placed an additional cost on the publication of our cyberzone, we have had challenges in blazing a trail to implement some of these solutions. We also believe that it is essential that other kids' sites follow us in this direction. We know that our sensitivity to these issues and our solution have been appreciated by parents and educators and that response has often been encouraging enough to keep us going.

For those who work from a business platform in addition to an ethical platform, we feel it has given us a competitive advantage in being recognized as a safe, responsible and electronic playground for kids, parents and educators. We look forward to seeing a corporate involvement with us in advertising and sponsorships and to grow as fast as our appreciative user base.

I'm also proud to tell you that not only have we taken these issues to heart on our own site, but we have started to spread the word at the industry. Last week at the industry's Digital Kids conference in San Francisco, we passed out approximately 200 CARU guideline pamphlets and used our feature talks to raise the awareness in the industry of all these issues.

We have also consulted with other kids to move them in this direction. We will show you a commercial kids site introduced last week called Avery Kids by the Avery Dennison Corporation that makes use of these new practices, so we have changed our own site and we are working hard to improve others. Now we would like to share with you some of what we have done date.

On the issue of online privacy and safety, KidsCom has worked hard to make parents aware of and involved in what their kids are doing on the site. Kids can play on the site without registering. Registration is only required to write content for posting on the site, to exchange E-mail addresses, to have contact in the chat rooms or to earn points on the site. Kids can earn points for educational activities, for giving us their opinions, and surveys, information from which is only released in aggregate form and has always only been released in aggregate form, and for getting their parents, teachers and friends to register on the site.

Registration information never has been and is not rented or sold to any third party. Registration information has never been used for marketing purposes. And again, just to set the record straight, registration information has never been used for marketing purposes. We've also taken big steps in providing notice on how information collected will be used and in gathering parental consent. Parents are notified by E-mail when their kids register on the site and are given the opportunity to have the registration information removed. And again, if the parents choose to remove the registration information, the children still are able to play on the site.

In our surveys, parents are allowed to have their children's responses removed even though we always only release findings in aggregate form. An individual child's responses are never released. We instruct the kids to get their parents' permission throughout the site and we have kid-o-fied things, such as our legal statement and our registration form, so children can understand them better. Users have the ability to opt-out of receiving E-mail about new features on the site and parents are reminded in every E-mail we send to monitor what their children are doing online.

In addition to opting out of some features, we also use opt-in. In order to have their child participate in the exchange of E-mail addresses in the key pal area, parents must mail or fax us a signed permission slip. In order for kids to receive any items that kids can earn from the KidsCom locker, a parent's check must accompany the request form. The check covers a small portion of the shipping and handling and also ensures parental permission in the ordering. We've learned the hard way as we ship aquariums that again this is important to have parents involved in this activity.

A fun and engaging safety game was developed using the kids' favorite characters in the KidsCom games and crafts area and they also are encouraged to play it when they first register on the site. It's called Iggie and Rasper's Internet Safety Game and here children receive points for playing the safety game and can earn additional points for having their parents review and sign off on the safety tips with them. This game, together with the parent signature, provides the highest single source of points accumulated on the site. An Iggie and Rasper safety shirt with Web tips has been produced and hundreds of kids around the world are now wearing these at school and on their playgrounds helping to spread the word on Internet safety. Among other things, the safety tips teach kids not to post or send to a stranger.

You can look at the safety tips that we're trying to communicate to children as one more way to educate kids. Just a few other points. It's helpful to understand what level of content your kids like on the site and currently who is using the site. But we strongly believe that the use of cookies in its current state of the technology is not appropriate for use on a kids site as a tracking mechanism. Kids should get cookies with milk, not with their hard drives.

We're working hard with kids, parents and teachers to draft a privacy symbol and a content model that can be used successfully to educate kids similar to the Ad Bug that I am going to tell you about.

Much of the discussion of online privacy and safety includes concerns about advertising to kids in this medium. We have looked at this issue in our cyber Zine and we now are leading the industry and trying to come up with safe practices. One of these is the development of the character called the Ad Bug and it's offered to the children's online industry as a symbol of the distinction between advertising and editorial content. The Ad Bug appears on kids' sites wherever there is advertising as a way to help kids know the difference.

MR. PEELER: Thank you, Jori.

COMMISSIONER VARNEY: I have to say, Jori, that I am so pleased that you're here. Last year you came, you took a lot of hits, a lot of people thought you guys were the bad guys and you have proved us wrong. You have turned your company into the model of working with the FTC. Although we may not agree with everything you're doing, we really appreciate the work that you have done to try and lead the way. Is it fair to say that your company now would be quote in "compliance" with the CARU guidelines? Have you looked at the CME guide?

MS. CLARKE: We have not received a copy of those. We have looked at them and we don't agree necessarily with all the things that they suggest, although we certainly agree and practice the principles of a lot of the things that they suggest.

COMMISSIONER VARNEY: Your company has done so much with us, I hate to put an additional burden on you, but would you go through the CME guides and in particular point out those areas that would be a problem for your company either because of technological reasons or other reasons, because I would really like at some point to get your sense. There seems to be a gulf between a CARU set of proposed guidelines and a CME set of proposed guidelines and I'd like to see where players in the industry are coming out on them.

MS. CLARKE: We would be delighted.

COMMISSIONER VARNEY: Thank you for coming.

MR. PEELER: Bill?

MR. BURRINGTON: Thank you, very much, Commissioners and professional staff at the FTC. It's good to be back yet again.

COMMISSIONER VARNEY: You know we got you an office downstairs.

MR. BURRINGTON: Thanks. I would like to in the short time we have, obviously there are some other points I want to bring up today which I'll simply incorporate when we do the Q and A. Let's take a step back to where we were a year ago in a general sense. I think we made a commitment, both as a company as well as an industry, to really deliver commitments about privacy in general, and we have some relevant industry guidelines coming from a variety of sources. We've delivered a consumer survey which turns out to be very reliable to find out what consumers really feel about these issues while we all sit here and talk about them.

We've really made movement in the overall direction on privacy. Clearly, the children's marketing area is one of our two or three top areas right now as a company in terms of consumers and let me go through briefly a few things that will explain our service and what we do.

We've been revamping our children's marketing guidelines for the last year or so and that's what I want to share with you right now. A couple of quick points before I do that is that we don't give out our lists of children period. We don't have such lists, therefore, we don't give them out. The second thing is we don't market to children period. And finally we have adopted sort of a principle within our company of parental permission first. We happen to think that parents need to give permission first before their children give out any kind of information or enter sweepstakes or what have you.

Let me take you through a couple of things and explain first what we mean by the Kids Only area. We've been able to segregate content and pick what we think is some of the most valuable content for children particularly ages six through 12. It's called our Kids Only Channel, and when parents sign up to America Online, in order to sign onto America Online, of course, you have to have a valid credit card, you have to be 18 years of age or older, you have to have a valid checking account as an alternative, and the bottom line is to be the master account holder on America Online, you must be 18 years of age or older. And certainly you're then allowed to create up to four additional screen names which could be screen names for your children.

As a master account holder you have the ability to set our parental control tools which we make widely available to our members and within that process you can select the Kids Only Channel, if you will. And that will channel kids into Kids Only areas that we feel are appropriate for them given that age range. One of the two popular areas within the Kids Only Channel are the chat rooms for kids and also pen pals. And when any child enters the Kids Only chat room area, the first thing they're going to see are the AOL safety tips, which I think it's worth reading these because these are the core common sense principles that we all have to educate parents about and children about.

One is don't give your AOL password to anyone, even your best friend.

Second, never tell someone your home address, telephone number, or school name without asking a parent.

Three, never say you'll meet someone in person without asking a parent.

Four, always tell a parent about any threatening or bad language you see online.

And five, if someone says something that makes you feel unsafe or funny, don't just sit there, take charge, call a guide which is a key word, Help, and leave the chat room or just sign off. These messages pop up frequently not only to remind kids about their own responsibilities, but about their need to connect with the parent.

One of the popular areas is chat. When children get into that chat room a screen is going pop up to tell them -- in this case this happens to be one of our front screens for

AOL Kids Only area. Also in the club area they can click on Pen Pals which is one of the more popular areas on the service. Kids from literally around the world can pick up a pen pal, start corresponding with them back and forth by E-mail and again the same warning pops up. And then at that point they can go into, this is just representative of the fact they can pick the age category if they want to meet kids who are six to eight or nine to 12 or whatever. They can go in there and read these individual E-mail messages that have been posted and decide if they want to become a pen pal with that person.

One of the other things that I want to talk about briefly is our approach to some of the areas that are most troublesome which have to do with selling merchandise or attempting to merchandise the children. One of our partners, Ringling Brothers Online has a store and the child will click on that area and when they enter a store there will be a splash screen that will pop up that simply says, "Only adults 18 and older with a valid credit card can order merchandise on America Online." And it's simply a reminder to them that they're not going to be able to order merchandise, they have to have a valid credit card which means they've got to go to mom and dad and say, I want to order this, I need your credit card.

It's important to know that right now in the Kids

Only area we only have two stores of this type that are selling merchandise, and we as a company are moving away completely from having any kind of merchandise sales in the Kids Only area. So there are two stores now but eventually there will be zero.

One other thing I just want to talk about briefly here is the Cartoon Network World. What this is about is a game pad, this is a pretty popular area on AOL. There's a thing called Mystery Tune which they get into and they have to kind of figure out who that cartoon character is. If they're the first person to post the winning entry, then they get a prize. So they would post it up there.

And one of the things that we're doing now which is part of our proactive policies in terms of protecting children in the market area is once they do that and they post it, the child will then receive back an E-mail saying, "Congratulations, you've been selected as a winner," so on and so forth, and what they need to do is print out this E-mail and then give it to their parent who has to sign it, fill out their name and address and other information and then either mail or fax it back into this provider in order to claim their prize.

So we think again it forces children to go back to mom and dad and say, look, I won this prize, I need your permission, you need to fill this out, you need to send it in. We think it's a very effective tool, it's been working. These are some of our newer policies.

And finally let me talk about another example of our changes and some of the issues that we're dealing with the Nickelodeon online area, which has to do again with some sweepstakes. When they get into this area, the sweepstakes area, there will be a pop-up screen that will come up simply saying to the child that's in there, "In order for this company to accommodate your prize winning entry, you're going to have to give your name and address and so on and so forth." This illustrates one of the problems we have right now. We're working with all of our content partners, the ones we have contracts with, who also have their own separate content that they give to us for the Kids Only area to essentially ask us and make them comply with our policies and most of our partners have done that very willingly; and we've been working together very closely with them.

One of the dilemmas we have is that a lot of these contract partners like Nickelodeon have their own Web site, so you as a child or anybody can go directly into that Web site, if you're on that online service. And so the best we can do right now is when you are connected into that Web site in this case it's a link to a Web site from AOL, we'll pop up a screen and at least warn children, to talk to your parents, that kind of thing. You're going to have to give out information, talk to your parents.

The other thing I want to note here is and if you want to go to the last slide. This is significant just because this is an example of our browser in the Kids Only area. You will notice if you're familiar with America Online, there are some key things missing here. For example, the child cannot go in and type in the URL for some other address so they can't bypass this because this disables the key features for our Web browser within the Kids Only area. They cannot click and make it part of the their favorite places so they can just go directly to that area so essentially they're stuck right there. They can't go anywhere else. They have to back out and then they'll get to other Kids Only areas. So these are some of the things that we're doing.

Let me finish with the key points and then I'll raise some additional ones during the Q&A session. One of the things we're finding as we work with MicroSystems which as you know is the developer of Cyber Patrol and they've done a terrific job in screening and helping to filter out content for children. What we're trying to work with them on right now, they're very seriously working on this and we're working with them on it, is to do the same thing not only for content but to do it with respect to privacy and with respect to appropriate privacy standards.

We've been supportive and actively involved in all the various industries' privacy guidelines development initiatives, and in the end I want to leave you with a couple of key points that we think that as this medium develops globally that clearly children are the key here. They really are. All of the issues that thus far have significance have involved children -- content with the Communications Decency Act, and how do we protect children against inappropriate contact. We've led industries on that for over two years in developments that we're taking in terms of enhancing our parental controls.

In the area of child pornography which you've heard about earlier, we've lead the industry in developing protocols with the FBI, with the Justice Department, with Interpol and other law enforcement agencies so that we can cooperate. We do not want child pornographers online, period. We don't want them on our service, we don't want them on any service, so we have developed very effective cooperative arrangements with law enforcement agencies worldwide. And now our children's marketing -- that is the great focus of our company right now. I think we're making progress there and I'll be happy to answer some additional questions on that product. Thanks.

COMMISSIONER STEIGER: When we heard from the law enforcement officials earlier this afternoon, they suggested that there was such a thing as a lazy pedophile who would use consumer profiles including profiles of children that they were able to gather, if I understood correctly, from service provider lists. Is that correct that such lists of profiles of customers are available, or did I misunderstand that?

MR. BURRINGTON: Commissioner, let me speak with respect to America Online and our eight million members worldwide. We again educate parents about the need to enable parental control tools and with that they can channel their children into the Kids Only area and once their children are in that area, if you will, corralled and roped off into that area, they are not allowed to create a member profile.

We also actively promote the creation of member profiles. If you sign onto AOL we don't remind people that Gee, you should create a member profile. It's an optional thing that members do. As an AOL subscriber, I can choose not to create a profile at all and then there's nothing to search on, and then certainly in the Kids Only area, we completely disabled that function altogether so that children are not allowed to create a profile. Clearly the issue here for us is to continue to educate parents on how to use these parental controls and they have those controls in their face all the time so they know how to use them.

Does that answer your question?

COMMISSIONER STEIGER: How accessible are members' profiles?

MR. BURRINGTON: Well, in terms again speaking for America Online, you can click onto -- there is an area on the top screen, the front screen of the service where you can go down and search for member profiles. So in my case if my business screen name is Billburr, I have Billburr in my title and company and I get a lot of strange E-mails because of that, but people could conceivably search for, for example, Washington, D.C., and then anybody who has chosen to create a profile, any adult who has and in the case of kids- only they can search and find other subscribers that are in Washington, D.C. for example.

The important thing to remember is there is no master profile data base of all 800 million -- excuse me, eight million subscribers to America Online. It is an optional feature some people like to do that because they want to tell other subscribers that I have an interest in this area or I live in this area and again it's a very optional thing and in the case of Kids Only kids, they can't even create a profile to begin with.

COMMISSIONER STEIGER: Thank you.

MS. RUSK: Within AOL the screen name that appears when a child is in a chat room is essentially their E-mail address and I wondered if you could comment on that in light of the problems we've heard about.

MR. BURRINGTON: Well, I think that -- we do have this unique feature in that we allow people to create screen names which in effect do become their E-mail address, if you just add the @ sign and AOL.com, that is their E-mail address, but I'm not quite sure what you're looking for in that regard. I just want to clarify your question a little bit in what you're looking for in that regard.

MS. RUSK: In order for a child to participate in the chat room, will that screen name automatically appear, so that everybody in the chat room sees their E-mail address?

MR. BURRINGTON: Yes, that's correct. Now the important thing here though is within the Kids Only area, we have dedicated Kids Only area chat rooms and on the overall service and I know I keep coming back to parental controls, but parents can, when they enable those tools, and we urge parents to do this, they can disable the chat room function altogether. They can say for my six year old or my eight year old, I do not want him or her to be able to chat with anybody.

They can select out and say give me the names of your five favorite friends on AOL and those are the only people that you will be allowed to get E-mail from. They're very sophisticated but yet easy to use.

If you can click a mouse and you can type fairly well, you can enable these controls, and so we think again this is an example where all of us have to work together on this.

This is not a government solution problem, it's not an industry solution problem, it's industries, government, parents, educators working together and also law enforcement to get these messages out to people, in our case to tell them activate your parental controls. If you just go into that area, it's very self explanatory, it walks you through their oncoming version of the service where they actually have an interactive which literally says if you have a child do you want them to do this? Do you want them to receive E-mail from everybody in the world or do you want to continue it to only a few people? Do you want them to be able to go into the chat rooms or not? We have the Kids Only area and they're welcome to go into that. It's a very, very effective tool. The challenge for all of us is how do we promote the use of those tools and keep making that.

MR. PEELER: Bill, do you know what percentage of your subscribers have children who are using the parental controls now?

MR. BURRINGTON: We have some data on that and I know there was a figure I think thrown around here today earlier when I was not here, something like 25 percent users. I know that our percentage is higher than that, but I can't tell you today exactly what that percentage is.

MR. PEELER: Fifty percent?

MR. BURRINGTON: I would believe it's less than that. And we're not happy with that. That's not a good thing and we want to work on that. We're undertaking some initiatives. Steve Case, our Chairman and CEO in a recent speech at the National Press Club, said we're all busy building this medium and we all, AOL, our competitors and others who care about this medium, have got to take the responsibility to start really educating parents.

We tried to do that a couple of years so when we created the Online Public Education Network through the ISA, Interactive Services Association, with an 800 number and a brochure -- and essentially we need to get the information about parental control tools and other blocking tools in peoples' faces and I think to the extent we can cooperate with government to do that, that's what we want to do.

We're going to be organizing with industry children's groups, education groups and government people a two-day summit in the Fall to talk specifically about child safety issues at the Family Online Summit. The idea is to bring everybody together that has a stake in this including law enforcement, educators, the President and people from FTC and other groups to say what progress has been made to make available parental control tools and how can we use our collective resources, including the President of the United States and parents to use these tools and here's how you use them and here's where you can get them.

That is the most effective thing that we can do.

MR. PEELER: Thank you. We'll now turn to Rob McHugh.

COMMISSIONER STAREK: Excuse me. I would like to learn a little bit more about the Kids Only area. When you turn on the computer and it's a choice that you can go there, a choice that the parent would obviously make and then once in there, you can't get out. Is that right?

MR. BURRINGTON: That's correct, Commissioner. Again, when parents begin to master, again it gets a little confusing, but I keep throwing these terms out so that we can clarify them.

Only the master account holder can make changes to those parental control tools.   And only an adult who's 18 years of age or older can get an AOL account. So presumably the master account holder can have four additional screen names, one for say Johnny M., who's nine years old, I'm going to go in there and allow him to have access to the Kids Only area and that's the only place he can go.

They can't go out on to the Internet or somewhere else and you can see there are barriers. We're putting up the reminders working with our partners to require a principle that we've adopted which is parental permission first -- you have to get your parents' permission before you do anything. We are also working with MicroSystems in terms of some privacy patents.

COMMISSIONER STAREK: So the Web sites that are highlighted here in the CME study would not be only in the Kids Only area of America Online because the vast majority don't require parental control?

MR. BURRINGTON: That's correct. You raised a very, very important point for these hearings which is that when you are a subscriber to America Online, we have our own content -- in the case of the Kids Only area we have people who have created their own content and of course that's all very carefully screened. We then have partners like Nickelodeon or Warner Brothers and we have contracts with them and we work with them and say, to the extent you're going to do business with us and we want your content very much, these are the rules you have to comply with, parental permission first.

And then keep in mind as the CME study shows that there are going to be a whole lot of other Web sites out there that we will not connect to. You can get to those sites if you get onto the Internet, but within our world -- I used this analogy before -- in some ways we're like at a resort and there's a swimming pool there that's got some lifeguards, lane guides and rules. And that's really the propriety, private America Online network. Then there's a little channel that will whisk you out into the ocean and that's the Internet.

We can work on a lot of things with respect to the Internet, but then there's other areas we simply don't have control over. To the extent we have some control, a contractual arrangement with content partners of our own content that we've created or not allowing kids to go to certain Web sites. That's the best that we can do and, frankly, it's very effective.

COMMISSIONER STEIGER: Can you tell me how broad the content is in this community of current events, how broad a range?

MR. BURRINGTON: Yes, Commissioner. There is quite a broad range that's appropriate for children ages six to 12. Now, we're going to be developing other areas in the future where the plans are well off the drawing board in the developmental stage to do a similar area for teens -- age 13 up to 17, so they will also have their special area. We always hand-pick the content that's appropriate for that age group whether it's news, education or whatever and I think that we all recognize here the value of this medium in terms of unprecedented opportunity for children to educate, to enable them to learn, to empower them to communicate.

I've had a lot of parents I've talked with that said my child won't talk to me at school or they're bashful, but when they got out onto AOL, they start to meet friends from around the world, they can actually be communicating and our big challenge is to continue to promote those positive benefits with millions of children, especially at that age. They are the ones that are going to be driving this medium in the 21st Century and making it truly a mass medium, but still we need to take care of these important children's issues, which are safety and child pornography.

COMMISSIONER STAREK: Just to follow up on the Web sites that are available on the Kids Only area, you indicated that with some companies you have partnerships with and work on developing content, and you cited that Nickelodeon was one of them, but in the CME study they pointed out and showed us on the screen here just before this presentation that Nickelodeon was in their view one of the worst and that it required tons of information and engaged in contests awarding prizes without any parental consent. So, www.nick.com would not be in the Kids Only area, the other Nick site would be?

MR. BURRINGTON: I need to clarify a little bit. We have what we showed you on our slide, there's Nickelodeon and what they do out on the Web, that's their site. What we can say is to the extent you're a partner with us, these are the policies that require you to link to our Web site, we are going to have splash screens that are going to pop up and tell kids to talk to your parents for example or get parental permission. I don't know if that answers your question or not, Commissioner.

COMMISSIONER STAREK: Specifically, you then have some sort of Nickelodeon site that's in Kids Only?

MR. BURRINGTON: Yes, that's correct. And then it is a -- in other words, there's the Nickelodeon Web page and whatever Nickelodeon chooses to do is what they do. They create content for us on AOL so you're going to be seeing Nickelodeon create content only available to America Online subscribers, in this case only available to those in the Kids Only area. But occasionally there will be links off out of the AOL swimming pool out into the Nickelodeon Web ocean in the Internet and in that case, we do have these splash screens and other policies that we've been putting into place to remind parents to tell kids you've got to talk to mom and dad.

COMMISSIONER STAREK: One last question on the Kids Only area I would like to ask about chat rooms. What if an adult pretends to be a child and sets up one of the screen names and pretends to be a child. Is there any way to verify that this child is actually a child and not really an adult?

MR. BURRINGTON: Again, Commissioner, you ask a very critical question. When you sign onto AOL, as I said, you need to be an adult to get that master account. Is it possible for people to say I want to be a nine year old?

COMMISSIONER STAREK: The adult signs on and then lists a child's name as one of the four screen users and it's really the adult.

MR. BURRINGTON: The great problem with this virtual medium as it is constructed globally with all computer networks all linked together is you don't know definitively the ages of people who are online. And short of us not knocking on doors, we don't know that. Now there are a lot of things we do in the Kids Only area. For example, we have that area staffed very fully in the chat rooms to make -- we're in people's faces in one respect. In other words, kids know and parents as well -- because parents are in the Kids Only areas with their kids a lot of the times, so we really rely on the sort of leasing program which frankly has been working very well.

Are there going to be occasional cases that are off the screen so to speak that are not appropriate? Of course there are. The way we deal with those is we have very tight cooperative relations with law enforcement. When we have information that somebody's in there posing as an adult in attempting to meet with a child or whatever information was reported to us or we discovered, it is immediately reported to law enforcement and we will prosecute those people.

I will say this, Commissioner, that in the last two years in fact I was very much involved with "Innocent Images" investigation a few years back. I think there's been a significant decline in the number of people, pedophiles, at least using AOL for that kind of activity. Are they still there? Of course they are. This is not going to be a perfect solution. But I think the message has been sent out loud and clear and we want people like that to know that we all know who you're talking to online, and it may very well be an FBI undercover agent. We want to scare the heck out of them because we don't want them and I think we've been getting that message out pretty loud and clear. And that's why we're seeing that kind of activity in our service drop significantly because they know they're going to get nailed.

COMMISSIONER STAREK: Thank you, very much.

MR. PEELER: Rob McHugh.

MR. McHUGH: Thank you. I'll try to be brief and if I skip any details, I'm sure you'll let me know. We developed a Web guide for kids called Yahoo just over a year ago and to understand the policies I think it's good to understand kind of the overriding purpose. It's designed to be a fun environment for kids, a place they want to go. Yet it's also designed to be a safe haven that parents and teachers feel comfortable having their kids come into. So they are serving two audiences, both parents and children and oftentimes their wants are at conflict. So when it comes to things like running contests and promotions and gathering information, we need to address both their concerns. We're currently viewing these screens out of time now that we have redesigned them and we're basically looking at doing a relaunch this summer. So a lot of what I can talk about that we've done could be couched in the context of what we are looking to do right now. We are again going back to the parents and the children to help in design as we did the first time. So, a lot of the decisions we're making are based on the info we get from them.

With regard to our policy for children's safety, we looked at it in several dimensions, one is how we advertise to children; two is the content we provide to children; and three is with regard to the privacy which we talked about today and which is really in regard to two areas; the gathering of the information and also our communication with children.

Our purposes for gathering this information are several. One is to just know who our audience is. I can tell you now we have 50 percent boys, 50 percent girls. I can tell you our age range. We also want to know how they use the site, what they like, what we should build up and what they don't like and what we should scrap.

And then the third area for gathering information is to provide communication back to the children. This is something that we got feedback from the start, that children are looking for this kind of community online. They don't want to feel like they're just acting as an individual. With that I can also tell you what we're not doing with the information we gathered. We are not doing any one-to-one marketing of services or products to the children. We're not using the information we gather to sell to any third parties and we're not doing any unnecessary spamming or using the E-mails to just litter them with like information.

So with regard to our approach to information gathering, our site is a free site. There's no subscription involved, no registration or information gathering is required to access the information on the site. The information we collect is basically in two categories of identifying information which would include a name and E-mail and the non-identifying, which would be more like preferences, their interests, things that help us understand who's using our site.

We never make any linkage between the identifying and non-identifiable, so we never publish or use in any way the names or E-mails in any regard with any preferences or any information we gather. We also make a distinction between the look and feel of the site on the pages where we are gathering anything that could be considered identifying. In that sense we want to make it clear that this is different than the site where they might be asked for their favorite movie or favorite TV show.

We want to make it clear this is an area where they need to get parental permission. It's also clear that this is a place that's optional and they don't need to give us information. We also have staff who are working on designing the text now that will identify -- spell in language that they can understand. We already have this in the parental section where parents can access it.

One of the things we do with the information is basically we just use it again in an anonymous, aggregate way just as I disclosed to you our breakdowns on the demographics. We keep the information secure on our service, the same as we keep the rest of our corporate confidential information. And the information can be deleted at any time by anyone who is interested in removing it.

With regard to the E-mail sent to children, we only send replies when appropriate. We have a section for E-back where children can tell us about things that are broken on-site which we want to know and suggestions they have. We feel it's important to give these replies because they get a sense that there is someone at the other end who is listening to them and that's encouraging. We only send E-mails to people who enter their names willing to receive the occasional newsletters or new announcements about sites that we're coming online with. All the messages come from Yahoo to our E-mail lists. So, it never gets in anyone else's hands and, as a result, we also have an easy system for everyone.

So, with regards to incorporating the parents' input into the site, we made a point from the start to work with them and they've been very encouraged to increase the level of community that we have on the site. They found that the responses they received from us to their children have been very encouraging and very empowering. They feel that when one of their children suggests something and they actually see on their site a thank you note from us, that does a lot more for them than their other alternative entertainment like watching TV. And also as a result all that we do on the Yahoo site, safety is at the core of it, so it's very important that we integrate that and in all aspects of our going forward on this. We're grateful to be part of the hearing today.

MR. PEELER: Do you get parental consent before you collect information from kids?

MR. McHUGH: We request parent consent, we don't require it.

MR. PEELER: How do you do that?

MR. McHUGH: We have a section on the screen that reminds them that we encourage them to get parental consent before submitting identifying information.

MR. PEELER: Are there logistical reasons why?

MR. McHUGH: Yes. A lot of the times the information they're sending to us is handled automatically and typically we send a reply automatically before anyone ever sees the information. For it to be handled by what we call snail mail now would be a big logistical situation. We really wouldn't expect anyone to register.

COMMISSIONER STAREK: What do you do with the information you collect?

MR. McHUGH: The information we collect on the site we use to look at what works and what doesn't work. The information about demographics we use also to let our advertisers know basically the age group of who's on the site and the gender breakdown. The information about their names and E-mails we use in a way that is basically what we call a community perception of the site and what we try to do is break down the areas that are of access to everyone which is most of the site. But for those who want this kind of communication, the only mail they get from giving their name in the mail to us is that they receive occasional information from us. That's their reward and if they don't want it they can remove their name at any time. The kind of information we would send them would be things upcoming on the site. There may be new sites being listed, there might be some new content basically giving them a heads-up, letting them feel they know something someone else doesn't.

MR. PEELER: The High School site, I take it, gives access to a number of other sites. Do you require that they all follow the same policy and practices you follow?

MR. McHUGH: No. We have a directory of other sites much as Yahoo has. Differentiation on our part is all of the sites within Yahooligans have been looked at by real people to make sure that they're appropriate for kids. We actually have a staff of people who review them based on the content inside and also check the external links to make sure that just because the site is listed in Yahooligans, it may link to another site that's inappropriate. So we actually check several levels down to make sure that they don't go through.

MR. PEELER: Is that checking for information collection or just for content.

MR. McHUGH: Content appropriate for the age group.

MR. PEELER: So these other sites could be collecting significant amounts of identifiable information?

MR. McHUGH: Other sites on the Web who have their own policies for gathering information, yes. We don't hold any covenants over companies that want to be listed in high school site with regard to their own policies.

MR. PEELER: Thank you and I think now we'll turn to Mr. Sackler.

MR. SACKLER: Thank you and, believe it or not, I'm glad to be back. Few things are more important than what we are here about today. Protecting children generally and specifically their privacy in the online world is vital. It requires special sensitivity, extra effort and extra safety guards. We obviously care about protecting kids and, from a very personal standpoint, because after all, among the 75,000 men and women who work for Time Warner, a huge number like a lot of you are parents too, who want to commend the FTC for bringing all of us together to think through this important issue. We're very pleased to be part of that. We also want to offer a special commendation to the FBI and what they're doing. We join with you in supporting as much as we possibly can.

Now I want to make a few points in general about what we're doing and then we've got a few transparencies that will illustrate what we're doing to try to improve the protection of privacy of kids online who are coming to our Web site.

I mentioned yesterday that, in general, we are going slow on collecting information from individuals. That applies particularly to kids. We're going especially slowly there. We're undertaking, again as I mentioned yesterday, an inventory of our nearly 200 Web sites. It's a painstaking process site-by-site, page-by-page. It's a work in progress, so in some cases we're still collecting too much information, or we don't have enough notice, that it's inadequate in some way. That is going to be fixed. We're working on it very intensively.

Now there's absolutely no transfer of any information collected from kids to third parties. That's even within our own company. We have a whole range of businesses. We don't transfer any of that information. We do not market to kids in the tangible world, only to their parents. That's all we market to. We are not and we will not market to the kids in the online world. We are collecting information in the aggregate to refine our sites in order to be able to continue to refresh them to make them interesting, educational and fun for kids.

And frankly, since we're in business to make money, it's to build brand identification and loyalty to our characters, our films, our publications and more. We do collect some personally identifiable information for things like editorial participation, like our letter to the editor kinds of things, opinions, contests, that sort of the thing. But we don't maintain files, we don't use that information in any kind of marketing way or pass it on, other than in the ways that I've just mentioned.

I want to emphasize again that beyond not marketing to children, we do not entice children and we do not again pass that information on. Now, what we do do is to post our privacy policies generally, and then we have special notices posted at all points of data collection for kids.

Here we have the SI for Kids home page. You can see there's a link there at the bottom to the Pathfinder privacy policy. That policy sets forth all of our concerns and restrictions with respect to protecting kids on issues like this.

This is something obviously called. It's Tube Time on SI for Kids and what we're doing is telling kids who are visiting that we're about to start a Saturday morning TV show coming to you on your local affiliate of CBS, so please be sure to tune in when we've got it. And we're telling the kids we may want them to even be on it. That's only part of what pops up on your screen. There's the rest of it.

You can see we ask for a limited amount of personally identifiable information there, the name, the age, the E-mail address, personal address and phone number. We put up a notice that asks the kids to talk to their moms or dads for permission before they give us any of that information. Then the notice is a work-in-progress, is slightly wrong. We say we need the E-mail address and phone number in case we need to contact you. We actually need the E-mail address and phone number to contact their parents and we're going to fix that notice. We're going to tell them that.

And we use that in order to be able to call the parents and say your child has expressed an interest in It's Tube Time, has been very creative in doing so, and we may want to have your child participate in this program, can we have your permission to do that.

That's why we need that information. We don't maintain the information over a long period of time and we will eventually just get rid of it. As you can see on that notice though, that's an example of how we want to have our notices all the way around our Web site where we are collecting information, where the language, the color contrast is designed to attract the attention and interest of children.

Go to the next slides.

This is a point of interest called Funny Photo and it illustrates the editorial participation that I was talking about as one of the reasons why we collect a limited amount of personally identifiable information. There you can see a sort of funny picture of Charles Barkley and we've asked the kids to submit some captions. As you can tell they're pretty good. And when they send us something that's good, we want to be able to put up their name and their age, at least their first name. That's one of our justifications.

Here's another one of our popular Web sites from D.C.

Comics. Kids visit this one a lot. This is the rest of the screen, there's the online privacy notice. When you click to that and move over one click, this is what comes up. And again we're trying to design a notice to appeal directly to children. We've also got information there that we are trying to attract the attention of the parents so that they can evaluate how they want to guide their children's online activities. At whatever point of data collection we may have in D.C. Comics, we will have a similar notice and when we get these notices complete, these too will be differentiated by color in order to attract the interest and attention of children.

So those are a few examples of some of the things we are doing. We do have a huge number of Web sites and we tried to hold this presentation down to just a couple of the most popular sites. We'd be happy to answer any questions.

COMMISSIONER STEIGER: Before we lose your wonderful assistant, could we go back to the very first page, the Web page.

MR. SACKLER: SI for Kids one?

COMMISSIONER STEIGER: Yes. Now, you mentioned there is a click-on area for the privacy policy. Questions have been asked about the effectiveness of needing to click on and go somewhere else to find out the privacy policy.

MR. SACKLER: Right.

COMMISSIONER STEIGER: If I were to click on Batomatic, for example, would I find a privacy policy or warning to kids for parental permission on that one? I'm trying to figure out how this is going to work. Or am I always going to have to click separately?

MR. SACKLER: I'm embarrassed to say I haven't played Batomatic, but I think we can now say that at least in Pathfinder that at every single point of data collection, there is a notice and it's of the kind with the format and the color that will stand out and advise kids that they ought to be sure to ask your mom and dad for permission before giving any kind of information to us or anyone else over the Net.

COMMISSIONER STEIGER: So you aren't relying on a general statement on some other site that they would have to go into?

MR. SACKLER: No, and we're going to go through all of our sites. That's why it's taking us some time because we want to be able to have that notice routinely anyplace we collect information.

COMMISSIONER STEIGER: Thank you.

MR. PEELER: And, again, the information you're collecting you're using for what?

MR. SACKLER: Just to refine and improve the sites. Are you talking about the aggregate information or PI (personally identifiable) information?

MR. PEELER: I guess personally identifiable information.

MR. SACKLER: No, we don't need personally identifiable information to refine the site. We use aggregate information and to make it more fun and interesting and attract the attention of the kids.

MR. PEELER: So, the personally identifiable information you collect, what do you use that for?

MR. SACKLER: That's for the editorial participation kinds of things. It's for contests or opinions. We don't use that information for any marketing or other purposes.

MR. PEELER: What happens to it after that?

MR. SACKLER: After varying lengths of time ranging from hours to weeks, it's gone. It's purged.

MR. PEELER: It's not assembled in any databases or retained?

MR. SACKLER: No.

MR. PEELER: Has Time Warner thought about what Dr. Westin's study seems to say, which is that a majority of the parents welcome control over even the provision of personally identifiable information for internal product development? Have you thought about ways that you can implement that beyond simply telling the kids that they should do it?

MR. SACKLER: Well, the product development is in the aggregate, so that's not a problem, I think, in terms of Dr. Westin's survey.

MR. PEELER: What about for the editorials?

MR. SACKLER: Well, on that one, I mean, we could eliminate it. I don't know how else -- what the other choices are.

MR. PEELER: I thought I heard you say, at least on one of them, where you were collecting information you go back to the parent and ask is it okay for your kid to do this.

MR. SACKLER: Well, yes, we are doing that, and I suppose we could do that for things like the editorials -- now I see your point -- that we could do that for things like the funny photo caption. But that really is a time-consuming thing to do and for a function like editorial participation, our view is that a notice should be enough, and if it isn't, I don't know for sure, but I would suspect some of our editors might lean toward discontinuing doing that, because it then becomes too burdensome for that particular function.

MS. RUSK: Do you know if any of your sites have chat rooms or bulletin boards? We heard this morning about the E-mail companies harvesting addresses, and I just wondered whether that's a possibility.

MR. SACKLER: First of all, we have no chat rooms anywhere that are aimed at children, our chat rooms are only for adults, and for those we do require registration and we give them a warning and we collect a fair amount of personally identifiable information. I know that there's a significant amount of concern about giving too much information, but there's also some concern the other way that with too much anonymity there's a problem that if somebody does do something that's untoward you want to be able to have the information to be able to trace back and maybe the fact that you have to provide information will deter some people who really don't want to be identified.

MR. BURRINGTON: I would like to make some clarifying statements just very briefly, if there's a moment to do that.

MR. PEELER: Sure.

MR. STEVENS: Being on the last panel at the end of day reminds me of a phrase I heard the other day -- that the mind can only absorb as much as the back side can endure. So given that, I'll try to make it brief.

For those of you who aren't familiar with DMS (Digital Marketing Services), we are a joint venture company of America Online who owns 70 percent of our company and the Martin Group who owns 30 percent. The Martin Group is one of the largest market research firms in the United States. With the Internet commerce and possibility of doing custom research over the Internet growing and becoming a reality, DMS was formed as the joint venture of AOL back in 1995, which puts us in Internet years at about a 14-year old company.

Internet years are often translated to dog years. So, that's exactly what we do. On behalf of Fortune 500 companies, we implement various marketing and market research programs and some quantitative market research programs. As director of research services, obviously I focus on the research side of the business and that's what I'm here to speak on today.

We have methodologies that we use throughout a variety of studies, but the one thing we do have that is consistent across the board are the guidelines, privacy and ethics guidelines, that we use internally at DMS. Specifically, I think Ruth is going to help me on some slides here.

Specifically in an area in America Online called Opinion Place, members come to do a variety of things. Actually, AOL Reward is another area that we just launched in connection with America Online in which it's basically a retention program. It gives members the opportunity to come in and earn an incentive for their time. They can earn points, and these points can be used to, for example, apply to your AOL fee. If you're a heavy user and you're on the $19.95 unlimited use plan, basically you can come in, you can earn 2,000 points and that pays for AOL's fee. And you can do a variety of marketing programs to earn points. Filling out a survey, this being a survey product, is one of the ways you can earn points.

Finally, a visitor comes into Opinion Place to earn these points. The researchers in the room are randomly selected from a variety of screening modules that we have out there. We could have 30 to 40 surveys. Obviously, you can't answer all the screening questions for each associated survey or you would take a 30 to 40 question screening before you even have the survey.

So, we randomly select or assign visitors to screening modules. Now, oftentimes we do research studies for marketers of children's products, services programming, and some of those marketers have been mentioned today.

If you go into Opinion Place in the screening process -- if you look at the slide -- one of the things that we ask you is which category best describes your age. Now, if you click that you are under 15 years old, we ask you two more standard questions, your gender and your zip code, which most children don't know. And then basically we say, "Thank you for participating, I'm sorry, but we don't have a survey for you today." Because we don't want to say, sorry, you're out of here the minute they give us their age because we're afraid they'll catch on and then they'll say, well, I'm older than I am.

However, if you're an adult and you say that you fall into an adult category, then you would get the next screen. You could randomly be asked is there a child in your household between the ages of 7 and 14 who uses an online or an or Internet service. That may be the age group that we're looking for. You'll see that that is the age group that we think -- you don't really want to go younger than seven because we're not real sure that they would, number one, understand a lot of the survey techniques and we don't know whether they would understand a lot of the questions, and we believe that over 14 a lot of 15 year olds are writing programs right now, so they know a lot more about their Internet use than their parents do (laughter).

So, if you click "yes," you would find the next slide, which says, great, would you grant them permission in a survey regarding, for instance, television programming? They must be available right now and you may observe them taking this survey.

Now, what's unique here compared to what a lot of other people are doing is instead of going to the child and saying, hey, will you please go get permission from your parents to participate, we go through the parent and ask them if they would allow the child to participate, which is a little different. So, the option is, yes, I grant them permission, they are available, I grant them permission but they're not available, and I would prefer to decline.

So, if they choose that they grant permission and that the child is available, they would get the next slide. This is just so we have all of the editing and logic that you would have in any telephone interview environment. So, we say, great, thank you, there's a high probability we'll ask you to get them in a minute. If so, please assist them as needed but try not to influence their responses.

So we're encouraging the parents to observe their child taking the survey and assist as necessary. Sometimes a child, such as an eight or nine-year-old, may not be able to type on a keyboard as fast as they would like to and one of the things that we have found that when children type themselves it's funny because they are perfectionists (laughter) and sometimes they were taking too long. We have a four-minute time-out -- and if you have a question we don't want you to come in and have to go answer the phone and you be on the phone and it would time out. Well, these children, they were answering it, but it was taking them longer than four minutes because they wanted their responses to be perfect. So we have encouraged parents to assist as needed.

Then they would answer two to five other screening questions based on other surveys that they may have been randomly assigned to to see if they may also be qualified for them.

We work very closely with AOL who owns 70 percent of our company, so we monitor what's going on in the industry. I think that we've all seen today that there's probably a little bit of a difference between the level of hype and the level of reality and I think that every day we're bringing that closer and closer to parity there.

In Mr. Westin's survey -- I think that's great -- I think it's very valuable for projecting against the general population. One of the things that I think that is being done a little bit differently is, for instance, not all marketers want to talk to all people, they want to talk to their target. So, when you talk about online privacy issues and online ethics issues and parents' attitudes with their children using an online service, I think that the attitudes and opinions of the people who are currently online -- we, anyway, consider this to be a little more -- I guess you'd say valuable -- but a little more relevant because they're a little more educated in their opinions, because they have been online and they know what it's about. There's not that fear of the unknown that sometimes -- and I apologize to the media representatives here -- that sometimes the media generates.

We, hopefully, have taken that a step further by monitoring not attitudes and opinions but behavior. And, hopefully, this next slide will address that a little. This is kind of a flow chart of the process that I just described to you. We went and selected a random selection of people who responded to the screen, N=2,166 here. We just did it in integrals with a maximum of 200 from each day. And it kind of walks through the process.

AOL currently has -- well, 48 percent of the AOL households have children in the household. You'll see that coming through, the first question: Is there a child in the household? Do you use America Online or Internet service? That in our sample, 19 percent said, yes, I do have a child between this age group that does use the online service.

Okay, great. So looking at that 19 percent as the whole, as the people that we would want to talk to about their opinions of their child in this age group participating, would you grant them permission to participate in a survey regarding children's programming, for instance? They must be available right now but we encourage you to observe them when they take the survey. Sixty percent -- this is a little different than Mr. Westin's report -- said they are available right now and I do grant them permission to participate in the survey.

Thirty-seven percent said, yes, I would grant them permission but they're not available; 3 percent simply said I would prefer to decline their participation. That's a little different -- that's 97 percent saying, yeah, I would grant them permission, with 60 percent saying they're here and I'll let them participate.

MR. PEELER: Craig, just a point there. I think what Dr. Westin's survey is showing is the concern about children doing it without parental consent and what your numbers are reflecting is at least you're asking for, at least in this environment, that the parents are comfortable.

MR. STEVENS: That is correct, that is my point, and that's what is in Dr. Westin's survey and I think it is very valuable in pointing out the general population, their attitudes and opinions about that. What we have done is we have gone beyond the general population, we've narrowed it down a little more to those people that are online and even gone further to measuring up not only the attitude and opinion but the behavior which gets a little more specific.

But I think the reasons for this, I think Bill -- he's right on target with a lot of that -- AOL is rapidly gaining the respect and popularity of parents as far as letting their children use the service because of the tremendous strides that AOL is taking to ensure the protection of children online.

Again, 48 percent of the households that are AOL households have children. I think the analogy that Bill used is accurate, one that I've kind of used to communicate the same thing is if you think of a castle with a draw bridge -- well, within the castle is AOL and the walls and the content are there and there is a tremendous amount of activity in content -- information and a lot of attractive things inside -- the draw bridge being the gateway to the Web. And that's exactly the analogy that Bill has used.

AOL has the ability to say not only, well, we're not going to lower the draw bridge for you to get into -- get out of the castle and get into the Web, but we have the ability to lock the doors within the castle, too. You don't have access to this. But you can have access to certain doors within the castle, certain areas that are -- that are deemed appropriate for children.

I think another reason is perhaps our own guidelines which hopefully the next slide will demonstrate. For those of you who can't read those, first and foremost we have obtained parental consent for the child to participate, no marketing or promotional overtones in the research. We also monitor the questionnaire length, we work with our marketers that we do those surveys on behalf of. And they come to us sometimes with extremely long survey requests and we're like, no, this won't work in this medium.

So, limiting the length of survey is very important. We don't want to even address certain topics, such as race, household income, marital status or parents, religion, relationship with other children, relationship with parents, grades and schools, family illnesses, things like that that maybe could potentially upset a child. We don't want to get into those things -- into their mind -- and we certainly don't ask personally identifiable information such as their name or screen name, their physical address or E-mail address or their phone number.

All data is provided and analyzed on an aggregate basis. We tabulate it on an aggregate basis and we present it on an aggregate basis to the sponsors of these surveys. And then finally some are more of the user issues, try to limit the number of open ends for the typing issue, use graphics when possible, especially for aided recall because sometimes a child may not remember something if you use a textural question. Instead, with this medium, this multi-media, we can input graphics into our surveys and we can say that, yeah, we visited this area on AOL. It could be the Kids Only area, it could be an area within the Kids Only site.

And, finally, the last one is pretty easy for you -- pretty easy for us over at DMS, and that's to try to think like a child. What that means is in constructing a questionnaire and the type of information which you're going to obtain and the way that it is presented, it means exactly that -- try to think -- try to put yourself in the shoes of a child that would be participating in the survey -- to ask them what best represents your gender -- I don't know quite what a gender was when I was eight but I knew I was a boy.

MR. PEELER: Can I get you to close up?

MR. STEVENS: Sure, I'm done.

MR. PEELER: Okay, thanks. Commissioner Varney.

COMMISSIONER VARNEY: I think it's obviously terrific that you try to get parental consent although you may have questions about how to do it and that all of the information is not personally identified and that goes a long way. And then you obviously, you know, companies are paying for the results of this research.

MR. STEVENS: That is correct and I hope they keep doing it (laughter).

COMMISSIONER VARNEY: That's right. But one question that I didn't have a lot of clarity on -- and you may have answered it most directly -- do any of you sell your lists of kids or E-mail addresses in any form or any capacity, ever, under any circumstances? Could you answer that one?

MR. STEVENS: No.

MR. SACKLER: No.

MS. CLARKE: No.

MR. McHUGH: No.

MR. BURRINGTON: No. This is really like that tobacco thing (laughter).

COMMISSIONER VARNEY: Now, here's the next question then -- that's great! How many are there two, four, five of you -- that's terrific! How many are there out there, more at the table -- 500,000, 5,000? I mean, you're acting responsibly. What do you think we ought to do about everybody elsewhere? Where are they? Why aren't they here?

MR. BURRINGTON: Well, if I may, Commissioner -- first if I may, just for the record, I made a couple of slight errors in what I said and as we said we always want to be very forthcoming.

COMMISSIONER VARNEY: Last year, the year before or (laughter) --

MR. BURRINGTON: Well, for the next year, actually. Just a couple of quick things for the record. One we said we're going to develop a new teens area and that really is just for teens aged 13 to 15 rather than 13 to 18. Again, to be accurate.

And the final thing is one that we talked about the linking of Web sites and so on and so forth. And I just want to -- it's a complex area and, you know, we have business relationships with some partners who have Web sites, but also there are people who we don't have, don't have any business relationships that we work with and so, you know, our challenge here is that we're trying as best we can within our area, we're cautioning partners to make them follow our revised guidelines, and most of them have been, it hasn't been a problem. There are some situations where that's not working and so we have some temporary fixes.

But this an all-important question and it gets to your question, too, Commissioner Varney, which is that this is like a sculpture and I hate to, you know, castles, resorts, I prefer the resort personally (laughter). But this is truly like a -- really like a sculpture and if you saw that sculpture wheel turning, it's moving so fast and increasingly there are more hands on that chunk of wet clay trying to figure this out and internationally as well, so it's a lot of hands.

And I think what we're trying to do is -- I hope I've demonstrated here and I know my colleague has, that when a problem comes up like spam, we try to get on it and attack it from a variety of ways. There are lots of different approaches we can try, and we're not going to get it perfect, but the important part is that we're on these things and we are trying different approaches.

For example, we're thinking maybe we'll send E-mails to parents if their kids do get into the sweepstakes. Some of those are more readily and easy to accomplish quickly, others are not. So we're trying to sort through those as well. But I think the great challenge in terms of how we capture the other folks -- and I don't think, you know, you want to invite 500,000 people here, but I think --

COMMISSIONER VARNEY: I don't think they would come (laughter).

MR. BURRINGTON: Yeah, right. As an industry leader and the largest Internet service provider in the world, we are building a global brand, we care deeply, as Steve Case said in his National Press Club speech -- we believe there's this incredible power in this global medium, and it is going to clearly be a mass medium. And we really do believe that we have a certain responsibility, and I think that our challenge is increasingly globally with other governments in doing what we are favoring is a self-regulatory approach.

And what we get from people back is, Well, where's the enforcement? How do you enforce that? And what we're running up against is anti-competition laws and anti-trust laws that we need to be modified to allow us to do some of these things.

COMMISSIONER VARNEY: Or -- and this is not a trick question -- is not the alternative if a majority of commissioners at this agency would agree -- which I have no idea whether they would upon consideration -- for the FTC to say Thou shalt not sell information about children. And I don't want to put you on the spot, but this is what you all are doing. I mean, would that be a reasonable position for this agency to take?

MS. CLARKE: If I might, one of the things that we haven't brought up in these last few days is the fact that while I believe that the number of kid sites done by companies is closer to the hundreds just because it's such a large amount of work, what we haven't talked about is the fact that there are thousands of kids personal Web pages where they themselves are putting their E-mail addresses, their full names, their home addresses, their telephone numbers.   And so for us one of the things that are very key is education, because we have to use the commercial sites to get out to the individual sites and just educate kids and adult parents, educators, what is actually safe practices on the Web.

COMMISSIONER VARNEY: Well, how would that be in any way in conflict or inconsistent with a straight-out prohibition against selling children's information?

MS. CLARKE: Well, I'm not familiar with a lot of the practices at the FTC and legal issues, but what I can say is for us what we have found is that education, again, is important because it's not often -- it's not only the companies that need to learn and practice right but it's the kids themselves. And we had to do a lot to let kids know what is safe and what is not safe.

You had asked earlier how do people get kids' E-mails. It's the kids themselves a lot of times that are publishing because they just don't know any better. And that's why it's important that there needs to be directives for companies but then for individual too.

MR. SACKLER: In the first instance, we, like everyone else, think that the best way to go is through a combination of self-regulation and technology, just like our colleagues at DMA and all of the other organizations that have come before you. But there's always some sort of the irreducable minimum of bad actors.

Now, I realize that none of us do or do we have any plans to sell, market, traffic-in or do anything else with personally identifiable children's information or children's information generally. But I hesitate, at least at the outset, to go to something like a sweeping prohibition against doing it in every single circumstance without kind of delving into are there some circumstances, with parental consent perhaps, where it would be something that could be done for some good purpose.

Now, if there were something, and I certainly -- we certainly have no proposal -- but if there were something out there from the Commission or the staff or one of the other parties that would focus on regulating truly bad actors in some way, maybe that would be a fruitful way to go. I don't have a specific for you, but if there was --

COMMISSIONER VARNEY: Not unlike the experience we had with you when we regulated two months ago.

MR. SACKLER: Not at all unlike it. And there have been a lot of other examples that this and other agencies have done over the years, but confined to the truly bad guys.

COMMISSIONER VARNEY: And do truly bad guys, in your opinion, include those people who collect extensive, personally identifiable information from clearly children without parental consent?

MR. SACKLER: I would hesitate to label them bad guys. It's a matter -- it was a matter in my own company of educating everybody, of having in incentive to say, Hey, wait a minute, what are we doing here? And are we collecting too much information? And, yeah, maybe we are.

COMMISSIONER VARNEY: All right -- collecting it without the parent's consent.

MR. SACKLER: And are we collecting it without the parent's consent. I think I would want to see who was educatable first, who could be incentivized, how well the technology might be developed and applied -- all of those things -- and then get at that residual, whoever that might be.

MR. BURRINGTON: Commissioner Varney, I mean I want to just echo what Art said, and I think that because this thing is evolving so rapidly and it's still so competitive -- and it really is -- is that what we're finding -- and certainly this is happening in other areas of children's-related issues, whether it's content or whatever -- is that if the market forces are so great right now, I mean, we're putting our money on the fact that we can be the most children friendly, you know, kid safe. We think that that, you know, over time there's going to become somewhat of this market pressure because we know that our members demand that. And Dr. Westin's survey, which I'm glad we did, confirms that a lot of parents have a big, big problem in this area. And the key is what's going to really, in the long run, be the most effective thing.

I -- I think that the Commission can promote the continued development of some of these technology tools, can partner with the industry and other groups on really getting the education message out there. I don't know what the alternative is here -- we can have a regulation that says, Thou shalt not whatever -- how do you enforce that? I mean how -- do you have people sitting at banks of computer rooms all day surfing the Net to find --

COMMISSIONER VARNEY: No, we get lots of complaints.

MR. BURRINGTON: Now, there are complaints and I understand that. But I think it's going to be -- it's going to be a combination of things here and then even if we do that here in the U.S. -- this is my deep concern -- what's the international approach? Because it's going to really be rendered almost meaningless. I mean, it will be good for all of us to say we tried something and -- but it's really going to be rendered almost meaningless when you start to look at this more globally.

COMMISSIONER VARNEY: But, on the other hand, you know as well as I do that the French Data Protection Registrar -- and I hope Jerry knows this -- when you go up in French language, the French Data Protection Registrar considers that you are targeting an audience of French people and he believes you are completely under his jurisdiction and he has and will prosecute you if you don't comply with the French data protection laws. Right now there's litigation involving several companies in France over that issue.

MR. BURRINGTON: But to the extent, Commissioner, we can have consistency I think that's the key area. We build a global brand as this is a seamless global medium that the consistency is the key to any of these solutions that we're talking about, including a regulatory one.

MR. McHUGH: If I could just follow on this. In terms of this being such a new media and you're constantly -- there are people trying to make analogies between this and other media, I think -- I think we need to constantly look at what kind of regulations we apply across publications and television and radio and telephone, and say that this should be no less stringent in that area.

But, as well, there's no place for people to hide on the Internet. If there are people who are doing bad things, people will know about it. And as we see with the spammers, the market in some way takes care of itself in terms of the -- you're not going to hear of anybody standing up and pointing to themselves and saying, I'm making a fortune collecting children's information and selling it.

So, the people who are doing it won't be on these panels and they won't be major companies spending a lot of money on Web sites.

COMMISSIONER VARNEY: I hope you're right.

MR. PEELER: Well, with that I think the hour is late, I have a couple of just administerial things to do first though. The first thing, panelists submit your visuals for the record. I would remind everyone that the Record remains open until July 14. We'll be meeting back here tomorrow morning at 9:45 to resume the discussion of children's issues, particular screening technology during the discussion.

I've also been asked to warn you that if you're not out of the building by 7:00 you will be spending the night here (laughter).

(The hearing adjourned at 6:00 p.m.)

CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: P954807

CASE TITLE: PRIVACY WORKSHOP

HEARING DATE: JUNE 12, 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: JUNE 19, 1997

____

JEANNE STUMM

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

____

DIANE QUADE