UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY

SESSION FOUR: DATABASE STUDY

Friday, June 13, 1997

Volume IV

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 9:45 a.m.

FEDERAL TRADE COMMISSION

I N D E X

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, Consumer Protection Bureau, Director,
Consumer Protection Division

Theresa Schwartz, Deputy Director of
Bureau of Consumer Protection

PANEL V: TECHNOLOGY AS A TOOL FOR ADDRESSING CHILDREN'S PRIVACY ONLINE

"How effective is technology in addressing online privacy concerns relating to children?"

PANEL VA: Software Filters:

Jeffrey Fox, Assistant Editor, Consumers Union

Susan J. Getgood, Director of Marketing, Cyber Patrol, Microsystems Software, Inc.

Robin Raskin, Editor in Chief, Family PC Magazine

Gordon Ross, Chief Executive Officer, Net Nanny

PANEL VB: Application of the Platform for Privacy Preferences "P3":

Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology, Internet Privacy Working Group (IPWG)

PANEL VC: Digital signatures/certificates and biometric technologies: Mechanisms for Obtaining Verifiable Parental consent:

Michael Baum, Vice President Practices & External Affairs, VeriSign, Inc.

Tom Carty, Vice President Business Development & Marketing, GTE CyberTrust

Gordon Ross, Chief Executive Officer, Net Nanny "BioPassword"

P R O C E E D I N G S

MR. PEELER: Welcome to the fourth and final day of the FTC Privacy Week. Thank you all for coming. And to begin our session today, we are fortunate to have Commissioner Starek for opening remarks.

COMMISSIONER STAREK: Good morning and welcome to the fourth and last day of the Privacy Week at the FTC. Today we will conclude, and I would like to just say something about what an outstanding professional job the staff that put this hearing together has done. I would like to congratulate our staff who worked so long and hard to put these hearings together. Thank you for such a terrific job. I especially would like to thank David Medine and Lee Peeler for chairing the hearings. Some of you may know I chair a committee on consumer markets, and I am required to lead discussions similar to this for a day at those meetings. I'm exhausted at the end of that day, and an OCD day is only six hours, so special congratulations to David and Lee who have done such an outstanding job.

Today we are going to look at some of

the most interesting issues about protecting children's privacy online. First, we are going to hear about the effectiveness and availability of various types of technology for protecting children from data collection that is not authorized by their parents, and about mechanisms for obtaining consent from parents or other adults responsible for supervising children. It seems to me that the attitude surveys discussed yesterday revealed the desire of parents to be empowered to be parents on the Net: to keep their children safe, yet to be able to give them the best, especially the educational benefits of the Net. I look forward to learning more today about what technologies are available to help parents be parents in cyberspace.

Second, we are going to hear about the self-regulatory efforts, including how they are currently working, ways to enforce self-regulatory codes, and their costs and benefits. In assessing regulatory solutions, I would be very interested in learning how much content for children, and how much variety, there will be on the Net without some form of commercial incentive to provide it, especially to

1 persons that may not be able to afford user or
2 subscription fees to access particular
3 educational sites.
4 Now, at the same time, extremely
5 serious concerns were raised yesterday about the
6 ability of predators to access and use children's
7 information to harm children. Now, clearly, this
8 is an area where there is a compelling need to
9 assess whether the current tools for protecting
10 children are adequate and how they can be
11 improved.
12 So appropriately, this session is going
13 to close with a round table discussion with
14 representatives from consumer and privacy
15 organizations, industry and government about the
16 likely success of self-regulation and technology
17 in responding to calls for privacy protections
18 for children. The round table will assess the
19 preceding panels on technology and
20 self-regulatory proposals and how effective these
21 approaches are likely to be. And finally, I
22 think most importantly, we want to hear the
23 panelists' views on where we go from here. What
24 steps should be taken next? What should be the
25 role of government? What is going to be the role

of government, if anything? What should the FTC do?

Now, after thinking about the discussion yesterday afternoon, I think some may have been misled about what this agency will undertake. When the panelists debate the proper role of government, I think it's important to keep in mind exactly what the FTC can and cannot do. We can pursue deceptive practices, such as a false representation that a site will only collect information for one purpose when, in fact, the site is using the information in other ways. We can't initiate enforcement actions against violations of an industry code unless they are also violations of the FTC Act or another statute that we enforce. The FTC Act's deception standard asks whether the challenged representation or practice is one that would likely deceive a consumer acting reasonably under the circumstances in a material way -- that is, in a way that affects the consumer's conduct or choice regarding a product or service.

Now, we can also challenge unfair practices under the FTC Act -- those practices that are likely to cause substantial injury to

consumers when that injury is not reasonably avoidable by the consumers themselves and is not outweighed by countervailing benefits of the practices to consumers or competition.

As we discussed yesterday, the collection and dissemination of personally identifiable information from children could expose them to being targeted by sex offenders. Now, in theory, it may be possible that some forms of collection and dissemination of children's personal information, without adequate safeguards, could successfully be challenged under the FTC Act as unfair practices. Attempts at rulemaking based on theories of unfairness, however, deprived the agency of a Congressional authorization for 14 years and I do not think anyone wants to make that mistake again.

Beyond rulemaking, guidance, and enforcement based on the FTC Act or other statutory authority, the Commission can study issues, as we are doing with these hearings; make recommendations, if appropriate, for legislative action; and encourage and participate in consumer education. We cannot and should not dictate the form of your self-regulation, or attempt to

1 regulate by threat of Commission action in areas
2 where we lack authority. To do so needlessly
3 risks stifling your innovative efforts, not to
4 mention having someone point out that the Emperor
5 has no clothes.
6 Don't get me wrong, I certainly support
7 facilitating your discussions and encouraging you
8 to come up with ways to avoid unfair or deceptive
9 practices or violations of the Fair Credit
10 Reporting Act. I just think we need to recognize
11 the limits on the FTC's authority in the privacy
12 area.
13 Now, although it's been a long week,
14 it's also been a very beneficial one. There have
15 been candid discussions of a wide range of
16 issues. We have learned and we will learn more
17 today of the continued rapid developments in
18 information collection, technology and
19 self-regulation. The panelists in this
20 proceeding and others who filed comments have
21 provided us with a rich record to review. In my
22 view, this is exactly the type of process that an
23 agency like the FTC needs to have available in
24 considering its role, and I want to thank each of
25 the panelists for his or her participation. Not

just the FTC, but also the general public and the industry can derive real benefits from timely discussion of the complex issues involved in online privacy. Thanks.

MR. PEELER: Thank you, Commissioner Starek. Our first segment today will discuss the availability of software filters and their use. We have four panelists who will be participating in the first segment. The first is Robin Raskin. Ms. Raskin is the Editor in Chief of FamilyPC, a magazine that helps parents raise kids in high tech times. Ms. Raskin will present the results of a FamilyPC poll that indicates that parents are concerned about privacy issues on the Internet and interested in a simple, transparent and built-in system that lets them safeguard their children without having to master the technical jargon in the Internet market. Ms. Raskin.

MS. RASKIN: Thank you for inviting me here. As he said, I'm Robin Raskin. I'm the Editor in Chief of FamilyPC. I was formerly the Editor of PC Magazine, so I could decide to come here today and talk to you either as a technology expert or as a representative of parents. I

chose to come and talk to you as a representative of my readership, who are parents. They are concerned parents and what we call active computer users in that they have made a commitment to care enough about their children and technology to subscribe to a magazine about computers.

So FamilyPC is lot different than most other magazines in that we have family testers. There are no experts and labs reviewing software. We have 4,000 family testers who live around the country, and they weigh in on issues in the form of questionnaires. They review products for us, and when a product receives a rating from a family, it's the family seal of approval.

When we started the magazine in 1994, there basically was no consumer Internet. There were a few online services just beginning to talk to the consumers on a mass level. So our readers have had to learn a lot very quickly. I'm going to share a little bit about some of the things that parents think.

I think number one, and I think we have to say it, parenting is a tough job at any time. Parenting is an especially tough job in high tech

1 times. And I think that a parent's job is not to
2 make a decision once. It's to make a decision
3 and evaluate it and reevaluate and reevaluate it
4 again, depending on a lot of things. Depending
5 on your individual child and what they need in
6 terms of you to play a role. Depending on their
7 age, and so we can't lump kids together, because
8 an 11-year old is very different than a 4-year
9 old kid, and depending on the situation. A child
10 in school is very different than a child at home,
11 and I think that the Internet will be
12 situationally different at various times.
13 I think that parents have come to the
14 realization that being a parent in the '90s means
15 giving up some personal privacy in a lot of
16 ways. I think they know that when they go to the
17 grocery store. I think they know that when they
18 go to the ATM machine. I think parents realize that
19 that is the case on the Internet, and it's
20 sobering.
21 I think the question now, and having
22 not been here for the last days and watched the
23 papers and talked to parents, the question now
24 that parents would ask you, if they were here, is
25 how much is real, and how much is conjecture and

1 what if? And that is not to say that conjecture
2 and what if and proactive behavior are bad. I
3 think we should be sitting in this room talking
4 about what could happen if this scenario played
5 out? I think it's very important to relay to the
6 public that that is what we are talking about.
7 We are talking about this is what could happen,
8 versus this is what does happen.
9 I think that parents want a safe
10 community but they have an order of priorities to
11 make that community safe, and I'll tell you what
12 I think our families believe in a moment. I
13 think they want control, but you have to ask how
14 much nuance and detail they are willing to accept
15 in their already very crowded lives. And the
16 best sound bite I can give you on that is to say,
17 do they want to fill out a 10-page personal poll
18 about their cookie preferences or do they want to
19 check off boxes that say I want to be safe, I
20 want to not be safe? There are a whole bunch of
21 interim steps between that.
22 I think that people also have to
23 recognize that a good Internet service demands
24 personalization and personalization demands
25 personal knowledge of what you do on the

1 Internet. I personally am gratified every time
2 Amazon knows what book I like and they tell me.
3 They know my reading preferences, they know when
4 a new author comes out and they are there for me,
5 and I like when Microsoft Expedia is doing fair
6 tracking information because they know exactly
7 where I'm going next week. Those are personal
8 preferences that I've chosen, but understand that
9 to make good services on the Internet, you must
10 have profiling information about your audience.
11 And that is one of the greatest things the
12 Internet can provide.
13 I also think that -- I'm going to take
14 a stab here -- I'm going to say that there is an
15 inherent danger when you talk about kids, and we
16 all know how highly charged and emotional the
17 issue is. We all know how vulnerable our children
18 are, but we must be careful that we do not use
19 our children as a ploy to enforce any adult
20 regulation. And we must clearly, when we talk,
21 separate kids' privacy issues versus adults'
22 because they are very, very different.
23 So at FamilyPC, we survey families
24 fairly regularly, about twice a year, how they
25 feel about various Internet issues. We have a

new study coming out in October. I'm going to take you to February of 1997 when we talked to 600 families. And what we found was that 62 percent of parents said that they have some form of rules at home for when their kids were on the Internet.

If you look at the Jupiter research report, they talk to kids. We talked to the parents. Jupiter reports 46 percent of kids saying that parents limit their time online; 45 percent saying that parents limit the sites they visit. I think our parents in particular, when you look at FamilyPC readers, you know that they are very engaged and active in computing, so FamilyPC readers are going to be more diligent than perhaps the rest of the population, and that is where some discrepancy comes from.

I also think that no matter how you look at it, if you look at the flip side, half the parents are not monitoring usage at all. When we asked who used blocking software, 25 percent of our readers reported that they use some form of blocking software for their children on the Internet. When we looked at those who use Microsoft Internet Explorer alone, that number

jumped up to 43 percent. And that clearly told us that there is a higher adoption of blocking software when controls are built into the browser and free of charge.

When we asked about chat, we found that 71 percent of our testers would not let kids chat. We think that that number has come down some. You will see that in October, that more people will let kids chat. We think this is due to the graying phenomena of our audience -- as kids get older, they chat. 52 percent said they were not concerned with Internet marketing problems. I think that number will go up. Part of the reason that number will go up is because we are sitting in this room today. And part of the reason that it will go up is because there will be an increased awareness. So we have to ask ourselves, if parents are not concerned, is it because we are playing it out of proportion or is it a lack of awareness. That is an important question I think we should keep in mind.

When we talked about content, things got different. While parents weren't concerned about privacy and marketing on the Internet, they were very concerned about content: forty-eight percent felt

that content should be regulated. Clearly, content, not privacy, was first and foremost in their minds.

Now, I'm not going to give you FamilyPC data. I'm going to be very clear here that this is an editorial opinion. I think that industry-initiated technology solutions are the fastest and best solutions that we have right now, and we need speed and we need to be able to react quickly as experts. I see the government's role clearly as a call to symbolic gesture, but I don't mean to take that lightly. I think the threat of legislation is a catalyst for very important things happening, and that threat has been a tremendous catalyst in what has gone on so far.

Now, let me talk about blocking software for a moment. Does blocking software help? I would say that blocking software is a good first-generation solution. It has done an adequate job of providing a moderate degree of protection, and I think in these times that is really saying quite a lot. I take issue with people who say that blocking software is no good when the statistics show that it does more than half or 60 percent of its job. I think blocking

software is an effective tool, so it's a matter of how you feel as a parent. All you can ask for are good tools.

But on the downside, blocking software requires parents to have a lot of time, effort, money and savvy about what they are doing. As a matter of fact, what I hear from parents most often at FamilyPC is the amount of time they spend overriding the block so the kids can get to the sites that they really want to see. For example, with Amazon, I wrote a column called "Best Stoppers." It was the first piece I wrote about the software. It was blocked by every single package. There you go.

I also think parents need to be very sensitive about the nuance. If you walk out on the street and you ask somebody whether it's a rating system or a filtering system, guaranteed they won't know, and we have not helped ease that confusion. I think that what you are asking a parent to do when they install a piece of blocking software is to understand first, various parts of the Internet -- World Wide Web versus chat, versus news group, versus mail server. You are giving parents a blank palette and

1 saying what do you want to disallow
2 your children to see when you have no idea.
3 You are asking parents to constantly
4 refresh a where-not-to-go list in some way or
5 another. You are asking parents to understand the
6 subtleties of a rating system, like what is the
7 difference between a mild expletive and a strong
8 expletive, who is the rater that created that
9 system, so you are asking parents to be incredible
10 experts in a lot of things.
11 I would argue that parents, while they
12 are -- many parents will be ready for that level
13 of detail at some point, not all are ready now.
14 To make blocking software better, and I think it
15 will become better, I think it should be built
16 into the browser. I think there should be a
17 quick override access: One password from a
18 parent to get into blocked sites. I think there
19 should be routine background updates and a
20 standard for rating and filtering that is widely
21 recognized.
22 I think more importantly, and something
23 that can really come out of these sessions here,
24 is that blocking software can help with privacy
25 issues by educating people about the hierarchy of

1 privacy issues. Junk mail and stalking are not
2 the same thing. But they are being talked about --
3 mostly in the press -- as the same thing, and
4 the solutions that we're coming up with are
5 treating them all as the same thing. I sort of
6 gave a hierarchy of junk mail, inappropriate
7 chatting, deception, selling of lists -- I
8 believe a kids' list should never be sold
9 anywhere, no way -- frauds and scams and bodily
10 danger. And I think there is a big difference
11 from top to bottom in that list that we must
12 remain cognizant of.
13 I think people who were here the first
14 days of the session heard about a lot of other
15 emerging solutions. I think generation two shows
16 a lot of promise. I think you are seeing the
17 beginning of consensus, that people want to be
18 notified and they want their consent. They want
19 to basically have a system where they can refrain
20 from having their information used, have it used
21 on one site, as I mentioned with Amazon.com,
22 where it's been very helpful, or have it used
23 intrasite and, typically, that will involve --
24 you can probably be apprised when there is some
25 monetary compensation.

Then I think the other question that we need to resolve is where the protection lies. Once you know what the protection is and what it should look like -- should it be at the site level, in the browser level, or at the server level. I think that is situational dependent, and I think that there will be hybrid varieties of those solutions.

Technology solutions are great because they let us stay current. They become standards without lengthy ramification, and they are created by experts with a deep understanding of the issues. On the other hand, they are created by experts with a deep understanding of the technical issues and not the consumer issues. They tend to focus on the issue of the moment, and I would point out that we haven't really had closure on the technical side to the content issue, yet we are marching forward on privacy issues. So if I had to recommend things, I would say technology can provide the answers provided we ask the right questions, and I urge everybody to work with real parents and real children in any solutions that they come up with.

I think we must separate content and

privacy issues in the consumer's mind, and we must make sure there is no premium price put on safety for the consumer. I think we need to create simple binary choices in the beginning. Having words come up like, you are entering a secure server, or, you are about to give up your cookie, is not an appropriate level of protection for most consumers. Building client level blocking software is another important thing.

And I would say, look at the movie industry for a simple paradigm. PG and R, when you go see a movie, does not tell you everything about that movie, but it gives you a feeling that somebody, and most people don't know who that somebody is who is doing the rating, somebody out there has looked at this movie's content.

I think on the Internet we have the wonderful ability to drill down and say, if you want more nuance, if you want more detail, click here, and we will tell you whether it's explicit violence or frontal nudity, but make that first entry simple because until you understand the metaphor, you are in no position to drill down to the nuance.

I just urge everybody to remember the flip side of the issue. While the Internet is a very scary place in terms of privacy, I think it also opens up some amazingly quick doors to taking action against violations of privacy. If you get a postal scam in the mail, some letter that tells you something that you don't trust, it can take you weeks to get through that. If you go on the Internet with any junk, scam or fraud mail, there is a pretty good chance that within 24 hours you will have a full detail between blacklisted sites, between chat groups.

We are quite good at self-policing, and I think there is a lot of economic incentive to act responsibly. I would go so far as to say Internet service providers will be able to use the fact that they create secure, private environments as an enticement. Thank you very much.

MR. PEELER: Thank you. Our next presenter is Jeff Fox. Mr. Fox is the Senior Editor for Consumer Reports magazine. He has spent over 15 years in software development dating back to 1972. He will discuss what the three major software filters right now can and

1 cannot do to block children's personally
2 identifiable information.
3 MR. FOX: I would like to thank the
4 Commission for giving me the opportunity to help
5 in this process. I'm one of those souls that
6 have been sitting here for the last three days.
7 I think I've learned a lot myself over the last
8 couple of days, and although I came here to talk
9 about the existing products, after
10 yesterday's session, I think it gave me some
11 additional things to say about how we can solve
12 the problem -- how the process can be improved and how
13 we can look towards the future and not simply to the
14 present. I do want to mention there is
15 going to be a demo later of future
16 technology. It looks as if that technology
17 probably won't be widely available perhaps for a
18 year or longer. So the present products, while
19 they will eventually disappear, are probably what
20 people are going to be living with for some
21 time. So they are still relevant.
22 I want to start with a prediction
23 here. This is a prediction I'm absolutely
24 certain of. Blocking software will never be able
25 to protect children's privacy unless parents use

it, and that is really something that became apparent yesterday. It's not just a question of how effectively the products block. Even the most effective blocker doesn't block anything if the parent isn't installing and using it properly.

So what I would like to start with is a look at what we have on the market now, which I will call the first generation of blocking software. We first tested these products a few months ago when we looked at how well they blocked access to Adults Only X-Rated type sites. In that case we found that they weren't totally effective, but they were pretty good.

The three products that I looked at for these hearings were three of the four that we had tested that do have a privacy protection feature by which a parent can actually attempt to prevent a child from typing in things like a name and address. Here is a look at some of the problems, situations we have with the existing technology. As we saw yesterday, these products are not that widely adopted yet. Only a relatively small -- I point to the statistics,

1 and I think that Robin kind of confirmed it again
2 -- that still a fairly small percentage of the
3 online parents are actually using blocking software. And
4 remember, these are available free to all
5 subscribers through American Online, CompuServe
6 and Prodigy.
7 You would think with a product available for
8 free, everybody would rush and get it. There are
9 some possible reasons why people might not do
10 that. We have also found that these products are very
11 hard to find in stores generally. I found from my
12 experience with them, that they sometimes can be
13 tricky to install. They can conflict with
14 perhaps your other Internet software or online
15 service.
16 Sometimes some of them can be hard to
17 use, as Robin pointed out, with all the things you
18 have to master. Some of these screens are fairly
19 complex, and they can be a bit daunting to a
20 mother or father who is sitting down for five
21 minutes, at 1 o'clock in the morning trying to
22 master them when the kids are sleeping.
23 Also, I have to point this out. This
24 is an issue that has arisen on the Net, that
25 their smut-blocking policies may be turning some

1 people off. I don't know what percentage but
2 they are developing -- there is a buzz on the Net
3 about these products and some questions have been
4 raised about whether they don't -- some of these
5 products will not let you look at the list of
6 sites that they block, and in some cases you can
7 add to those lists. But if you can't see those
8 sites, you feel like you are kind of stuck with
9 what they are handing you, and there are some
10 cases of blocking sites that many people would
11 consider legitimate sites. I'll show you an example of
12 somebody online who is really ticked off at
13 that.
14 The tests that I performed, the next
15 point is that these products are not that hard to defeat.
16 I know the manufacturers may disagree with my
17 assessment, and I hope that we don't have to get
18 into a real argument about this because I think
19 we are looking more towards the future.
20 I want to clarify something because
21 sometimes these findings get reduced to a sound
22 bite, and I'm not saying that these products don't work,
23 that they don't block. I'm simply saying that
24 the security could be quite a bit better, and I
25 think I've learned now that the approach that is

being taken is possibly not the best approach to begin with, and I think the manufacturers are probably coming to agree with this.

I was speaking with one of the manufacturers before the session, and I think we agree that the kind of approach that is called P3 (Platform for Privacy Preferences), that we will talk about later, is probably a better approach. So we may be just arguing a moot point if we argue about whether you could tighten blocking software a bit.

Also, on the Web, these privacy features are remedial. They try to block speech rather than access to a site. As we saw with the E-mail issue, junk mail issue, blocking speech is problematic because whenever you try to block "bad speech," you always run into the issues of how to preserve good speech. It's absolutely true even when you try to block kids because if you try to prevent somebody in a chat room from asking a kid what is your name, what is your address, you block the words name and address. If you block enough ordinary words in the English language, you make it impossible to hold any kind of meaningful conversation. You can have that problem when you are trying to censor kids.

Other problems -- the burden right now is

1 on the parent to install and maintain the blocking software.
2 Also, the parent solutions don't put any responsibility
3 at all on the commercial Web publishers. I don't
4 think that type of burden should be on the parents.
5 Let's take a quick look at the existing
6 -- this is the Cyber Patrol privacy blocking
7 screen where you enter some of the names and
8 phrases that you want to prevent your child from
9 typing in. And on the right is a place where you
10 can add another 26 or so additional words or
11 phrases, so this is actually from my test
12 that was performed about three or four weeks ago,
13 and the sample that I used for most of my tests
14 was totally fictional, Lois Lane, residing in
15 Metropolis. I found out that in some
16 cases, when I attempted to go to Web sites, that
17 the zip code didn't match with the state, so in
18 some cases, Web sites actually gave me some
19 problems over the zip code. In some cases I had
20 to fudge it.
21 I'll just show you very quickly, here I
22 am at the KidsCom site. If you look in the lower
23 left-hand corner, you can see me beginning to type
24 in the name Lois. I typed in L-o-i. This is
25 where it asks for the first name, and Lois is one

of the words that was blocked.

Next slide, this is still Cyber Patrol. You notice when I typed the S, it was X'ed out. That is basically one of the ways that these products work. They will erase the characters you type or just replace them with X's. So that is an example of actual blocking at that site when I attempted to type the name.

If you look at the next screen, all the products are pretty much bound to looking for exact matches, which means that even slight variations are not easily caught. In this case, I inserted an X in the name before the S, and so far it has not recognized that. If we go to the next screen, I then go back and delete the X, and at this point it does not recognize the presence of Lois because I didn't type it as L-o-i-s. The fact that I inserted a character was enough to kind of throw it off my trail. And now I've actually typed in the exact name that was prohibited. This is what I would call an undisguised plot phrase. This is where there was not even any attempt to really disguise the phrase. It's just kind of a little typing trick.

If we go to the next slide, we will see, for example, that when I went to a site -- I don't think you want your kid going to the Old Tap Room Beer site -- I was able to enter the name, E-mail address and my city and state. Basically, I skipped over the sequence of inserting the extra characters, but that is how I got them in there.

On the next screen, I'm going to take a very quick look at one example using Net Nanny. This is the Amazon Bookstore site. If you look just to the left of that box in the center, you will see where Lois Lane was once typed. At this point Net Nanny puts up a warning. It has erased it. That is an example of effective blocking.

On the next screen, you will see this is the end of my placing an order, assuming that little Lois wanted to go out and buy a lot of copies of Winnie-The-Pooh for all her schoolmates, and she managed to get hold of her parents' credit card. Here she is ordering 21 copies of Winnie-The-Pooh. I didn't use a valid credit card number to get through because they check your credit card number. If you were going to a site that wasn't using credit cards, you wouldn't

be able to type in the name and address information.

Moving on to the next slide, this is Cybersitter which I found somewhat better at blocking, in the sense that it didn't rely on checking your typing. Cybersitter monitors what you are actually sending out in the Internet. So here I set up Lois' friend Lana Lang. That is the setting in Cybersitter for blocking.

Move to the next slide. Here is my order, again, 20 copies of Winnie-The-Pooh for Lana. Again, you can see I got Lana Lang in. If you look closely at Lana Lang, I put a period between Lana and Lang. Cybersitter was a little harder to trick. I had to actually leave something else in the phrase so that it wouldn't recognize the name, but as you know, it's not very much. That name and address is still pretty easy to recognize. I suspect a lot of Web sites, particularly if you weren't actually ordering something, would have no problem cleaning that up or even leaving a name and address like that in a database.

So I have to resort to that because, as I say, Cybersitter actually does scrutinize what

goes out to the Internet. The other two products appear to rely entirely on monitoring the keyboard or the screen which I would liken to stationing a security guard in a store, not by a door but in another department of the store. You really need your security where stuff goes out. Not in the middle of a store.

A quick look, we heard yesterday about parents having some hesitancy or problems reading the software. Here is a look at CompuServ's parental control form where people are discussing Cyber Patrol. That is the product that is available for free on CompuServ, so they are not discussing the other products here.

I don't necessarily say that everybody that uses the product would have problems, but these are indicative of the kind of problems some people experience who are actually using the product. You can have problems like this. And it's good to see whenever people just throw around, This is a great software; it does this, it does that. The reality is you sit down at the computer and start to get into DLL files, and all kinds of technical things can come up that many parents won't have a clue about.

Moving on to the next one. Here a second person who responds to the first person, had the same problem. Called the manufacturer, got finger-pointed out to CompuServ. I'm going in circles. How do you fix it? Not everybody, but this can happen to people. It can be very frustrating. I'm sure some people have had this problem, perhaps with larger software companies.

MR. PEELER: Jeff, two more minutes.

MR. FOX: One more slide and then I'll come to my conclusions. Here is some of the advice given by the manufacturer, to give an example of the kind of technical things that people can get into, always kind of technical files.

Some suggestions for what would make blocking technology more useful, more widely used, and much more effective: I think I agree with Robin. The only way you are going to get most parents using this kind of technology -- I don't think we can go make them track it down, download it, go out to stores, try to find it -- it's got to be there just like Windows or the operating system. I think it should be built in.

1 Preferably built into the browser and then
2 everyone's got it. Also, building into the
3 browser strengthens the protection
4 capability and eliminates a lot of these
5 complications conflicting with everything else.
6 We also should bear in mind it is
7 possible some parents may never be willing to use
8 privacy software. It should be intuitive, state
9 of the art. It should be preventive, blocking
10 access rather than trying to control speech. And,
11 I think that parents must completely trust the
12 rating system. I don't think there should be
13 doubts in people's minds about these things.
14 Move on to the next one, please. I
15 know we are going to see a demo in a little
16 while, a discussion of P3. This is putting the
17 cart before the horse. But it was described, I
18 think yesterday or the day before, maybe we can
19 discuss some of this later when P3 is discussed,
20 but having seen it already, I would say it is
21 superior to the existing first generation
22 products. P3 does not appear to do anything
23 about chat rooms, which is a whole separate
24 issue. It's still defining vocabulary. It's not
25 going to be ready for a while. It does require

1 adoption by most Web sites. That is a problem
2 because the existing smut-blocking rating system
3 has been adopted by very few Web sites. That is
4 something most people I think agree, there is
5 enormous incentive for that. That is still
6 having a hard time reaching acceptance.
7 There is a risk that parents will
8 typically set their privacy preference and forget it and
9 not get involved. They think, hey, it's protecting. It
10 needs to be able to authenticate parents'
11 approval and give parents more control. I think
12 that any rating system needs to be subject to
13 some kind of independent audit.
14 I think P3 should cover some of the
15 marketing practices, JD marketing practices, and
16 blocking friends' names. I don't think a kid
17 should be allowed to negotiate -- as the
18 presentation of P3 the other day mentioned --
19 with the Web site, and maybe compromise
20 the parent's privacy settings. I don't think
21 a child should be allowed to do that.
22 This is important: I think that the
23 default setting out of the box should be for
24 maximum protection. We saw that browsers have
25 come set up to allow cookies without notifying

the user. And that's been basically like an unlocked door. You've got to start persuading millions of people to go and turn the latch. I think the default for P3 should be set to the maximum protection. Let the parent decide whether they want to lower the privacy preference setting. Don't force parents to learn and start with less than the best protection, and I think P3 also must protect a child who visits a non-kid Web site.

These are some suggestions that I have. I think working with the industry, I think we can make the technology a lot better. Thanks.

MR. PEELER: Thank you, Jeff. Our next presenter is Susan Getgood of Microsystems Software. Ms. Getgood is Developer of Marketing for Microsystems. Microsystems is the manufacturer of the world's leading Internet filter known as Cyber Patrol.

MS. GETGOOD: I actually don't have any visuals right now. I do have something a little bit later. What I want to bring up is that as a company, we are committed to developing simple and easy to use, effective tools for parents to address these concerns, both

in content and privacy. Our philosophy has always been to combine our own technology, to build software that helps the parents and integrates the industry like PICS and like P3 and anything else that comes along as this technology evolves, as it will, to help parents solve the issues they face when they talk about their kids going online. And in a little while, I'll be showing you some stuff that we recently started working on in a prototype to show how P3 and these types of privacy preferences will work in commercial software.

In the beginning, I just want to talk a little bit about the first generation. I think it's important to remember that this technology is always evolving and always changing and that is part of why technological solutions and self-regulation are often the best way to begin approaching those problems, because sometimes the technology moves a whole lot faster than any type of law could and we want to keep doing the best job we can.

I'm really here more to answer questions that the panel or the people from the FTC have about the existing technology and how

it's being used by our customers, how it's being used in the market. Other than that, since Chatgard has been around for the past year, we have had quite a number of people using it to protect their kids from giving out personal information online, and the key to anything with filtering software, blocking software, the online controls, America Online or any of the other online services, is they work when you use them properly.

Support forms, like the ones Jeff showed you, exist to help parents learn how to use this software. Our challenge is to keep making it easy for them to use. Nothing is going to prevent the determined child who wants to disobey the parents' rules about going online or giving up personal information or anything from doing it. What we can do is prevent that inadvertent slip of information, the child who gives out their name not remembering that they are not supposed to do it. Then all the sudden, those XXXs remind the child, I'm not supposed to do this. That is a first step. The second step is really allowing the negotiation to take place so that parents are truly comfortable that

1 their children aren't giving up personal
2 information, or when they do, they know they are
3 giving it to only Disney and they like Disney, so
4 that is okay. That is really sort of the
5 nutshell of my comments unless there are any
6 questions.
7 MR. PEELER: I think we will have some
8 questions for the whole panel, but we would like
9 to hear from Mr. Gordon Ross, and Mr. Ross is CEO
10 and President of Net Nanny.
11 MR. ROSS: Good morning. I want to
12 thank first of all the Commissioners for inviting
13 me down here from Vancouver. It's a privilege to
14 be here. I think over the last two days, I
15 popped in here yesterday to hear what was going
16 on. I have had discussions with the FTC over the
17 last year or so regarding what we are working
18 on.
19 First and foremost I think what we have
20 to look at -- and I think we all agree on -- is
21 protection of children. The philosophy from day
22 one has been to be able to protect the children
23 and free speech on the Internet. We strongly
24 believe technology can do that. We come from a
25 security background, not just a software background,

and as such there is technology that is being rolled out this year and next year which can basically secure the individual, whether it's a child or adult.

I think there have been many surveys over the last couple of years on the Net about what is going on on the Net. But very few of them have been true to form of what is really happening out there. We truly believe that the educational community has to be educating the parents, not the children. The children are already being educated. I think the government should be spending money on educating what I call a lost generation, which are mom and dad of those kids out there.

I had the fortunate opportunity back in September to be in LA at the county fair and put on a seminar for a month educating parents and educators on the wonders of the Net. The Internet is truly a wonderful place. It's not just filled with smut. People aren't just stealing information. Ninety-five percent of the Internet is filled with wonderful material. It's the first time in mankind's history that we have got global, open communications with virtually no way to shut it

1 down. Right or wrong, that is the way it is.
2 What we can do is develop technology that allows
3 the individual, the corporation or the schools,
4 or the libraries to control what is happening
5 within that system.
6 There are many products out there in
7 the world today. Three of them have been
8 reviewed by Consumer Reports. In that article
9 there are four or five other products also.
10 Those are not mentioned today. Microsoft is also
11 in that report. We are all working to try and
12 offer the consumer technology, let them control
13 what is happening on that PC -- not under my
14 control, under your control. What we have to do
15 is make the software simple, make it easy to use
16 and understand and update.
17 Granted, on our site now you can
18 download the list, read them within your
19 software, you can know what you are blocking.
20 However, the download is a little complex, so
21 technology is changing that. Cyber Patrol is
22 coming out with new products. We all are coming
23 out with new products trying to address the
24 issues that we are here to discuss today, and
25 what has been discussed throughout the last week.

So it's truly our belief that the technology can address these issues as long as we know what the definitions are. And as technologists, we can define. I try to tell people that digital technology is really a simple principle. It's not complex. It's based on binary numbers, 1s and 0s. It's either on or off. Now, if I can control that switch, then I can control what is happening within that system, whether that system is in my home PC, or whether I'm talking to you. I'm either talking to you, or I'm not. It's as simple as that. If you can get down to the simplicity of it and educate the consumer on how simple it is to use, instead of making it mystifying -- something mysterious out there -- consumers won't wind up doing what they are doing today, still trying to program a VCR, which has been around for almost 20 years.

Today, people are going to have to use computers whether we like it or not. And as such, we are going to have to educate the masses on how to use these systems. And, as software developers, we have to make these systems simple to use from the interface standpoint. There is not a piece of software on the market today that

1 doesn't have a bug in it, including Net Nanny,
2 Cyber Patrol, and Windows '95. All of them. Anybody
3 can crack them. There is not a major system in
4 this world that has not been cracked by somebody,
5 whether it's a child, or a very efficient hacker.
6 Major government systems have been cracked.
7 Security is only as good as the people involved.
8 As such, we have to get our parents involved with
9 our children again. And once the parent finds
10 out how truly wonderful the Net is, with the
11 child, the kids will have a difficult time
12 getting on the Net. And the parents will take
13 that control back once they understand how to use
14 it.
15 So I'm here to answer any questions
16 today along with the rest of the distinguished
17 guests here. So I'll be quiet now. If you have
18 any questions of me, I'll be more than happy
19 to answer them.
20 MR. PEELER: I just wanted to point out
21 we have been joined today by Eric Wenger of the
22 New York State Attorney General's Office.
23 MR. WENGER: I think that this is one
24 of the areas that is most appropriate for
25 technology. However, I do caution that as many

speakers point out today, there has to be a balance struck between the level of detail you are providing and the level of protection that the software allows. We are far from making computers into something that are as easy to use as a toaster. I don't know if we will ever get there, or if we do, that the technology will be transparent to the users.

Just to share a personal anecdote, after this conference last year, I went home and I have a much younger brother who just became a teenager, and I said to my parents there is a lot of awful stuff out there. We have to set up software to block this out. First of all, my brother was upset -- why was I trying to take away things out there that he might be interested in seeing and why don't we trust him, things like that -- but I persisted. I said the software has to be set up. It has to be configured. I downloaded one of the products. I won't go into details because I think the problem is with all of them. I configured it and you have to set up different user IDs and passwords for each member of the family because there are different levels of access that you provide.

I allowed my parents pretty good access and restricted my brother, so I get a panic phone call a day or so later. My father can't remember what his password is to start the browser. First thing you do when you run the browser is you challenge it to find out who you are so it knows what level of access to provide you. How many minutes will it take me to get over to the house and disassemble what it was that I had put on there because they can't figure out what's going on.

So the end result was that I took the blocking software off because everybody was upset with me -- my little brother and my parents and even the dog. So while the software is very powerful, and if I had a child, I personally would have it set up, and I feel confident that I could configure it. But I'm still pretty confident that, as I think it was Jeff pointed it out, there is a lost generation. I don't know if it's just a matter of education: I think that there has to be a fundamental advancement in the technology before it can be useful to many people.

MR. PEELER: Thank you. A question for the panel in general, but particularly for Robin,

what is it that parents should tell their kids about disclosing personally identifiable information on the Net? What do you advise your readers?

MS. RASKIN: I think actually our readers are sort of generation two of disclosure. Let me give you generation one, where I think most of our readers are at. I think most parents who have children on the Internet know: no names, no addresses, no credit card information, and don't shop without permission. I think that is becoming ingrained in them.

I think generation two is a little more subtle, and I think what we are trying to teach our children are things like look at the URL. Not all URLs are the same; there is a big difference.

I'll give you a great example. My daughter was doing a report on a Greek goddess the other night. We found one paper from Princeton and one, Witches Coven, in New Jersey, and she had no way of knowing which information was true. So she must learn to read URLs and understand where the source of the information

is, so that if somebody says earn $50,000 tomorrow, she can go back and know how to track the source of that information as true or not true.

I think the second generation is much more difficult because it's much more subtle. It's analyzing the truth in URLs. It's going to places to double check, places like the Better Business Bureau, which is online, other blacklisted Web site places, which are online. If you have a suspicion that something is not true, and I'm talking about a nice little solicitation like when that happened a few weeks ago where the American Cancer Society, everybody who was online got a nice letter to donate money to the American Cancer Society to save some poor child. The poor child never existed. The American Cancer Society never sent it out. It's very easy and believable to do that. But the Internet stopped it fairly quickly because of blacklisted Web sites, because of news groups, because of the type of communications that you can instantly have. That is why I'm hopeful that the next thing we have to teach children is how to protect themselves through knowledge, not

1 just: you must do this, you must not do this.
2 MR. PEELER: So you are saying that
3 right now the rule ought to be don't give out
4 information but --
5 MS. RASKIN: Yes. I'm saying right now,
6 the simplest rule is very binary. No name, no
7 address and as Susan said it can be very
8 tantalizing. I actually have a 17-year old who
9 met somebody who seems very nice and he only
10 wants to send his picture to the house and she
11 really wants this to happen. I said you cannot.
12 And she is 17 years old. I said you cannot have
13 this picture sent to the house. At the very
14 worst he can send it to my office if he really
15 wants to send you his picture, or he can send you
16 a J-peg as an E-mail attachment and let him
17 figure it out.
18 I think you must keep the binary
19 rules: No name, no address and no shopping online
20 without permission. And then the second
21 generation, which is harder for a parent to do,
22 is to start to teach about the subtleties of
23 where this information is coming from.
24 MR. PEELER: We have had two
25 suggestions today that actually your user rates

1 in general that you are reporting are very
2 similar to Professor Westin's rates overall, and
3 we have heard two suggestions that the only
4 way those rates are going to go up is if the
5 filtering is integrated into the browser. I'm
6 wondering if Mr. Ross and Ms. Getgood would
7 respond to that suggestion.
8 MS. GETGOOD: Basically, I think there
9 is some truth and, indeed, we found that
10 America Online uses great components of our
11 technology and Cyber Patrol is listed within America
12 Online's own parental controls. In the last year
13 America Online has seen their rates of use rise dramatically
14 because it's in one place, simple and easy to use. On
15 the other side, you have the fact that along with multiple
16 children in a family, parents may use multiple
17 online services which may do different things and have
18 different browsers. So having filtering software
19 as a separate entity that can be set up once, for
20 whatever possible online service you use, has
21 benefits to some families too. So integrating blocking
22 software into the browser is certainly an easy solution.
23 I think you are going to see it
24 continue along in much the same way as we have in
25 the past year. Online service adding support

1 within their own online parental controls, and
2 then as these self-rating systems -- as rating
3 systems become more prevalent, you will see that
4 kind of control being integrated into the
5 browser.
6 MR. ROSS: I agree with that point.
7 I think most of the browser manufacturers
8 are busy with other issues from a screening and
9 filtering technology standpoint. There are two
10 issues here, and I think Consumers Union
11 mentioned one of them and that was the
12 availability of this software at retail. What a
13 lot of people don't understand is to develop a
14 software package and get it into the retail
15 market, just to get it into the retail channel,
16 you are looking at an expenditure of roughly a
17 half a million to $1 million. And that is to get
18 it in with distribution.
19 We currently are distributing to a
20 large distributor to get the software into various
21 stores. Those stores have to order it through
22 the distributor. They can't come directly to us,
23 or we can't go directly to the stores. It's just
24 the way the system is set up. To get it into
25 that channel, you are looking at a half million

dollars to $1 million expenditure.

MR. PEELER: You are primarily sold through stores?

MR. ROSS: We are sold both electronically online, electronic distribution, in retail channels through distribution and also internationally through distribution.

MR. PEELER: Could you give us a rough idea of what the retail versus the Internet distribution is?

MR. ROSS: Retail versus the Internet distribution: retail right now probably counts for about 8 percent of our revenue. That is drastically starting to change. Within the retail channel now, the cost of packaging is relatively expensive because you have to make the box in order to get into the stores. That four-color box is relatively expensive to produce. Electronically you can distribute it much cheaper. It's just a file download. The majority of the software packages today come with online help, which is basically the manual online. Then the customer can print that out if they so choose.

But as you see more and more electronic distribution going on on the Web, you will see

more and more software being distributed directly to the home.

MS. GETGOOD: We all have been in retail in one form or another in these past couple of years and one of the things we found is that the traditional computer retail store, like Comp USA or whatever, was not a place that parents went to when they were looking for things to protect or use for their kids, like educational software. They go to Comp USA to buy cables and modems and stuff for their home business, or whatever. So you quickly saw a lot of filtering software in the bargain bin.

One of the things that we are looking at is more family-friendly retail channels where parents really go to buy software or buy for their kids because that was one more outlet that might be an appropriate place to put this kind of software.

MR. PEELER: If in order to really up the rates the filtering has to be built into the browser, how many years out are we talking before there would be substantial increases in the rates?

MS. GETGOOD: Are we talking content

filtering still?

MR. PEELER: Privacy filtering.

MS. GETGOOD: I think that Deirdre Mulligan from IPWG can probably answer more specifically in the next piece of this some of the progress that is being made on the privacy labeling side. As far as supporting privacy in software, that is actually one of the easier parts of it, from my point of view.

MR. PEELER: Do you have an estimate of what type of time frame you are talking about?

MR. ROSS: That, I think, becomes a resource and cost issue and a priority within the organization. As a small software developer, that is our priority. Some of the larger software developers have other priorities such as operating systems, et cetera. So it's not a high priority item for them.

Larger software developers normally approach organizations like ourselves, Cyper Patrol and others and make licensing arrangements to incorporate that technology. I believe that is going on in the industry right now.

MR. FOX: I want to comment also on the availability. It's not just a question of how soon

1 filtering software will be incorporated into the browser,
2 but also how soon a large number of Web sites will
3 actually support the system once it's fully
4 developed. Because we have a situation where
5 Microsoft's Internet Explorer supports the RSAC
6 content blocking and yet a very, very
7 small percentage of Web sites have
8 incorporated the RSAC content blocking.
9 So even if you have it in the software,
10 you have a second problem, which is getting
11 enough Web sites to support it, so that it's
12 actually useful.
13 MR. ROSS: That's right. I think that
14 is due to the globalness of the Net. The
15 PICS consortium, which we are all members of in
16 the filtering arena, has been in place since
17 '95 when they made the announcement in
18 the Internet world. However, for global
19 acceptance of PICS technology, you run into the
20 same issue you run into with the movie rating
21 system: what is X-rated in the United
22 States or Canada could be PG-13 in Paris,
23 France or some other country.
24 When you get into these ratings
25 procedures and decide to rate your Web

page with RSAC or SafeSurf or some of the other rating organizations -- how do I rate it. The rating will depend on what country I'm in. So it becomes very, very difficult. How do we force the Web to rate, other than on an honor roll system.

There's a company called Net Shepherd which has currently rated 300,000 English pages according to content. Out of those, roughly 5 to 8 percent are adult-rated content. However, since they rated that -- an expenditure of roughly $1 million to do that -- you are now up to a million pages out there that are English content and growing every day. So it's an astronomical cost factor to administrate that. If you do a simple mathematical calculation to rate all those pages, at the time they started there were 57 million pages on the Web. They were going to do it in a 90-day period with 16,000 people; they were looking at a $52 million expenditure just to rate it.

As all of us who are involved in this technology on the Web know, as soon as you rate all these pages, probably 30 to 40 percent of

them will have changed or disappeared, and I think somebody pointed out that most of the Net citizens out there right now will get on an issue when they see it on the Web, either a news group or an E-mail regarding a certain situation.

There is one organization that has been slamming all of us as filtered or censor-ware people. When you look at what the individual is doing, he is basically a freedom of choice individual which I commend him on because he is trying to protect the First Amendment. He's a young man but he also has a valid issue with some people who have been flaming him. It's become a war of the words out there.

But we as technologists, specialists or or whatever you want to call us, we know what is happening on the Web. We also know how to develop the technology to take care of that. It's just a matter of time and resources, and what do we want to do, and I think the first priority is to protect our children. I don't think anybody in this room will argue with that.

The other issue that always comes up is the pornography on the Web.

There is one subject globally that we all agree on and that's child pornography. Unfortunately, there are countries in this world that live off pornography. And even though these countries say they agree, their child pornography is still going on. We as technologists are trying to track that. From a security standpoint, we are developing technology so we can backtrack.

MR. PEELER: Thank you. Commissioner Starek.

COMMISSIONER STAREK: I think I heard Jeff say that AOL, CompuServ and Prodigy are offering this technology but most people don't utilize it. How does it differ from what those companies offer?

MR. FOX: Those three companies actually offer Cyber Patrol. I think in some cases it's a customized version that is designed to work with their servers. It may be slightly different but similar to those products.

COMMISSIONER STAREK: How effective are they at this point?

MR. FOX: How effective are the products?

1 COMMISSIONER STAREK: Yes.
2 MR. FOX: You mean protecting privacy?
3 COMMISSIONER STAREK: Yes.
4 MR. FOX: As my test showed, it wasn't
5 that difficult to get around the blocking software.
6 We don't have statistics yet that actually show what
7 percentage of parents were having problems with the software
8 or think it doesn't work.
9 MR. ROSS: I know we do have E-mail. I
10 can't speak for Cyber Patrol or any others, but
11 we are all in the same game. I know we do have
12 E-mail from customers and various other
13 organizations that have incorporated this type of
14 technology where viewing the audit trail they
15 have, they just monitored what is happening on
16 the terminal and did an audit trail afterwards
17 and took appropriate steps. Some of the
18 steps have resulted in termination of employees
19 for downloading inappropriate material. So these
20 organizations are using this type of technology,
21 and once it's used correctly, they are not trying
22 to hack through the system, which I know Jeff has
23 done. We can develop technology and make it more
24 sophisticated, but the whole issue is how do we
25 educate the consumer in how to use this

technology. It's difficult enough to push the issue of "security" without making it sound paranoid. And as most of us in the security business know, security is based on paranoia.

We currently have alarm systems in our homes and cars. We walk down the streets with guns and pepper spray. The only thing we don't have secure is that guy coming into the home. That is what we are working on here. How do we control the information highway coming into our house. We are going to use that to communicate in the future. So how do we make sure your digital data is secure at home?

This is the way we are going to communicate in the future, and I think the technology, the companies that are involved in this technology can develop these products. It's just a matter of resources and time.

MS. GETGOOD: Certainly, each of the online services should say more specifically about what they do. Since we are involved with the three you mentioned, I think I will just tell you what they each do in terms of filtering and privacy. CompuServ and Prodigy both

provide Cyber Patrol, so they have control over chat much as we provided Chatgard. They also do some level of control over their own content and availability of information. America Online has pretty sophisticated parental controls in terms of what kids can and can't do. If you select the Kids Only channel for an America Online child, you have a relatively safe enclosed environment, and that is an application of technology. And I'm sure America Online has already said something more about what they provide.

MR. FOX: I want to say I have to take exception to the characterization of my work as "hacking a product." As I wrote up in my submission to the FTC, I did not do anything that involved programming or anything that anyone who knows how to use a word processor couldn't do; any person in this room could do exactly what I did. I did not do anything highly technical. It's not hacking.

MS. RASKIN: Kids actually do it. They are right there with Jeff. They all know how to do this. So keyboard control is not really an effective blocking mechanism for

privacy. Ultimately, I would say we are two years from the point where you can walk up to a computer and in some way have it recognize who you are: be it voice, be it face recognition, or fingerprint. Some sort of digital signature. It remains to be seen which one will play out. We are still in the very prehistoric times of blocking sites, and authentication will really move us along very very quickly.

MR. ROSS: I didn't mean to insinuate you hacked, Jeff. I'll take that back. Hacking is a criminal offense. I think you are right, Robin: the technology is going to be developed, and through the authentication process in the near future, we will know who is typing or accessing the system. Some of us here will be talking about that later. But I think that we really have to sit down and try, like I said, from the very beginning to educate the lost generation. And that is mom and dad.

Many of my friends don't understand what I do because I've been doing it all my life. They don't how to start up a computer.

They have to ask their children.

MR. WENGER: I want to make this clear. This is just me talking. I think one of the things that we tend to do is we all get fascinated with the fact that this is a global medium. The fact that I published a Web page and somebody in Pakistan can read it is all well and good. If we were trying to impose some kind of regulatory scheme, then we should be worried about trying to impose our laws on other people. But I'm not sure that I buy the objection that was raised here that if we have some sort of voluntary rating scheme that that would be imposing our will on other people.

First of all, I have to mention the fact that the vast majority of users of Web sites and software designers are here in the U.S. If the industry in the U.S. decides to try to voluntarily adopt standards that would make it easier for U.S. customers to use their software, I don't necessarily agree that we have to worry about what the effects are worldwide.

MR. PEELER: Thank you.

MR. ROSS: I would have to take

exception to that. In a global community, we have to look at it globally. Granted, we do have a large scientific community here in North America. However, there are Eastern Bloc countries that have a large software development community. A lot of software that is currently being developed is being developed by programmers offshore because the cost of labor is much cheaper.

That is happening, so we have to be aware that with a global medium, we have to look at a global issue and no single country can develop a set of rules. So we have to get together globally and develop a global standard. And that is what we are trying to do with PICS, and that is what we are trying to do with filtering technology.

The National Computer Security Association here in the United States has formed a new consortium called SIFT, which stands for Superior Internet Filtering Technology. SIFT wants to set standards just like they have done with antiviral software.

MR. PEELER: I think that is a good

transition. Our next panelist is Deirdre Mulligan.

MR. WENGER: Can I make one follow-up point?

MR. PEELER: Sure.

MR. WENGER: The U.S. movie industry makes movies and releases them here in the U.S., and they are rated here in the U.S. And the fact that they are released worldwide and then receive maybe other ratings in other countries is certainly worth considering, and I think, I'm just saying that it shouldn't always be the governing principle. We have to face the fact that we are here in the U.S. and so much of what is going on is here in the U.S. Obviously, it would be ignorant to ignore the rest of the world, but if we are working here under voluntary standards, it might just be appropriate to think about the effects here in this country.

MR. PEELER: I would also like to ask the panelists that used overheads or slides to supply copies of those for the record. Deirdre Mulligan is Staff Counsel for the Center for Democracy and Technology. I think she has been

1 on the panel for all four days. She is joined by
2 Susan Getgood in this presentation.
3 MS. MULLIGAN: Unlike some places where
4 being around for four days might not be an honor,
5 I want to assure you that it has been.
6 On Wednesday we did a very
7 brief presentation about a joint effort to
8 develop both a vocabulary for privacy or a
9 language for privacy and an underlying technical
10 tool that would allow the user, being you or I or
11 a parent, to set up privacy preferences about the
12 use, disclosure and collection of their
13 information and allow Web sites to very easily
14 state their information practices. What I'm
15 going to do today is talk a little bit about how
16 this might work in the children's area and some
17 of the unique issues surrounding implementation.
18 I want to start by saying that last
19 year, and I think certainly at the workshop this
20 year, the baseline has been the principles that
21 were put out by the Center for Media Education
22 and Consumer Federation of America -- everyone
23 agreed that notice and parental consent were the
24 right model for dealing with information when it
25 deals with children. And I think what you

1 have heard from everyone in the past two days has
2 been completely on that issue; no one has
3 said that that is not the right model.
4 The Center for Democracy and
5 Technology independently filed some comments
6 on CME/CFA's proposal last year completely
7 agreeing with their principles of notice and
8 parental consent, but saying that we were very
9 concerned about how you verify parental
10 consent in this medium.
11 As someone noted the other day, one of
12 the beauties and difficulties of this medium is
13 that people still do not know who you are. You
14 are not required to identify yourself. And that
15 goes for children as well as for adults. And
16 that in looking at the proposal put on
17 the table, the notice and consent portions,
18 for me are very compelling.
19 The idea that the Ronald McDonald site,
20 if they are going to use a child's name to
21 display for a one-time, your day in history and
22 then discard that information in order to let a
23 kid participate in that, we are going to suggest
24 that a mailing goes in to Ronald McDonald
25 containing the child's name, probably their

address, the parent's name and a written permission sounds to me more like the parent/child database provision of a privacy proposal, and that is what I would like to step back from.

What we tried to do is focus on how do we facilitate the idea that parents should be in the decision-making position without requiring that anybody know that the parent is making decisions for the child?

We don't have to let anybody know they are dealing with a child in this medium and we think that is important, specifically when you put it in the context of the concerns that we heard yesterday. There are two types of privacy concerns. There are the privacy concerns that are very compelling concerns about how our children reveal information about themselves to others, be it in the offline world or the online world; we want to encourage our children not to tell strangers their name and address, not to tell strangers how to reach them and find them and not to set up planned meetings with people outside their parents' purview.

1 On the other hand, we have another set
2 of children's privacy issues, which is not about
3 pornography. It's not about pedophiles. It's
4 about information being disclosed to known
5 entities, to Web sites. I want to keep those
6 issues separate partially because I think they are
7 addressed in different ways, and I think that has
8 been highlighted by some other people who have
9 spoken.
10 This is a slide that you saw the other
11 day. It outlines what the underlying
12 vocabulary for the Platform for Privacy
13 Preferences would likely look like.
14 I'm speaking of a vocabulary that was
15 developed by the Internet Privacy Working Group,
16 which I should say has been a long effort over
17 the past six months by a number of organizations,
18 consumer organizations, privacy
19 organizations and companies. And particularly in
20 the children's area, I think the help of
21 organizations such as the Center for Media
22 Education have been helpful in figuring out some
23 of the ways in which this should be implemented
24 to respond to children's privacy issues, and also
25 in very clearly indicating where they come up

short.

The top line of this just talks about different types of information. Physical contact information is information which we are most concerned about usually when, as a parent, we are thinking about our child: their name, their address and their phone number. We are also concerned about their cyberspace contact information, their E-mail address, but there are also other types of information: their navigational data, which we discovered on the Internet can be used to harvest an awful lot of information about someone's activities, dislikes and likes.

On the left-hand side, you have two categories about users and disclosures. These are if you are a system administrator at a Web site. These are probably fairly straightforward for you. If you are a parent, I think as everyone here has very clearly stated, these are not.

I would like to move to the next slide. We were very cognizant that a parent would not necessarily want to or be able to understand the nuances unless they were given

1 some context. We were also very, very wary of
2 saying that there should be defaults.
3 Generally, defaults are set by a company when they
4 decide to implement a product. And while we can
5 certainly talk about what a default should be, we
6 were looking at what should the choices be and
7 what should people be able to choose from. And,
8 hopefully, in this paradigm where the ability to
9 click is a fairly simple activity, we can
10 get to a point where there isn't a default: that
11 the parent makes a choice at the front end.
12 What we thought first was that this
13 should start with a warning to parents. One,
14 that there is no substitute for parenting.
15 Whether you are putting your child down in front
16 of a computer or in front of the TV, that you are
17 their best tool. But that there were ways that
18 parents could engage in protecting their children's
19 privacy.
20 Also importantly, that while we can set
21 up preferences that will protect your children's
22 privacy when they are dealing with a Web site,
23 there are many activities on the Internet
24 that your child can engage in -- bulletin
25 boards, chat rooms, other areas where your child

1 might be giving up information -- that a Web site
2 is not necessarily going to have any control over
3 how other people on that site might use that
4 information.
5 So the first four choices here reflect
6 the way in which you would be limiting or
7 prescribing your child's interaction with Web
8 sites. And they say things like, I want my child's
9 online privacy to receive a maximum allowance of
10 privacy protection. Pretty straightforward.
11 "My child can visit Web pages that
12 collect information as long as it's not tied to
13 his or her real identity;" perhaps the child
14 is filling out or clicking on different icons
15 that indicate his or her three favorite colors. Just
16 so long as they are not collecting information
17 about my kid's identity, that is okay. This may
18 facilitate the ability of kids to do different
19 types of interactions, both with each other and
20 in games without kind of saying that any
21 interactivity is, per se, bad.
22 The next one says, "My child can visit
23 Web sites that collect personally identifiable
24 information for internal purposes only." So my child
25 can go to the PBS or CTW site, and she can

1 release information there as long as it's not
2 going to go outside that entity.
3 And the last one says, "My child can visit
4 Web sites that share personally identifiable
5 information with others." Now, a Web
6 site might have very, very specific information
7 practices that they would reveal to you. But we
8 thought as a baseline this would help parents in
9 making some type of choice.
10 As I said, these deal with kind of
11 the Web site privacy practices, but in order
12 to really address the children's privacy
13 concerns, we thought there were two other
14 issues that had to be addressed. One was,
15 the second, that says I want my child
16 to be blocked from all Web pages offering
17 bulletin boards, chat rooms, electronic pen pals,
18 programs where kids might disclose information
19 that is going to be available to someone other
20 than the person operating the Web site, and this
21 is a yes or no. As a parent, do you want your
22 kids going here or not?
23 Similarly, we thought that pages
24 that have a credit card number request or
25 request some other payment mechanism, often are

1 pages that are registration pages or order forms
2 where there is already a lot of collection of
3 information, or they also have some tie to sites
4 that people have noted might have objectionable
5 content. So we thought that having a
6 button that very easily allows you to block your
7 children from Web sites that were going to
8 require some kind of payment mechanism would be
9 useful.
10 Now, I just want to be clear that
11 this is not a Web site. If you can label
12 specific pages at a Web site so that my
13 child might be able to go to all of Nabisco
14 Online except for the page on Nabisco that
15 asks for information, this might solve some
16 problems, but it might also cause some
17 problems.
18 The Internet Privacy Working Group and
19 the P3 platform are not about controlling
20 content. They are not about marketing practices
21 or advertisements. They are about information
22 collection. However, I think, as some other
23 people will probably discuss later, that the
24 context in which information is requested,
25 particularly when you are dealing with children

1 is, of course, a relevant consideration.
2 I think even more importantly as the
3 Platform for Privacy Preferences is a project of
4 the World Wide Web consortium, making sure that
5 children's experiences as well as adults'
6 experiences online are seamless, which was the
7 reason that this is trying to be built into the
8 infrastructure. This is a really paramount
9 concern, so I think that in figuring out how a
10 site might describe its practices, we would want
11 to think about doing that in a way that was not
12 going to set up difficult interactions between
13 parents and children, nor set up a frustrating
14 experience for a child where they see Get Free
15 T-Shirt, Get Free T-Shirt, Oh, give us
16 information. Those three things might all come
17 under the same information practice because they
18 are tied together in a sequence.
19 So in closing, I just want to say that
20 there are things that the technology can give us,
21 and there are decisions about implementation that
22 I think have to be made with guidance and advice
23 from a larger community, and as Jeff pointed out,
24 this is a process under development. The World
25 Wide Web consortium can respond to some of the

1 questions about when. The World Wide Web consortium is
2 having its first kind of full meeting to look at the P3
3 project on June 26th. I am pleased to say that I know
4 Susan Getgood will be participating, and I'm hoping
5 that some other people who have experience in
6 communicating with children will also be. We
7 have been fortunate enough to have the advice of
8 Elizabeth Lascoutx from CARU and that of people
9 who are in the business of knowing how to
10 communicate with children. I think it's
11 incredibly important that they influence how this
12 develops.
13 I would like to turn it over to Susan,
14 who is going to demonstrate a mock-up of what
15 P3 might look like in a child's product.
16 MR. WENGER: I was just curious about
17 what this particular part means. This is the
18 privacy preference, right, the one that said they
19 can't collect personally identifiable
20 information. It seems like that's what the title
21 was. And halfway through it it says, My child
22 can provide her name, address and phone number or
23 E-mail address for which -- that's mainly used
24 for the purpose for which it's solicited. I
25 thought that would have been the second choice,

1 You can collect personal identifiable information
2 as long as you are not sharing it with everybody.
3 MS. MULLIGAN: I think you caught a
4 glitch. As I said, this is a process, and I
5 think what this should say, let's see, "that
6 collect information as long as it cannot be
7 tied to his or her real identity," I should
8 think they can collect information about navigation
9 or allow my kids to participate in a way that
10 they would not be disclosing information. Sorry,
11 thank you.
12 MR. PEELER: Susan.
13 MS. GETGOOD: As Deirdre said, what
14 we have done is implemented a prototype
15 to give you an idea of what parents
16 might be able to do with P3 within
17 one of the most popular filtering software
18 products.
19 This is a prototype that is using
20 an existing vocabulary, and it's just
21 giving a beginning of an idea. As we started
22 to look at this, we started to think about
23 things we wanted to do to improve it, which
24 which is why we are going to be participating
25 in the W3C.

1 This is your highway. You are all
2 familiar with Cyber Patrol, and this is a
3 first look at implementing privacy profiles.
4 We looked at two things. First off,
5 implementing privacy for children is actually one
6 of these things that is a little bit easier than
7 trying to deal with it for adults. Adults, you
8 may negotiate with a Web site, well, maybe I
9 might be willing to give this up or give that
10 up. Parents generally are interested in one
11 thing. If a site's policies don't match the privacy
12 preferences set for my child, I don't want my child
13 to go there, or I want some mechanism to review this site
14 later and make a decision for myself for my child.
15 So what we did was look at parents who
16 want to take these vocabularies and apply them
17 and either issue a warning that the privacy
18 preferences don't match, possibly for an older
19 child who understands more of the rules of the
20 road, or block the site if the family's
21 privacy preference for that child
22 don't match those Web site practices. And
23 secondarily, once they have blocked that site,
24 they might want to give the child an option to
25 allow that site to be stored for later parental

1 review. The child should have this option to
2 store a site or not, based on their decision about
3 whether they really want to go here and whether they want
4 their parents to look at this or not. Because
5 you don't want to allow your children to go
6 everywhere they want.
7 These are the same four statements that
8 you saw before. Again, this has got to be made
9 simple for parents to use for their children.
10 Web site administrators can certainly
11 understand that there are various variables.
12 Parents want to make a simple choice
13 choice, My child can visit Web pages that
14 collect information as long as it can't be tied
15 to his or her real identity. Then, as Robin
16 pointed out earlier, parents might want to drill
17 down and if they do, let's give them that option.
18 But I can guarantee you I don't think most
19 parents are going to want that right now. But
20 you can indeed go down and look at all of the
21 pieces behind this and make further decisions.
22 This is for the technical people
23 actually parsing a rap file. You are seeing the
24 actual contents of the information. This is
25 just a preliminary implementation, and when they

select it, it will actually bring up the various things that match a reasonable profile, and that is pretty much it.

MR. PEELER: Thank you. Is Deirdre still here? I have one quick question for you. I guess the question is the same one I was asking earlier, which is -- how long?

MS. MULLIGAN: I am hesitant to speak on behalf of W3C, but I think Joe Riegel is still here. My understanding is the P3 project and the specification that will come out of it are basically built upon possibly two already existing underlying technologies. Specifications one is the Platform for Internet Content Selection, which, as Jeff pointed out, is an existing specification. It is already built into Microsoft's Internet Explorer, and my understanding is that it will be in the next release of Netscape, which will be almost the whole browser market.

And then it's also based on P3, which is a negotiation protocol, and that is also an existing specification. And I think it's supported by the existing browsers, and that is

the part that I'm not completely sure of but I'm fairly sure of. So this is more of a question of figuring out how those two things weave together. My understanding is that W3C is thinking in terms of a year to a year and a half. My understanding is that the browser -- when Netscape's browser comes out -- will be close to being able to support it and that it will be more a designing of the user interface, and I know that Microsoft has already been looking at how to design a user interface, because we have been in discussions with them.

MR. PEELER: Other questions?

MS. MULLIGAN: Could I add one more thing?

MR. PEELER: Yes.

MS. MULLIGAN: As Jeff Fox pointed out and as we at CDT have been long in the position of pointing out, software specifications without the supporting stuff that you need to make them work are useless. So part of the reason that we have pulled together the Internet Privacy Working Group is to work on that public

education piece and market saturation piece: these tools are not going to be effective if they don't work.

I have to say that unlike the content area, where from a true free speech perspective, it kind of cuts both ways whether or not people use them, from a privacy perspective, the lack of market saturation does not have good consequences for privacy. So I think that there has to be a very large commitment to that implementation. And I'm happy to say that I do think it's there, but it will have to be a joint effort, and I certainly would hope that the FTC would help with the education piece of that.

MR. PEELER: By market saturation, you mean the number of Web sites that are actually used?

MS. MULLIGAN: Yes. One of the unique things is that as a user, if it's a child, my kid can't go to any sites that don't have privacy practices. So you can actually drive a market for privacy practices because if all of a sudden there are no kids going to those sites, this sends a signal that perhaps there needs to be

some action.

MR. FOX: Creates a cyber-boycott in a sense.

MS. RASKIN: Deirdre, do you see PICS plus P3 as being one set of choices that a user makes?

MS. MULLIGAN: Yes. I am not a technologist so I speak cautiously, but a lot of the P3 platform or specification is a PICS rules type application and Susan might be able to speak more eloquently. Oh, Joe, excellent.

MR. RIEGEL: I'm Joe Riegel from the W3C. Deirdre did a pretty good job of describing what it takes to probably get this thing to roll out and be used. We are expecting all specifications in six to nine months, from a multi-cable in June. I also expect products will be developing previous versions before we actually have official specifications that are released, and as the specifications come to closure, people will implement the final standard.

What was the last question in terms of the difference between PICS and P3? PICS was driven by content

1 selection. The general sort of technology
2 is to be able to make assertions or
3 descriptions about Web resources, and in the PICS
4 application, the driving force certainly was
5 content selection.
6 We discovered that the technology is
7 actually quite useful and in general we can apply
8 it towards multiple problems, one of those being
9 privacy. Another is intellectual property. And
10 in terms of technology development, we
11 expect that the technology development that
12 occurs on P3 will be bundled together so the next
13 generation of technology sometimes has been
14 called PICS Next Generation. The applications
15 will all coexist with one form of technology, so
16 P3 or PICS NG will be multiple
17 applications, including privacy and content
18 control.
19 MR. BERMAN: I want to make one other
20 comment. I think Deirdre pointed out, but just
21 to emphasize it, content labeling, which
22 involves some decisions and subjective judgments
23 about content, raises significant First Amendment
24 issues. That has been a problem with the PICS
25 implementation on the content side, but in the

1 privacy area, it doesn't raise the same issues.
2 People aren't saying who is going to rate my
3 site and what is the government going to do.
4 It's, you have a policy, this will support it, you
5 want to put it up, whatever that policy is, you
6 put it up. If a Web site doesn't have a policy, the
7 customer doesn't have to go there, and parents can
8 make it so that their kids don't go there. So I
9 think it's a very different issue.
10 MR. PEELER: Are you working with
11 industry associations right now so they would be
12 ready to --
13 MR. BERMAN: Yes. The Internet Privacy
14 Working Group is working on the policy and
15 implementation side of this issue because part of
16 the W3 platform on content labeling was kind of
17 stranded because there wasn't a real
18 implementation from the market and companies and
19 associations. There are efforts underway in
20 another forum to rectify that to deal with content
21 issues.
22 But here, from the start, there is just
23 an awful lot of buy-in and there will be even
24 more I think after this hearing because up until
25 this hearing, everybody was trying to

1 differentiate their market thing. TRUSTe and
2 P3 and we are all doing this, and DMA is doing
3 that. Everyone wants to make sure that they
4 are doing something -- the IPWG process -- to get
5 everybody together and say these things all work
6 together. I think there is a big momentum
7 once we get this language developed to
8 get it out.
9 MR. FOX: What kind of auditing is
10 there going to be of the ratings?
11 MR. BERMAN: Those are choices that
12 have to be made. The platform does not
13 ensure that what people say is happening
14 is going to happen at that site. That is
15 why TRUSTe is out there. That is what the
16 FTC is about. That is what Fair and Deceptive
17 Practice is about. That is what the BBB (Better
18 Business Bureau) online is about, and there will be other
19 good housekeeping verification processes that
20 consumer groups are going to have to perform.
21 There is something for everybody out here.
22 COMMISSIONER VARNEY: I think we all
23 agree that if a site says it's collecting
24 information for one purpose and is using it for a
25 different purpose, that is either fraudulent,

deceptive or unfair. I don't think you have got any disagreement about that.

MR. FOX: Somebody needs some means of checking that.

COMMISSIONER VARNEY: What we currently do is we get consumer complaints, and State AGs get consumer complaints. People go to sites. They realize that although they have given information or they have said they weren't going to give information, they are getting E-mail. We only have the mechanisms that we always have to detect fraud, deception and other practices.

But I have a different set of questions I would like all the panelists to comment on if they are qualified, and maybe none are, because there's nobody here from Netscape or Microsoft. There was a very interesting comment in Stan Greenberg's focus group about the fact that privacy is important, and we need it but it's not easy. We have spent a lot of time talking about this this morning, and this isn't so much a question for proprietary software systems as it is -- is it going to be possible, feasible, advisable that either Netscape or

1 Microsoft are going to load onto the front end a
2 mechanism for parents to make these choices
3 before they turn on their software?
4 MS. RASKIN: I'll go first. Netscape
5 and Microsoft, I think there is a really simple
6 rule: If there is a business reason, they will
7 explore it. And more and more, if you think about
8 it, privacy and content are becoming serious
9 issues in the workplace. That is really good
10 news for parents because when it affects the
11 economy and the business of this country, you
12 better believe that Netscape and Microsoft will
13 be there implementing solutions and tacking on
14 the kids' part, and that is exactly how I believe
15 they view it.
16 I had a conversation with Bill Gates,
17 and he said you tell us what you want and we can
18 do it.
19 COMMISSIONER VARNEY: He doesn't tell
20 us that.
21 MS. RASKIN: Just tell us what you
22 want. Netscape has not. They actually draw out
23 authentication and all sorts of complicated
24 diagrams. It's daunting.
25 COMMISSIONER VARNEY: It is conceivable

that this kind of a standard could be very easy for parents to access themselves?

MS. RASKIN: I think so.

COMMISSIONER VARNEY: My next question is, what about the Firefly/Netscape/Microsoft proposal for the Open Profiling Standard? How does that fit in with this because although nobody can comment because it's in the Technical Standards Committee, but maybe Joe would have some thoughts on this. It seems to me one of the potential problems with the Open Profiling Standard, unless there is an override option or the default is on override, is that you have to put a lot of information in there or potentially you have a lot of information in there. So then I have a third question. How does OPS work with the P3 platform, and how do cookies work with the P3 platform?

MR. RIEGEL: They're a couple of difficult questions. I'll start with the first with respect to there is, sort of, this relationship, between complexity and ease of use, and it seems that the relationship is

that you want to make things easy for people to use so it will be used, but to do that, you are taking some of the control away from the people that are making the decision.

When you do that, this is the big default question, when you do that, certain entities will want to define those settings in certain ways that people might not agree with and a lot of controversy happens as a result. In terms of technology development, we try to shy away from making those decisions for those people. You want to have as many options as possible.

The nice thing about the IPWG work is that third party services can make the recommendations. You saw an example of IPWG vocabulary and IPWG recommended settings. Our strategy has been to develop technology which supports fairly granular statements, but that allows other people to hide these granular statements and make very simple statements for you on top of the granular statements and you have the trust relationship with these people.

COMMISSIONER VARNEY: Do you have any comments on the relationship between OPS and P3

and cookies?

MR. RIEGEL: On the OPS front, the model I think about is that you want to potentially automate the exchange of certain information. The scenario I would use is that I go to a Web site. There are two big pieces. One is talking about how that data is used to negotiate: I don't want you to use this data; I want you to use this data. The other big component is actually exchanging that data in a secure manner. What we have been focusing on with respect to P3 is what data needs to be used and how the data will be used. The OPS part is what I call the data store, which is how to store it and control it and exchange it in a secure manner.

COMMISSIONER VARNEY: So, in fact, even if OPS comes out, it's in the system and you fill it in with your age, credit cards, kids' names, addresses, dentist, everything; it can be totally secure so that it's kind of underneath, so to speak, my P3 preferences?

MR. RIEGEL: Right. P3 is sort of the way to talk about how you want that data used. You can use that data in a secure manner. You

1 could set up different personas, hopefully:
2 the me at home, versus the me at work,
3 my child at school, versus the child at
4 home.
5 COMMISSIONER VARNEY: I think it's
6 important, and I know you guys are going to think
7 about this in your standards committee, it's
8 important to have, and maybe the technical group
9 isn't in the right place, but it's important to
10 have a consideration, I think, of the policy
11 consequences of how the OPS standards are set.
12 Whether or not there has to be a certain level of
13 information in there for it to work, whether
14 or not it can be overridden, or there is minimal
15 choice or sort of, what are the policy
16 considerations of how much information is in
17 OPS?
18 How about P3 and cookies?
19 MR. RIEGEL: First, the OPS standards,
20 I just want to clarify the point. There is an
21 OPS specification that everyone is working on and
22 that has been submitted to the W3C for the P3 to
23 look at. Here is something. How can we build on
24 OPS, so that the specifications coming out will
25 be P3 specifications? The cookie control issue

is fairly complex. People have expressed interest for us to be at the place where the cookie control is -- how those specifications are further developed.

I honestly don't know whether we will need to go further in developing cookies because a lot of the capabilities that people wanted to do in the next generation of cookies will be addressed by P3. It may be able to exist as is for some sort of issues.

MR. PEELER: I think we need to have one quick contact from Jerry, and then I think we are going to need to close.

MR. BERMAN: Just one clarification on the clarification. The P3 platform has all of these pieces to it, including the cookies piece, and the IPWG work, which is focusing on the first job, which is getting that privacy language out there. And there is already, the buy-in from associations, Direct Marking Association, ISA, BSA, Microsoft, AOL, Netscape, they are all working, developing this language.

I mean, this is really a work

underway. It's not something that starts here. It's been underway, and that is why we are so optimistic about this.

MR. PEELER: Thank you. We appreciate all panelists' participation. We want to move on to the third and final technology panel, and I think this one will move us out even further in the future.

We want to talk about how Digital IDs/ certificates and biometric technologies might be used in the future as a means of providing verifiable parental consent.

Our panelists are Michael Baum, Vice President, Practices and External Affairs of VeriSign. His responsibilities include developing practices which VeriSign conducts in its public Digital ID and private label certification operations. We are hoping that today we can focus on the question of what the implications of technology are for providing parental consent in the future, as opposed to necessarily exactly how the technology works. Mr. Carty.

MR. CARTY: Yes.

MR. PEELER: Michael Baum is going to

be joined by Tom Carty of GTE CyberTrust. He is the Vice President for Marketing and Business Development at GTE CyberTrust, a commercial certificate authority that provides online products and services for securing business over the Internet between corporate Intranets, and also Gordon Ross will participate from our prior panel. Mr. Baum.

MR. BAUM: Good morning. I appreciate the opportunity to be here. I think I'll stand over here and attempt to control these slides as I run through them. Just as a matter of context for those of you that, I should say almost everyone here, appears to have some passing understanding of technology. So given that fact, I'm assuming that many people here have heard something about what are called Certificates or Digital IDs. Here are a few thoughts.

First of all, you can think of Digital IDs, or some people think of them at a very high level as driver's licenses for the Data Super Highway, but having said that, it's also important to understand that you can make these driver's licenses anonymous. Also, please think about the technology in the slides I'm presenting

more in the context of simply being an enabling technology rather than what is presented as being any particular application that is specific and etched in stone.

Also, understand that certificates are something that work very nicely with biometrics and are not a substitute. It's not an if, or an or. Biometric templates, that is, the data making up a biometric, can simply be included in a certificate, and that way you can authenticate over the Internet. Similarly, you can take certificates and put them on Smart Cards. So the point I'm trying to make before I even get started is that this is an enabling technology and should not be viewed in competition with these other technologies, but indeed simply an enhancement.

So quickly about VeriSign, we are perhaps the leading provider of digital certification services. We are based in Mountain View, California, with offices in various places. We have various strategic investors, as you can see up there. We provide authentication for Web sites, for secure electronic mail, such as something that is called

S MOM that is rolling out pretty much everywhere these days. And you will hear a lot about it over the next couple of years. And also simply content authentication.

So when software is downloaded, you can determine who it came from and whether or not it had indeed been modified since the time it was communicated. We have over a million certificates out there, and the important thing is these are actual commercial end-user and consumer certificates, rather than certificates dedicated to a particular government program.

Now, some of the goals that I would like to propose this technology might be helpful in providing -- again, understanding that these are just possible goals -- would be to prevent children from viewing objectionable content, to prevent children from undertaking certain unauthorized electronic commerce activities, such as charging credit cards, and to obtain parental consent to collect marketing data on a child so that if they visit a certain Web site, a parent can actually prevent that from happening.

So I would like to propose that some of the requirements to actually satisfy those goals

1 could include authenticating a child's identity
2 or independently authenticating a child's age.
3 Again, I want to underscore it is possible to
4 create certificates that are anonymous, so you
5 don't really identify the child, but you know
6 that the holder of a particular certificate is
7 indeed a child, or for that matter someone who is
8 over the age of 21 or any age. Certificates can be used to
9 authenticate the relationship between parent and child,
10 and then to authenticate the scope or the extent to
11 which a parent gives authority to undertake
12 particular activities.
13 So I wanted to urge, and I guess it's
14 consistent with some of the things we have heard
15 today, that we have heard about the limitations,
16 albeit the benefits, of blocking technology. And
17 I think we can just mention the actual
18 inadequacy of any kind of an honor system --
19 click here if you are over 21, and
20 for that matter, this notion of password access
21 control.
22 Passwords are great if you have got a
23 prior relationship with a particular site and
24 that might also require that the site
25 actually can authenticate who you are. But when

1 we are really dealing in a global environment as
2 we have heard over and over again, and there will
3 invariably be a consistent use and access of
4 sites, surfing, where the end user or the child
5 has had no prior relationships with the site,
6 which is really the underpinnings of the Internet
7 explosion, then the notion of passwords just
8 really doesn't cut it.
9 So, instead, I think some of the new
10 vocabulary, and some of the things that perhaps
11 might be helpful for the Commission and for this
12 community generally to start thinking about a
13 little more, would be the notions of actually in
14 a more robust fashion authenticating identity,
15 finding mechanisms to explicitly authorize
16 provably certain actions, and to provide for the
17 non-repudiation of transactions.
18 So one way to do that and, in fact,
19 something that most experts will tell you
20 when you go over the Internet is that when you
21 go over an open system where you really lose
22 control because it's out there in the clouds, so
23 to speak, the only mechanism that can provide for
24 assurances of authentication, non-repudiation and
25 the integrity of the data, in fact, is the use of

1 cryptography.
2 It's important to understand when we
3 talk about cryptography, there are two
4 fundamental uses. One is to keep information
5 secret or scramble it. But independent of that
6 is the use of this technology to authenticate.
7 You can actually implement cryptographic methods
8 to authenticate without otherwise scrambling or
9 interfering with the actual text of data.
10 Now, we don't have time during this
11 presentation to get into any kind of a technical
12 review of what public key technology is, but
13 suffice it to say what happens typically is that
14 an end user, whether a parent or a child, can
15 generate their own keys. They keep one key on
16 their computer. They keep one key secret at all
17 times, called the private key, and the public key
18 can be distributed without otherwise disclosing
19 what the private key is. The public key would be
20 used by a site to authenticate the child
21 or parent that is digitally signing a
22 transaction. Again, it's impossible within a few
23 minutes to present this in more detail. Perhaps
24 between what I say and Tom says, we will get a
25 little closer.

1 Now, despite the fact that a person
2 will have a key pair, that is a public and a
3 private key, the real hard thing is how to create
4 a binding or ascertainable relationship between a
5 given key or the digital signatures that are
6 created with a private key, and the person's
7 identity or persona, even if it's maintained on an
8 anonymous basis. That relationship is
9 expressed and authentication activities are
10 undertaken with what is known as a certificate.
11 And the certificate can include various
12 information, and there are various domestic and
13 international standards, but at the highest
14 level, you can just think of a certificate as a
15 digital data structure, just a file, that is
16 digitally signed using this cryptographic
17 process. And it simply includes data
18 that, at a minimum, would include either a
19 real name or a fake name and a public key. And
20 it is digitally signed by a trusted third party.
21 Sometimes we might call them certification
22 authorities.
23 So the content of these certificates
24 or, as I mentioned before, these driver's
25 licenses for the Data Superhighway, can vary

1 immensely. You can think of it as an enabling
2 technology. How the certificates are loaded and
3 the purposes for which they serve are rather
4 remarkable. So let's assume that we get these
5 credentials out there and we can indeed
6 credential children and parents.
7 Let me now just drop down to what some
8 of the tough issues are. First of all, the kind
9 of decisions are going to be made that if we want
10 certificates to be out there ubiquitously, we
11 have got to balance the cost or level in
12 difficulty in actually credentialing people with
13 having, again, the certificates out there
14 ubiquitously.
15 Some of the tough things will be: do we
16 actually allow people to sign up for certificates
17 by going into online databases and paying them,
18 that might have certain information, to
19 authenticate them; do we need these people to
20 actually go to a trusted third party, such as a
21 notary and say hi, here is my identification.
22 This shows my age. Here is my birth certificate;
23 do we need the submission of other documentation
24 directly to the certification authority, or what
25 is called the local registration authority? And

by the way, how accurate does this data have to be?

If you are going to be satisfied to have this ubiquitous, at least national if not international, mechanism to authenticate and say this is an adult or this is a child, how accurate does it have to be? Is it good enough that it will just show who is an adult or a teen or a preteen? Again, the level of accuracy and the confidence that you have in that data will be major policy issues that will invariably affect what we can do as an industry and how quickly we can actually stage this.

Also, you can think about authenticating the parental relationship. That's pretty tough. How do you know an individual really is the parent of another person? And how would you do it online without actually seeing the person? Do we need to get birth certificates? Do we have to go and attempt to get data from the IRS that shows who is a dependent? Is there other investigation that needs to be done?

Again, I could lay out a whole series of possibilities, even something as weak as an

1 authenticated person, so let's say myself. And
2 if I were to say, you would be able to know who I
3 am and come and get me, if I went ahead
4 and made a misrepresentation. But I said
5 X, Y, Z is my child. Is that enough
6 of an assertion so that at least if I was wrong
7 and it blew up later, you would be able to come
8 back and get me? Again, these are a lot of the
9 issues that get to really be explored in terms of
10 what is going to satisfy this marketplace over
11 time.
12 What about the consent to gather
13 information? Switching gears again. More on the
14 technology side, the point here is that
15 certificates are intended to be used and can be
16 used to enable various mechanisms,
17 for example, the OPS. To provide the
18 authentication mechanism in a strong way, who
19 gave the authorization? Where did it come from?
20 Also, again, going back to this issue, if you
21 have any type of authentication information you
22 want to communicate onto the Web, how strong does
23 it have to be? How robust? How provable?
24 Again, these are all possibilities, and it's going
25 to be policy issues that are going to drive that, as

1 well as the user community and, certainly, the
2 government.
3 And so on the commercial side, already
4 VeriSign provides different assurances or levels
5 of certificates that require different levels of
6 effort, different costs and that have different
7 levels of provability of where these certificates
8 come from. And again, the ultimate data
9 and the level of requirements for any
10 particular certificate, call it a Kiddie
11 certificate, can be driven and explicitly
12 laid out independently and on a
13 custom-made basis.
14 Let's assume that the use of
15 certificates indeed has a positive social
16 benefit and that the community determines
17 that perhaps there is a good use for them.
18 Then the question would be, how will
19 this really be staged on a massive level?
20 That is really the tough question. Anybody can
21 go out and say well, come right to me and grab
22 certificates from me. But how do you get certificates
23 out there massively?
24 And so what I would assert is that the
25 certification authorities that will be able to do

1 this must be in what we call the public space. You have
2 got to be able to provide certificates on an open
3 basis. You have got to also assure that
4 the public keys to authenticate the certification
5 authority -- remember the certificates are
6 signed by a certification authority -- must be out
7 there in the browsers and the other end user
8 equipment so that we can properly authenticate
9 the authenticator, if you will.
10 And then finally, the certification
11 authorities that issue these certificates -- if you
12 are going to trust that these certificates duly
13 demonstrate authority, or consent, or a person's
14 age -- you have got to trust the certification
15 authority to do so. I would assert that the
16 certification authority needs to have published
17 practices that they need to adhere to. I
18 left a copy of what is called the Certification
19 Practice Statement for each of the Commissioners
20 this morning, and a Certification Practice
21 statement is a public statement that
22 simply says what the certification authority is
23 going to do, how they are going to do it, and
24 from this perspective, it could be used as a basis
25 of misrepresentation.

MR. PEELER: Finish up.

MR. BAUM: Certificates are available right now. They are being used increasingly. It's just remarkable how the mechanisms to enable them are being implemented almost everywhere. Certificates can be specialized or enhanced to satisfy particular purposes, and this whole market for privacy in the protection of children is simply one. Indeed, a very good one.

Implementing these special certificates, say to protect children, I believe optimally will require public and private sector cooperation; specifically, again, and some other day, this would be a worthy discussion, would be to the extent you want the certificates to be out there ubiquitously, to what extent will there be a compelling need for the certification authorities to gain access to government databases, even in order to affirm information or identity, even if the certificates ultimately are anonymously issued? So, finally, we believe that certificates are indeed a critical part of the solution here, and I think we are really just at the beginning of exploring

how they will be implemented and working in order to satisfy many of the needs that we have heard.

MR. PEELER: Thank you very much. Mr. Carty.

MR. CARTY: Good morning. I would like to thank you for inviting me here this morning. I would also like to say I think Michael did an excellent job in terms of putting the use of certificates in perspective as very much of an enabling technology.

I represent GTE CyberTrust. We are also in the certification authority business, which really is the issuance, if you will, of digital certificates in products that do much the same thing. I would like to begin by saying that it is very clear that the growth, and what is drawing us all here today is just going to continue if you look at the number of people that are online today and the number of people under 18 or so, and this number is expected to grow to 20 million or so certainly by the year 2000 or slightly after 2000.

And the motivation for this is something, if you look at children at the age between 4 and 12, it's

1 attributed to them that they directly influence
2 over $170 billion worth of sales, services and
3 goods today, and that teenagers are driving the
4 equivalent of about $100 billion. Direct
5 influence, that is. That is where the money is.
6 That is where the merchants are going to go and,
7 therefore, Web sites are going to be creative.
8 They are going to attract children too, as a
9 result of that.
10 The approach dealing with controlling
11 access to constitute privacy is typically
12 classified in either opt-out or opt-in types of
13 strategies. An opt-out is more of a default
14 collection of information, if you will, and
15 someone has to take overt action to have that
16 stopped, as opposed to an opt-in approach where
17 one would effectively program what they would
18 like to see before information is collected.
19 But what the opt-in approach really
20 does typically require is an enforcement,
21 effectively at the server level, for those
22 instances where technology is going to employ an
23 enforcement policy at the server, and I think
24 Robin mentioned earlier this morning there will
25 be multiple places of enforcement. In some cases,

1 the browsers. In some cases, the servers. But
2 typically, at the server side.
3 Typically, the information that has
4 been collected in the physical world is listed
5 here, and it is nothing that you haven't
6 seen before. The issue is that we have moved to the
7 electronic world. The embodiment of that
8 information is going to change, clearly. In some
9 cases, the type of information is going to change
10 as well. The point is that the information is
11 going to move to be embodied in digital
12 certificates, as Michael indicated. Digital
13 certificates are effectively a vehicle for
14 carrying information that could be authenticated
15 against, so that someone that needs to rely on
16 that information has a vehicle that they can
17 positively use, that is unforgeable and that
18 hasn't been tampered with, and they can use that
19 information in a trusted type of fashion for
20 making decisions.
21 Other ways of providing identification
22 information also include biometric data. That is
23 up there. As Michael said, these types
24 of technologies can be combined. They can
25 be used separately, but there are distinct

1 advantages and disadvantages when used separately
2 and a tremendous amount of power when they are
3 combined. You will see that evolving in the
4 future.
5 And again, I really believe you are
6 going to see this embodiment of the same
7 information move from PCs to move to
8 Smart Cards. Smart Cards will be able to add the
9 dimension of mobility to individuals so they can be
10 authenticated as they move from things like the
11 game room at the hotel, when they work on their
12 PC at home, so they can bring their credentials
13 or identifying information that one can
14 authenticate with them. There are capabilities
15 today to basically be able to provide digital
16 certificates on Smart Cards.
17 I quickly tried to just state what a
18 digital certificate really is. There is a
19 worldwide standard against which digital
20 certificates are created. Digital certificates
21 are created in an unforgeable manner.
22 Effectively what you are saying is that the
23 contents of the digital certificate are verified,
24 and they are verified by somebody that you trust
25 when you issue them. As a result, others

can then trust the contents of those digital certificates.

They are created in a very unforgeable manner so that, in fact, somebody else can't create that same certificate and the integrity of the information is maintained through the process as well, through the process effectively of a certification authority. Michael talked about signing that certificate. The certification authority represents somebody that you trust. I'll give you an example later of how that may happen in a real world environment with children.

There are a number of different mechanisms. I mentioned biometrics. If used alone, biometrics typically has some disadvantages today. The infrastructure is not quite there yet. We don't have anonymity readers. We don't have, typically, speech recognition software on platforms, et cetera. So it's an infrastructure lag, if you will, in terms of the technology. Not that the biometric technology isn't good. It's just a build-out of that in a ubiquitous type of a way.

In addition to that, if used alone, biometrics

1 requires so much of a centralized database that
2 you will go back and verify the identifying
3 information, the biometric information, again.
4 So typically the biometric information only
5 provides, if you will, identity-type
6 information. However, by using digital
7 certificates, there are multiple options.
8 One is, and it's interesting that
9 Michael and I both picked the same example, in
10 terms of age. Obviously, using identity and age
11 to provide information in a very
12 scrupulous way to a server. The server
13 then, based upon a set of policy rules, can make
14 decisions as to whether in fact this is a person
15 of a particular age level -- be they below 13 or 18
16 or whatever the policy may state -- that can be
17 checked against and verified. So with the server
18 you can check that, in fact, the
19 certificate is valid. You can check the age of
20 the user effectively, and then you can make
21 decisions based upon that age.
22 Other mechanisms and powers of
23 certificates are, not only could certificates
24 provide identity information but they could also
25 contain privilege information. So now you can

1 include in the certificate not only who the
2 individual might be but also what privileges they
3 have. Privileges could be parental consent. It
4 could be what levels, let's say, of a rating
5 system children are allowed to subscribe to, as an
6 example. You could use the movie industry
7 ratings.
8 Everything you need to make that
9 decision then exists within the digital
10 certificate. It doesn't rely on some centralized
11 database that is stored somewhere where everybody
12 might have access to it. So the power of the
13 certificate really is a token that carries with
14 it, not just identifying information but also the
15 privileges, the parental consent or whatever you
16 would like to define as privileges.
17 Michael also made the point, and I
18 think it's critically important, that the
19 identity that I'm talking about here in the
20 digital certificate, it does not have to name the
21 individual. It could be a pseudonym associated
22 with that individual. Once the certificate is
23 issued, and the certificate of the individual
24 person is registered, then in fact we can issue a
25 pseudonym so that the individual's identity is

not disclosed, but the privileges associated with that identity are defined and included and encapsulated in the certificate, and that certificate is made unforgeable, if you will.

One real quick example. How might this certificate be issued? Well, the issuer is some trusted agent, if you will, of the parent in this case, and that could be as an example. There are many ways to issue a certificate, but one example might be the school system or the Department of Education. It It could be the PTA or library or anything that you could define that makes sense is acceptable from a social level based upon the parents' signed letter of consent.

So the parents' signed letter of consent clearly defines what permission you are providing that child, and that is done many times today in the real word. How? Using what is called a local registration authority, if you will. So each school department might have a registration authority, and they already have the information associated with the child. So you are adding to that what privileges you are allowing children to

1 have. And this is a standard part of what is
2 called the certification authority. As
3 Michael said, they exist today. They exist
4 in both our our companies, for example. And
5 when will this happen? This might happen,
6 for example, when you register your child
7 for school.
8 Both GTE CyberTrust and VeriSign have
9 digital certification authority systems
10 that are today issuing digital certificates.
11 Those digital certificates are being used
12 in a number of different applications,
13 some very sensitive applications in
14 the banking community. Certainly they are
15 being used by the credit card companies.
16 Many of you have heard about electronic
17 credit card shopping, as an example. They
18 are being used by corporations. What
19 are they using them for? In all cases,
20 identity, authentication of that identity and
21 then making some access decisions based upon that
22 identity, so we already have in use
23 digital certificates.
24 This diagram is an illustration of what
25 I was talking about. You have a child down here,

1 and this happens to be one instance of a way that
2 it might be ruled out, a child applying for, if
3 you will, a digital certificate. Now, that
4 application would only be granted, the issuance
5 of a digital certificate, if the parents provided
6 some sort of a consent letter, let's say, to the
7 school department, and the school department decides
8 then, based upon that letter that they approve the issuance
9 of the digital certificate. Very simple
10 process. It's getting on the Web. It's filling
11 out a very limited amount of information in terms
12 of that application, and then the certificate is
13 mailed back to the individual. That
14 certificate then contains, if you will, maybe a
15 pseudonym, but would also include privileges
16 associated with the child that have been granted
17 by the parent. And that could then be presented
18 to any Web server who is enforcing a policy of
19 the network in terms of what they will, in fact,
20 allow certain people to do and what they
21 subscribe to.
22 There is a very simple pictorial effect
23 of how to go about implementing it. This same
24 example of a solution is one that, in fact, as I
25 said earlier, is being used in the real

1 world today. They happen to be with some credit
2 card shoppers, as an example.
3 I think I want to close with the fact
4 that digital certificates clearly can provide a
5 solution, I believe, to providing verifiable
6 parent consent. As Michael said, it's an
7 enabling technology. There are a number of
8 different ways that you can use this technology
9 to craft different solutions. The important
10 point is that there are certification authorities
11 out there today. There are, in fact, digital
12 certificates being used in the real world today.
13 What doesn't exist for this type of
14 application is really that the policies need to
15 be enforced at the Web sites in a standard way of
16 having a policy defined, so that then you can
17 create those digital certificates. The digital
18 certificates are based upon a standard and that
19 standard allows for extensions today, so it's
20 very easily incorporated into digital
21 certificates. And I do believe that they will
22 start to even become much more ubiquitous when it
23 starts moving to other technology, such as Smart
24 Cards. Thank you very much.
25 MR. PEELER: Thank you, and our last

presenter, Gordon Ross.

MR. ROSS: I'm currently logging onto the system, and this is a technology which we call BioPassword. It's a biometric technology based on what we call keystroke dynamics. I've been told, congratulations, you have successfully logged on and proved you are who you claim to be. That means my typing, my signature is stored on this computer. So anybody else given my name, which is Gordon Ross, can type it on this machine, and they will be blocked. If anybody wants to come up here and try it, they are more than welcome to.

This technology was developed over the last 15 years. I started off in 1979 with Stanford Research Institute getting involved in the technology. It came from the old days of the telegraph, and in the days when I was in the military, we would send Morse code, and I knew who was sending me code and who it was by the rhythm hitting my ear. In 1979 at Stanford, they worked and developed timing algorithms up until around 1984. In 1985 a private company developed the technology into a hardware device and came to us

in Vancouver for financing, and we financed them in 1989.

To make a long story short, we acquired the technology in late '89 along with the patents and continued development into this software package, which is currently a DOS package. This package was developed in 1993, put on hold because of a requirement and reared its head when the Internet opened up. I went to my Board of Directors and said let's stop this technology development. Let's take our knowledge and develop filtering technology and roll this stuff out later to prevent the kids from being harmed in cyberspace.

I had a hard sell with the Board to put it on hold because it was more or less at that time a high corporate issue with this technology. We are going to be implementing this into Net Nanny and, of course, Net Nanny Pro, which is a networkable version which will be released next week for the corporate. This BioPassword technology will be released probably the first quarter of next year. There will be a demo of BioPassword on the Web in late July, first part of August for anybody to download to

develop a single signature and play with it. It's based on keystroke dynamics.

Biometric technology is really a measure of an individual trait. Simply put, a fingerprint, a palm print and retinal eye scans are examples of biometric technology. The problem with most biometric technologies is they are intrusive. People are afraid of what is going to happen if they give their fingerprints up. What's going to happen with my base print? That print can be digitized and converted and used against me. What will happen with retinal eye scans? To my knowledge, to date, there is no long term medical information on what happens to my eyeball when I'm scanned continuously by a laser. I have weak eyes. I wear glasses, and I'm not about to put my eye in front of a laser to be scanned every time I want access. I do know from my electronic background that electronic technology does fail. You just don't know when.

Currently in use today, the main biometric technologies out there are fingerprint systems. There are also palm print systems in use. Canadian Immigration currently has a system: as a returning resident, you can stick your hand in

there without showing your passport, but that is dependent upon whether you want to give your hand print up or not up. If you don't, then you go through the normal passport patrol.

Malaysia will be implementing palm print technology later this year, mainly, for passport entry control. With respect to voice print technology, IBM has currently released dictating technology. However, voice print technology is still not there for "biometric access and control."

Within the digital industry, and most of us that are involved in it, we know we can take a voice and redigitize it. And when you speak, you will sound like me, so virtually any biometric technology, except the one that belongs to you personally, can be cracked. Fingerprints can be cracked by being scanned and rescanned and regenerated. Voice prints can be cracked. Palm prints can be cracked. The only thing that cannot be cracked in human beings is their internal rhythm. That is where this keystroke dynamics technology came from.

I'm here today to answer any questions on where this is going in the future. BioPassword was mainly developed for access and control along

with digital certificates, which is an add-on to that. Keystroke dynamics will give the individual a true identity when they access the system or go somewhere.

For children and Internet service providers, a child can develop a signature. Most kids can type very well today. A lot better than I can. A lot better than most parents. They are being trained on these terminals. These key strokes that develop a signature can be collected over time, and then one can implement biometrics at any time you wish. Set the time of the day for a week or a month later, and the algorithms that were developed at Stanford are capable of monitoring an individual's pattern of typing throughout the day. In the early days of testing, they had to turn the biometrics off throughout the day because the data entry clerks began to get tired. The screen would come up and ask the clerks to "re-verify" and make sure who was typing on the terminal.

Keystroke dynamics technology is available today. It's being developed into the Windows environment. As I said, this product here is an old DOS product. It was put on hold in '93. We

1 felt we would hold onto it until Windows '95
2 cleaned itself up and Windows NT became a
3 standard.
4 In the future what I see happening is
5 each one of us will have a unique signature.
6 Along with methodologies encryption, such as PGP (Pretty
7 Good Privacy), biometric technology will secure our
8 data to as tight a control as we so choose. That
9 is the amazing thing about technology. A lot of
10 people don't understand the true wonder of it
11 when it is used correctly.
12 On the law enforcement side, they are
13 very concerned today. If you look at Internet
14 business today, how do I collect my taxes? It's
15 becoming a very, very big issue. I cannot put
16 stuff up in cyberspace for sale. As a Canadian
17 company, if I put it up onto an American bulletin
18 board, I no longer collect taxes for my
19 government. Foreign countries are now ordering
20 American goods off the Internet through
21 cyberspace with no collection of taxation. So
22 how do I monitor and control that and get my
23 piece of the pie? Technology is being
24 developed today and will probably be here by the
25 end of this decade that will allow you to monitor

1 and control the flow of information as you deem
2 fit.
3 What we have to do, as I said in the
4 beginning, on the filtering side, is educate
5 people to use filtering software to protect themselves. We
6 are entering into a cashless society. In the
7 future we won't have cash. How do I protect my
8 digital signature cards from being used? How do
9 I protect my credit cards from being used, my
10 Smart Cards from being used? By implementing
11 biometric technology along with the technology
12 that both GTE and VeriSign have presented here
13 today. With that, the individual will be
14 secure.
15 MR. PEELER: Thank you. The outline
16 you put up on the screen for use of the digital
17 certificate as a means of getting parental
18 consent basically would rely on the child or the
19 system forwarding that certificate to the Web
20 site at the time that the inquiry is made?
21 MR. CARTY: The example that I used
22 there was the request for certificate that was
23 made by a child, let's say, to the certification
24 authority or the local registration authority.
25 No certificate would be issued back to the child

1 until approved by whomever the trusted agent might
2 be. Once that was issued back, then that
3 certificate would be used to present the child's
4 identity and for permission into the Web site.
5 MR. PEELER: Can it be used the other
6 way? If a Web site provider said I only want to
7 do business with underage consumers who have
8 their parent's consent to come here, is there
9 some way that the Web site could use this to come
10 back the other way or --
11 MR. CARTY: What has happened is the
12 child is presenting, in effect, a token to the
13 Web site. I'm not quite sure what you mean when you ask
14 can it come back the other way.
15 MR. PEELER: Can the Web site go back
16 to the child and say I want to see your parent's
17 certificate before I grant you access to the site
18 or allow you to provide this information?
19 MR. CARTY: Effectively, the technology
20 is there to do that. What isn't currently there
21 is the software to support that. That is not a
22 major deal. You can link certificates together.
23 You can link the child's certificate to the
24 parent's certificate. You could break apart the
25 identity of the child or the parent and

privileges to separate certificates.

MS. LEVIN: I think what you are getting at, Lee, is that the certificate would have to be ubiquitous at that point; parents would have to already have them. I think Lee is asking if the parent doesn't already have a certificate, could the Web site initiate the certification process?

MR. CARTY: The parent, in fact, doesn't need a certificate in this case. All that is really needed is some form of proof to whoever's going to authorize it, that that child is authorized to have that certificate. The parent doesn't need one.

MR. ROSS: If I understand right, what the ISP, or Internet Service Provider, could do is make a request to the parent and ask, is your kid really allowed in here. That being the case, then with biometric-type technology, the parent would say yes, here is my ID or password. That would be stored on the ISP level, and the file, when that signature is flying up and saying yes, that is the parent of Jimmy, so it is okay, and they would allow that child access. So the technology is working hand in hand

1 together.
2 MR. BAUM: If I might go back to this
3 issue of ubiquity. This stuff has to be widely,
4 massively deployed. And VeriSign has been the
5 primary player of putting certificates out for
6 online registration purposes, specifically to try
7 to get ubiquity. That is what probably
8 distinguishes us from other providers, and we
9 have learned a lot from that. One thing that
10 we have learned, and it's no secret, is how
11 difficult it is to get massive use of any
12 particular technology. If we look at the
13 level of effort -- if it were to write a letter,
14 then you are going to get into, how are you going
15 to authenticate the letter and is it going to get lost in
16 the mail? What is the expense of trying to match
17 that letter up and who makes the decision? What's
18 the level of proof? I could give you a long
19 laundry list. That is why one of the
20 considerations I raised was that if you can get
21 this registration process started by a parent,
22 you have got to authenticate who the parent is,
23 authenticate the relationship between the parent
24 and the child, and then you have got to credential
25 the child. And in order to do that, it will

1 invariably raise questions: what level of proof
2 and what will be the mechanisms, the resources to
3 provide the probative evidence of, and in fact, the
4 assertions that are being made.
5 That is why I coupled back to, to what
6 extent will you require proof and at what
7 levels? And finally, to what extent would even
8 Motor Vehicle Department databases provide proof, and it just
9 starts and goes from there. It could even be as
10 crazy as using the dependency records at the
11 IRS. I'm not advocating any particular methods.
12 I'm simply using these as examples of the
13 difficult issues to get clear authentication on
14 an online basis because my belief is that failure
15 to do this on a fully online basis will just
16 create greater consumer resistance. It may be
17 the only solution, but it will create greater
18 resistance that will only delay the ubiquity
19 that much longer.
20 MR. PEELER: Thank you very much. I
21 want to thank the entire panel for its
22 presentation. Again, if you have used slides or
23 overheads, provide copies of those to us. We
24 will break now and reconvene at 1:30. And I
25 would add for the people in the overflow rooms,

there are some seats in the main room now.

(Whereupon, at 12:30 p.m., the hearing in the above-entitled matter was recessed, to reconvene at 1:30 p.m., this same day.)

PANEL VI: SELF-REGULATORY APPROACHES

"A review of self-regulatory guidelines that address concerns about children's privacy online, including how they define notice and parental involvement, how they are implemented and enforced, and their costs and benefits."

Patricia Faley, Vice President Consumer Affairs, The Direct Marketing Association

Elizabeth Lascoutx, Vice President/Director, Children's Advertising Review Unit of the Better Business Bureau (BBB)

Jeff B. Richards, Executive Director, Interactive Services Association

***

AFTERNOON SESSION

(1:30 p.m.)

MR. PEELER: If everyone will take their seats, we will try to get started.

I want to thank you all for coming back to the final afternoon of the Commission's privacy hearings. This afternoon we will be starting with a panel discussing self-regulatory approaches to children's privacy issues online. Our panelists today include Elizabeth Lascoutx who is the Director of the Children's Advertising Review Unit of the Council of Better Business Bureaus which was established in 1974 by the National Advertising Review Council to promote responsible children's advertising. Elizabeth joined CARU in 1991 as a staff attorney and has been Director of CARU since 1994.

Our second panelist is Pat Faley. Pat is the Vice President of Consumer Affairs of The Direct Marketing Association working out of the Association's Washington, D.C. office. She is responsible for the management of DMA Ethics and Consumer Affairs Department and moving the Association's agenda forward on issues of privacy including online marketing. Pat is also a former

1 FTC employee from a while ago.
2 And finally, sitting in for Jeff
3 Richards is Jill Lesser, who has been another
4 regular on panels all this week. Jill is the
5 Deputy Director of Law and Public Policy in AOL
6 and also serves as Senior Counsel in the AOL
7 legal department. I would like to start
8 by asking each of the panelists to spend about
9 five minutes outlining their self-regulatory
10 programs in the privacy area, and why don't
11 we start with Elizabeth.
12 MS. LASCOUTX: Thank you, Lee. And I
13 want to add my voice to all of the others in
14 thanking the Commission and the staff for
15 convening this whole series of really important
16 workshops. CARU has had self-regulatory
17 guidelines for years now; and as the marketing
18 venues and techniques to kids have changed, we have
19 revisited them and revised them periodically.
20 Some years ago at the same time that
21 this agency was looking at 900 numbers, we wrote
22 a new section for 900 numbers.
23 Two years ago, our Board of Advisors,
24 which comprises leading experts in child
25 development, education, communications and

industry leaders, sat down and began to look at the online environment and to identify where we needed to write new guidelines. The process took a lot longer than we thought, but what we did come out identifying as the critical issue, which was also a brand-new one for us, was privacy. We never dealt with privacy in the offline world. But we realized that where a child is a mouse click away from transacting informational transactions with Web sites that we needed to write some guidelines for our industry.

I think I should point out that we are not a membership industry organization. We don't self-regulate only those people who are members of our organization. We have no members. We consider the entire children's advertising industry to be under our jurisdiction. That is sort of a broad jurisdiction, but we do our best.

The level of compliance that we get with the industry is phenomenal. Quite frankly when I joined CARU six years ago, I was a little bit skeptical about self-regulation. However, I was quickly disabused of that skepticism because

1 all of the major players who know about us have
2 complied with our guidelines; new entrants into
3 the arena who don't know about us, as soon as
4 they are told, they comply with our guidelines;
5 and, of course, we do have the enforcement
6 fallback of referring to this agency or the FCC.
7 I would like to talk a little bit about
8 our goals, specifically about our guidelines.
9 CARU has never set out the means by which
10 advertisers should comply with our
11 guidelines. The guidelines are a set
12 of goals. In terms of the electronic, the new
13 media, the goal in the privacy section is notice
14 and choice to parents. We don't tell the
15 industry how to do that. And because the medium
16 is evolving so quickly, we expect that the
17 guidelines in this section will evolve as quickly,
18 and that the goals that we set which call simply
19 for "reasonable efforts in light of the latest
20 available technology to ensure that parents" -- I
21 shouldn't misquote myself here -- "to ensure that
22 parental permission is obtained." That that is an
23 evolving standard. Maybe two months ago, it was
24 sufficient to, or maybe not, but two months ago,
25 it was sufficient to have in large red letters on

your Web site, Kids, you must be over 18 to answer these questions.

Other sites have found ways of getting a higher degree of certainty that parents are giving permission to an information exchange, so that becomes the threshold standard, and we expect that in two weeks someone else will find another way of achieving a higher degree of certainty and that will become the standard. So our standards are always evolving standards.

And before I pass it over to Pat, I just wanted to say that the self-regulation, which I believe is the answer in this arena for a lot of reasons, that I'm sure you will grill me on later, doesn't exist by itself. The technology component, particularly the P3 platform that we saw this morning, has an enormous potential to really solve a lot of those questions by giving parents an actual opportunity to make those choices for their children before any information is exchanged.

MR. PEELER: Thank you. Pat.

MS. FALEY: Thank you, Lee. I was here over the last couple of days to hear some of our other member marketers talk about how they are

1 addressing privacy concerns about children in
2 cyberspace, and the fact is Time Warner, who
3 spoke yesterday, is very typical of the DMA
4 members. They are proceeding very slowly, but
5 very cautiously and deliberately. And their goal
6 is to assure the trust that the families, that are
7 their customers, place in them.
8 I also heard Dr. Westin and Stan
9 Greenberg describe the complexity of the issue.
10 Parents are clearly deeply concerned about the
11 safety of their children, but also clearly this
12 issue is part of an overall concern and a general
13 feeling of the lack of control parents have over
14 their lives. We do believe the issue is broader
15 than privacy.
16 We also heard Sharon Stover from Texas
17 make a plea for guidance to parents so that they
18 know how to protect their children online, and
19 you heard this morning I understand from P3 and
20 IPWG, a process and a technology which DMA
21 strongly supports and is involved in very much,
22 and we will follow that through the next year to
23 completion.
24 We know that direct marketing has been
25 a wonderful and valuable resource for parents and

1 provides so many benefits from scholarship
2 opportunities, book clubs and career
3 opportunities to products and services.
4 Direct marketing, you know, does provide many
5 conveniences and a great value for many families,
6 but we also know that in cyberspace, probably
7 more than any other medium, parents want help
8 protecting their children.
9 Now, even before this hearing, we knew
10 and it has been reaffirmed here that parents are
11 looking for help, for tools and information so
12 that they can decide their own comfort levels
13 when it comes to privacy so that they can develop
14 the rules for their family.
15 And the more people know about the
16 Internet, we believe the more control they will
17 be able to have over the information that enters
18 and leaves their home. And that is why the DMA
19 created what I personally think is a wonderful
20 resource, "Get Cyber Savvy," to help bring parents
21 up to speed and to teach them how to talk to
22 their children about privacy and the online
23 world.
24 I'm going to show you some pieces of
25 Cyber Savvy in a minute, but first I wanted to

1 talk about the responsibility of direct
2 marketers in protecting children's privacy.
3 Direct marketers build their businesses on
4 consumer trust. Parents trust Highlights For
5 Children and Scholastic and Disney, and these
6 businesses and all responsible marketers
7 recognize the need to be very careful in the
8 traditional world and even more so online. We
9 believe that one of the best ways to protect
10 children is to encourage responsible marketing
11 online.
12 Now, before the FTC had set the agenda
13 for this workshop, we had been trying to learn
14 more about our members' practices. Of about
15 550 consumer marketers that we talked to, 65
16 percent of them or about 350 of them had Web
17 sites that were used for marketing.
18 Among companies that do direct
19 marketing to consumers, whether through
20 traditional media or online, that's marketing in
21 any media, about 15 percent of our marketers
22 market products for children. But of that group,
23 the vast majority, and we're talking 80 to 90
24 percent of that group, direct their message to
25 the parents because they are after all, in

1 general, the ones that are going to be doing the
2 buying.
3 Of the 350 consumer marketers who have
4 a Web site, only 17 of those marketers say that
5 their Web site is directed to an audience of
6 children. And at least one of those is a company
7 that targets high school seniors, who probably
8 don't consider themselves children.
9 A total of 24 marketers said that they
10 thought that the Web site was or might be visited
11 by children. We don't know which companies these
12 were, but I would imagine Columbia House, someone
13 like that that markets to a very broad audience.
14 In the separate telephone survey that
15 we did of 390 companies, 36 or under 10 percent
16 said that they market products for children and
17 only 9 of them directed their sites to children
18 and only two of these sites said they rented or
19 exchanged information from children online.
20 As the Commission well knows, the
21 direct marketing industry has regulated itself
22 very effectively for more than 30
23 years, and we have worked closely with the
24 Commission, and government in general, consumer
25 advocacy organizations and so forth to enforce

1 our guidelines and principles.
2 As part of the DMA online marketing
3 principles, we have focused specifically on
4 children's protection. And last year, if you
5 will remember, we presented to you a draft
6 statement with the ISA. And we are here today to
7 say that our Board has approved the principles,
8 and the DMA has further refined the principles
9 with more specific guidance for our members. And
10 we have also printed up an attractive book, which
11 I didn't bring today but Elizabeth did, which I
12 think has been distributed here, and we have put
13 these into the hands of every one of our members
14 around the world.
15 Our principles, to summarize,
16 support the ability of parents to limit the
17 collection of marketing data through notice
18 and opt-out. Our principles encourage
19 parental permission before furnishing
20 information online. They encourage the
21 implementation of strict security measures
22 against unauthorized access to data collected
23 online from children. And lastly, they
24 support making it very clear that when
25 information is collected, that it is

1 for marketing purposes.
2 Our guidelines are enforced by the DMA
3 ethics review process, which has been described
4 by others earlier. The DMA also understands that
5 it's our responsibility to educate our members
6 about these guidelines and about responsible
7 marketing online. And as you know, this year,
8 the DMA did an aggressive campaign called Privacy
9 Action Now to educate our members about the DMA
10 policies regarding online marketing and
11 children's privacy protections.
12 While the DMA is educating its members,
13 we are also educating parents. It's very
14 important that parents have the information and
15 the education to set rules with the children
16 about the types of information they can and
17 cannot share online. DMA is providing parents
18 with both education and technological tools to do
19 this.
20 In cooperation with Call For Action and
21 our friends from the Children's Advertising
22 Review Unit of the Council of Better Business
23 Bureaus, the DMA launched Cyber Savvy just this
24 week, which is a guide to parenting skills in the
25 digital age. Online basics, behavior and privacy

is what it's all about. It's an interactive tool to help parents learn more about the Internet and to teach the children about safety and behavior and privacy online.

"Get Cyber Savvy" contains five different hands-on exercises that parents and children can work through together to learn about the Internet. And I wanted to just very briefly walk you through these.

We have first an Internet Privacy IQ quiz. This is 10 questions to test a family's knowledge about the Internet. Secondly, we have a family tour of the Internet. This is from E-mail to encryption. This is a guided tour to help parents understand the basics of the Internet in a very simple vocabulary for digitally challenged parents.

"What Should I Do If" is ten real life situations that families may encounter online such as, While surfing the Web, I found a site with an interesting game that I want to play, but before I go any further, I have to fill out a form which asks questions about my interests and hobbies. What should I do? Parents and children will sit down and decide what to do in those

situations.

The next section is How to Talk to Your Family about the Online World. This is a discussion guide. It's really a multiple choice exercise that is a discussion guide for families that helps families know what areas in which they need to set rules and helps them set them.

And our last page is a Family Pledge which is a pledge that families can put in writing to define their own rules to ensure safe and responsible use of the Internet. "Get Cyber Savvy" also helps families handle problems online by providing information on parental control software and on organizations where families can forward Internet complaints.

What is important is that Cyber Savvy is not only available in print, but it's available on the DMA Web site in a special parents section of our Web site. In this area you also find links to the Parental Control software, some of which was described this morning, and it does allow parents an opportunity to oversee their children's access to the Internet.

We are encouraging links to our site to

1 Cyber Savvy, and some of our members have already
2 linked to the site. For example, Time Warner
3 showed you yesterday where it had linked to our
4 site. And so in closing, I just want to say that
5 the DMA plans to continue educating in this area
6 not only to parents, but to teachers and others
7 who will be in a supervisory responsibility role
8 over children. And I think we have learned from
9 the research presented during the Workshop that
10 education really is the key to protecting
11 children online.
12 MR. PEELER: Thank you, Pat.
13 Jill.
14 MS. LESSER: Thank you. I have
15 obviously been here earlier in the week on behalf
16 of America Online. And you heard yesterday my
17 colleague, Bill Burrington, talk about AOL's
18 approach to online privacy and in particular
19 privacy as it relates to children; that we have
20 adopted a "parental consent first" mantra at AOL,
21 and we are trying to figure out how to move that
22 beyond just our company to our information
23 providers and hopefully to the rest of the
24 industry.
25 I am here today, however, to talk as a

1 representative of the Online Policy Committee of
2 the Interactive Services Association ("ISA"), which is a
3 unique association in that it really does
4 represent the entire interactive services
5 industry which goes from online providers like
6 America Online to companies like Netscape and
7 Microsoft, some of the content providers. So ISA
8 has a unique opportunity to reach out to
9 companies who are, in fact, doing business in the
10 medium we are here to talk about today.
11 The ISA sees itself really as a
12 convener for this industry and as a leader in
13 terms of what issues are important both to
14 policy makers and what should be important to the
15 companies. So that what we have done is to put
16 on top of the agenda an issue that we thought,
17 based on last year's hearings, our participation
18 and what we perceive from our participation in
19 Dr. Westin's study as well as our participation
20 in the Internet Privacy Working Group in support
21 of the P3 platform, that privacy is clearly an
22 issue that is central to this industry. We
23 cannot as an interactive services industry or
24 association move forward without the trust of our
25 members and particularly as it relates to

children.

So we have done a number of things. And part of that is to heed what we heard at last year's hearing and what I think we have heard for four days straight over this year's hearing, and that is education. It is absolutely critical, particularly for the industry which has the resources, to get consumers to take the initiative. So what we came here to the FTC with last year was a brochure that we had put out that is available through an 800 number. It is available on the Internet and it is really available in bulk from the Interactive Services Association that was put out by Project Open, which is a joint product of ISA, several of its member companies and the National Consumers League called "Making the Network Network For You."

What we thought after last year's hearing, which this brochure went into a lot of detail about Internet access, about parental controls, about empowering parents to make decisions for their kids, but what we heard last year was it was really privacy that was at the top of everybody's list. That it was not just

about general knowledge of the Net.

While that brochure is still critical and it still exists and parental control is obviously a huge piece of it, there were some fundamental issues that were not covered in the detail that we thought was necessary. So we have recently, in May of this year, put out another brochure called "Protecting Your Privacy When You Go Online" and, again, that is available through a number of different mechanisms.

And we have also throughout Project Open developed camera-ready public service announcements, two of which I have here which I can submit for the record. I apologize for not having overheads. One says, "Before you hit the digital highway, call for a free road map." And the second says, "Give your kid some drivers ed."

And I think what we have seen at the ISA is that when we engage in these kinds of education efforts, we do get the support of large companies: AT&T, Microsoft, Netscape, and AOL.

Now, the other thing that we can do and that we are doing is, again, because we have such a broad membership, is to bring these issues to

the fore for our membership. So at this year's annual conference in July, there is an entire day devoted to online privacy and to the issues that the industry has to look into. And I think what that does is allows us to hear from everybody here, go back to our membership and say, this is a really serious issue. How is this industry going to deal with it and build the industry so that it is an industry built on trust?

Now, we have also heeded your calls from last year and gone back and revised the guidelines that we developed in partnership last year with the Direct Marketing Association. Our new guidelines also refer to the guidelines put out by CARU, and part of the reason that they do that is because we view CARU truthfully as the expert in this area. They have spent a lot of time thinking about guidelines with respect to advertisers and, therefore, it seemed rather than reinventing the wheel, what we should really do is make sure that our members were educated since they are primarily members of a number of different associations. So ISA has members who are advertisers, members who are direct marketers, and so rather than reinventing the

1 wheel, we have basically tried to redo those
2 guidelines to make them clearer and also to get
3 more and more ISA member companies to endorse
4 them and sign on to them.
5 So it is, what I would say from an ISA
6 perspective, an evolving process. If we thought
7 that we had done perfectly, I don't think we
8 would be back here. We are here to report that
9 we have made a lot of progress and that we have
10 heard a lot of new and interesting ideas this
11 week, which again we have to take back to our
12 membership. Some of those companies are already
13 leaders. I would like to think America Online is
14 one of those leaders, but certainly you have
15 heard from Netscape and Microsoft this week about
16 their new initiatives in the area of privacy. So
17 I do think that ISA can continue to act as a
18 convening role and also can continue to act as
19 the segue to the industry from the Federal Trade
20 Commission and from policymakers.
21 MR. PEELER: Thank you, Jill.
22 MS. LESSER: Sure.
23 MR. PEELER: Elizabeth, do your guides
24 require children's Web sites to provide notice to
25 parents when they are collecting identifiable

1 information?
2 MS. LASCOUTX: Yes.
3 MR. PEELER: And when does that notice
4 have to be provided?
5 MS. LASCOUTX: It's supposed to -- we
6 don't specify -- one of the things that we make
7 very clear is that our guidelines are an overlay
8 on the broader and still developing industry
9 guidelines.
10 What we looked at was what was unique
11 to children. The broader industry guidelines,
12 such as the DMA guidelines, provide that there
13 must be notice and choice given. Our guidelines are meant
14 to layer over the existing guidelines. So we
15 don't say the notice should be given before Web sites collect
16 identifiable information. We don't spell it out. But in our
17 guidelines I think it is quite well understood that the notice
18 should be given in a reasonable way in light of
19 the latest available technology.
20 We don't at this point, as I said,
21 require prior parental permission. We believe we
22 will get there. That is certainly the goal and
23 the intent of the guidelines. And I believe we
24 will get there with the help of the
25 technologies. But, at this point, we don't say

1 that that notice has to be given before collection.
2 MR. PEELER: But to comply with your
3 guidelines, a Web site collecting personally
4 identifiable information must give the parent
5 notice of the four things in the DMA guide?
6 MS. LASCOUTX: They must give parents
7 notice of the fact that they are collecting
8 information, what use it's going to be put to,
9 what information the child has provided and that
10 the parent can request that the information be
11 deleted.
12 COMMISSIONER STAREK: Can I follow up
13 on that?
14 MR. PEELER: Yes.
15 COMMISSIONER STAREK: We had a
16 presentation here yesterday by the
17 Center for Media Education and the Consumer
18 Federation of America. I don't know if you are
19 familiar with it, but they looked at
20 about 38 Web sites that were directed
21 to children and were apparently quite popular
22 with children. They analyzed these sites and
23 they are from large marketers, probably several
24 who are members of the DMA. And they pointed out
25 that rarely was any notice given for parental

1 permission or any warnings provided about or
2 disclosures about how the information that they
3 were collecting was going to be used. And so
4 when you said in your presentation that you see a
5 large amount of compliance with your guidelines,
6 I was wondering if you had any thoughts
7 on the presentation that was made yesterday.
8 MS. LASCOUTX: Well, I haven't had a
9 chance to go back and check all of those sites
10 that they looked at. I can tell you right off
11 the top of my head of three sites that are
12 collecting information from children that also are
13 collecting an E-mail address of the parents and
14 are sending the parent a letter that says Your
15 child is registered on our site. This is the
16 information that he or she has given us. These
17 are the uses to which we will put it. We invite
18 you to come visit our site and see what we are
19 doing there. And if you don't want us to have the
20 information, let us know and we will delete it. That is
21 Disney, Mama Media and KidsCom.
22 MR. PEELER: But with respect to these
23 other sites listed here, we don't know whether
24 they --
25 MS. LASCOUTX: I haven't gone back and

1 checked them. One of the things I think is
2 important to understand is that right now we are
3 in this consulting time with the sites. We are
4 calling people up. I got a phone call at my
5 hotel on Tuesday night from two sites, Microsoft
6 and Galoob.
7 Microsoft is in the process of a
8 redesign. They put in some interim changes to
9 address some of our issues and when they do their
10 redesign, they are going to make it more
11 effective. Just a few of the sites: Kellogg's,
12 KidsCom, You Rule School, which is General Mills,
13 Nabisco, and Frito Lay.
14 I ran into somebody from Frito Lay the
15 day after checking out their Web site, and there
16 were a bunch of questions on the site that requested
17 personally identifiable information, and I pointed it out to
18 them. The next day I got a call from Frito
19 Lay saying we have taken those questions off our
20 site.
21 There are an enormous number of sites
22 that we are working with and we are bringing them
23 up to the standard. They are making changes,
24 coming back to us saying is this what you
25 meant? And we would say "no." How can we address

it? So we are working with them.

By the end of the summer I think you will start bringing our cases in the same way as we have in other media having to do with Web sites, but at this point we consider that it's only fair to the industry to work with them as we all figure out what the standards are and what the implementation is.

MR. PEELER: Would you be willing as a follow-up to Commissioner Starek's request to provide us with a little bit more analysis of whether the sites listed here are currently in compliance?

MS. LASCOUTX: Sure.

COMMISSIONER VARNEY: First of all, I want to thank you, all three of you, but particularly CARU and DMA for working so hard and so diligently to come up with guidelines. I asked if you got the guidelines. I know it's been very difficult for you to try and get pen to paper and a consensus of your members to do this, and I think you have both done a spectacular job and your associations and members are to be commended for taking the issues seriously and coming up with the first approach.

1 What I want to talk about is that, the
2 first approach or the starting point. And I
3 don't want to misinterpret what you are saying.
4 These are where you are starting and you have got
5 a goal, at least CARU is saying you are not quite
6 where you want the goal to be. So there is no
7 misunderstanding, is your goal that highly
8 identifiable personal information from children
9 should never be collected and sold without a
10 parent's consent? Is that your ultimate goal?
11 MS. LASCOUTX: Yes, it is.
12 COMMISSIONER VARNEY: And, Pat, is
13 that the ultimate goal with DMA?
14 MS. FALEY: I think you have to look
15 at what is highly personal data from children.
16 Clearly our marketers are very responsible
17 marketers. Trust has been built between the
18 marketers and the consumers over a long period of
19 years.
20 We have looked, and frankly from my
21 consumer background, I can say that whenever I
22 had to address an issue, I would look at whether
23 complaints were filed and what was the harm. And we
24 have looked to see if the child has ever been
25 harmed because their name or some information

about them was on a marketing list, and we can't find that evidence. So I think what we want to do absolutely is protect children from the unscrupulous actors online, and that is what we are trying to do by helping people understand how the medium works and how parents can protect their children.

But we do not think that the fact that a marketer and children are having an interaction is necessarily a negative.

COMMISSIONER VARNEY: So CARU's goal is that highly personal identifiable information from kids should never be collected and sold without a parent's consent, and DMA's goal is well, maybe, maybe not. It depends.

MS. LASCOUTX: The important words there are "and sold." And, again, this is the goal that we want to reach. When the technology is in place, to help with the self-regulatory efforts to make it, what looks to me like, a snap for parents to indicate "yes," "no," their consent out front before a child even goes anywhere near a site selling that child's personally identifiable information -- yes, I think that is a very reasonable standard to apply.

1 COMMISSIONER VARNEY: I think that you
2 point out an important distinction. The question
3 was, should there be a flat-out commitment or
4 prohibition or goal to never collect
5 and sell children's information without
6 parental consent?
7 Let's take the selling part out. Is it
8 okay to collect detailed personally identifiable
9 information from children without their parent's
10 prior consent? Anybody?
11 MS. FALEY: Again, you have a
12 presumption that the collection of any
13 information is on its face a negative, and --
14 COMMISSIONER VARNEY: No, no. I'm
15 asking the question: Is it okay to collect
16 detailed information from children without their
17 parent's prior parental consent?
18 MS. FALEY: I think that if you have a
19 relationship with a marketer that you trust, I
20 think that it is okay to collect some
21 information. The name of the person, for
22 example. I know that in some of the sites I have
23 looked at, we have even the White House
24 collecting the name and age of kids on the Web site.
25 So I don't think that it's

1 necessarily a negative to collect that kind of
2 information from children.
3 MS. LESSER: Can I say one thing which
4 is that I think that one of the points that Pat
5 is pointing out is an important point. And that
6 is that it is difficult to answer that question
7 without some context. So, for example, there are
8 a lot of marketers who are marketing educational
9 materials to kids that are, you know, taking
10 information from kids, for example, in a
11 nonprofit setting, in a school setting, in a
12 White House setting. And so I do think it's
13 difficult to answer that question without some
14 level of context. That is some of the
15 challenge for the industry because if you answer
16 the question in a blanket way, it's difficult
17 to figure out whether you are actually hampering
18 access to, for example, very important
19 information that a kid might need, for example,
20 example, for health reasons or for educational
21 reasons.
22 COMMISSIONER VARNEY: Well, I
23 disagree, Jill. I think when you ask the
24 question in its most basic form, it's much easier
25 to answer. It gets more difficult as you

1 introduce all the gradations. I mean, is it okay
2 to collect the name, the address, the age and the
3 gender of a child under eight without his or her
4 parents' permission? That for me is a fairly
5 easy question. Now, it gets harder. Is it okay
6 to collect the same information from a
7 12-year-old on some sort of site that some people
8 would say is a great site? That may be
9 harder.
10 But, for me, when you ask the question in
11 its most basic manner, I find that the easiest to
12 answer. I find it more difficult to answer as we
13 go up the age range, as we look at the purposes
14 of the information and as we look at the use of
15 the information.
16 MS. LESSER: I actually agree with
17 you. I just think maybe it was in the way you
18 phrased it initially, which is if you ask for a
19 firm commitment. I think ISA and I know AOL
20 would love to be able to give you that firm
21 commitment, and there is always a question of how
22 far you go at a public hearing when you don't
23 understand the ramifications of the context. I
24 agree with you. I mean, every time you ask
25 another question about context, the answers to

your questions get a lot more difficult.

MS. FALEY: Our goal really is to give the parents the control over this process. That is why we are working so hard on the P3 process and the technology to give parents the kind of information they need, to know what their kids do online. Let the parents make the decision as to whether --

COMMISSIONER VARNEY: And what is the default if the parents haven't been involved?

MS. FALEY: The parents can set the browser, set the technology so that --

COMMISSIONER VARNEY: And if the parents don't have the browser?

MS. FALEY: -- so that no information, no personal information could be collected.

COMMISSIONER VARNEY: And if the parents don't have the P3 software, or they don't have the Net Nanny or they don't have anything?

MS. FALEY: I don't think the government should be dictating whether parents --

COMMISSIONER VARNEY: I'm not asking that. Should marketers ever collect name, street address, age and gender from children off of a

1 site that they have targeted to be attractive to
2 children under eight, under 10, under 12 without
3 the parent's prior consent?
4 MS. LASCOUTX: I would say that that is
5 one of the places that CARU and its supporters
6 and advisers and the broader constituents that we
7 work with will work on together. And, personally it
8 would be my hope that that is where we arrive. But
9 in a self-regulatory system, my boss, Wiley
10 O'Brien, loves to quote -- I guess it's his
11 father who said, "Those who would lead can only do
12 so with the consent of those who would follow."
13 And so that is why we are an evolving process and
14 we're working with the industry to bring them
15 along.
16 COMMISSIONER VARNEY: But I get the
17 sense that I think DMA would be, and I don't want
18 to put words in your mouth, DMA would be more
19 comfortable with not such an absolute line
20 whether it's self-regulatory or
21 government imposed regulation.
22 MS. FALEY: Parents should set the
23 rule, not the government.
24 COMMISSIONER VARNEY: And my only
25 question is, if parents don't set the rule for

whatever reason, should marketers or Web operators or anybody then have the ability, unfettered ability, to collect and sell information from kids?

MS. LASCOUTX: I think one of the problems is that if you answer that "no," then you are saying that there can be no data collection because you can never be sure. As I understand the technologies now -- they say P3 exists and two years from now, P3 is in place -- my understanding is that the Web site is not going to know whether the browser has been configured. So what you are effectively doing is initially banning all personally identifiable collection from all children, and by implication, maybe from everybody because there is no way, unless we have got our digital certificates or whatever, of ascertaining for sure whether it's an adult or a child. So I think if you go down that road in that absolute fashion, you are really effectively banning all data collection.

COMMISSIONER VARNEY: What I'm trying to get to is, is there an irreducible minimum, which everybody can agree to? And it doesn't sound like there is, basically.

1 MS. FALEY: The minimum is: Put the
2 parents in control and provide notice and choice
3 to the parents, the notice and the education they
4 need to make the decision. I think that is
5 something we can all agree to.
6 COMMISSIONER VARNEY: Right. But my
7 question is what about when there isn't the
8 parent there. That is where we don't have the
9 agreement. There is no consensus on that, it
10 sounds like.
11 MS. LESSER: Just to comment, and if I
12 could take off my ISA hat and put on my AOL hat
13 for a minute, I think that there is no consensus
14 because while we have all spent the last year
15 thinking about it, we have all started to come
16 to the right conclusions. I mean, what
17 we said yesterday was that as AOL -- and I
18 think Elizabeth's quote is interesting -- as
19 AOL tries to say we want to have a parental
20 consent first policy, we need to look around
21 us and say well, we also have partnerships
22 with other people in the industry. We link
23 link to folks with whom we have no
24 partnership, and so there are additional
25 challenges which you lead to a certain extent.

1 You bring people along, I think, four steps, and
2 then you get four steps, you are on the same page,
3 and you try to move to six steps or 10 steps.
4 That is really half an answer
5 to you, Commissioner Varney, and I admit
6 that that is half an answer. I can't answer more
7 extensively for ISA truthfully because I don't
8 think there is a good ISA answer out there yet.
9 But I think if I see it from my company, the
10 struggle that my company has gone through, that
11 is a struggle that says we have realized what
12 trust means and we have realized what our
13 relationship to our customers mean. And
14 therefore, here is where our policies need to
15 be.
16 But again, the relationships you have
17 with other members of the industry, who really
18 just want to transfer everything from the offline
19 into the online world and don't necessarily yet
20 comprehend the true dynamics of the online world,
21 you know what we say at America Online. We
22 understand those dynamics, so we are in a perfect
23 position to take a leadership role.
24 Unfortunately, it takes probably too much time,
25 but we hope that six months or a year from now we

can come back and say we did it.

COMMISSIONER STAREK: Elizabeth, I think the approach that you outlined -- working closely with industry in trying to bring industry into conformance with your guidelines is exactly right, and I think your timetable is a good one by the end of the summer.

I would also like to say a word about the DMA's Cyber Savvy. I think that is an outstanding publication and one that I intend to use with my six-year-old when she goes online. So I really thank you for that. I think it's excellent and I was thrilled to receive it.

COMMISSIONER VARNEY: I want to go back and I want to give Pat the opportunity to really talk to us for the record so that we can, as we deliberate -- tell us in the most positive way the circumstances under which you think that it is okay for 12-year-olds to be engaging in interaction where information is collected without parental involvement because I'm sure you have some, and I do want you to give us those.

MS. FALEY: I think that you have to put it in context. If a first name is collected, is that a negative? I don't think so.

1 COMMISSIONER VARNEY: I mean, give us a
2 site. Give us a site that you think in your
3 judgment --
4 MS. FALEY: Well, we looked at Time
5 Warner yesterday. They had the first name, I
6 guess a first initial and the last name, and they
7 entered a contest and they had a prize, and I
8 thought that was terrific. But our bottom
9 line is that we need to place our trust in
10 the parents. It's very difficult for parents
11 to parent in this new online environment
12 because many of them don't understand
13 how the forums work, how information flows. But
14 I think once parents understand how the
15 information flows, they will be there by their
16 child's side when they are online and take
17 control if they have any problem of trust with
18 their child. That is really the bottom line. I
19 don't think that the government should be making
20 an across-the-board statement about there shall
21 be no collection. There's a difference between a
22 12-year-old and a 17-year-old.
23 COMMISSIONER VARNEY: I want to
24 emphasize I'm not saying or suggesting the
25 government should make the statement. I'm asking

1 why if industry hasn't, it hasn't. That is my
2 question.
3 MS. FALEY: Industry has made the
4 statement that we think that parental permission
5 should be sought before furnishing information
6 online. And we even have in our guidelines an
7 example of notice to parents and what that looks
8 like.
9 The whole goal is to bring the parent
10 in to the child's process. It's our guideline.
11 We support the ability of parents to allow the
12 children to opt-out of the marketing process. We
13 are encouraging the involvement of the parent in
14 the child's online process. We want to educate
15 parents and give them the tools to make decisions
16 about the child's behavior online, and that's
17 where we think it should be.
18 MR. PEELER: Pat, in terms of the
19 notice to the parent, where is that given
20 to the parent on a typical Web site that is
21 asking for information about a child?
22 MS. FALEY: Well, we say that the
23 notice should be easy to find, easy to read and
24 easy to understand. So those are our
25 guidelines. When we put our own Direct Marketing

1 Association notice up, we put a privacy notice
2 lock and key on the first page of our home page
3 so that it could be just that, easy to find, read
4 and understand. So we believe that the notices,
5 any notices, should be easy to find.
6 MR. PEELER: But the parent really has
7 to go to the Web site. A parent has to know the
8 Web site.
9 MS. FALEY: Now the parent does, but as
10 I said, we're working on technologies that on
11 down the line will empower parents to make
12 decisions beforehand to set their privacy
13 preferences for them and for their families, but
14 that is the future. So we have the stopgap method of
15 let's have the notices. The President
16 demonstrated our privacy policy tool, which we
17 have created for businesses to use today for free,
18 to state the privacy policies to parents or
19 children. We are supporting IPWG and P3. In a
20 year we are going to have the technology that is
21 going to meet that concern. But that is what
22 we're working toward.
23 MR. PEELER: I guess the point I'm
24 trying to make is right now the notice is really
25 to the child. It would only go to the parent if

1 the parent goes to the site also.
2 MS. FALEY: Yes. We are trying to
3 encourage the parents to go to the site with the
4 child.
5 MR. PEELER: Elizabeth, we have been
6 told by some very large marketers that as long as
7 the site displays, Ask your parent's permission
8 before you supply this information, that complies
9 with the CARU guides. That is incorrect?
10 MS. LASCOUTX: I would say that that is
11 incorrect. We want more than that. I think
12 that is an analogy from the television world
13 where there is an 800 number on the screen and
14 marketers are supposed to say Remember,
15 kids, ask your parents' permission before you
16 call.
17 Again, one of the things that is
18 happening in this discussion and education and
19 consultation period is that we are learning. Not
20 only are we educating our constituency about what
21 our guidelines are, but we are learning from them
22 what is possible, and again, it's bringing that
23 along. But I would say yes, that we would
24 require some effort beyond just saying Ask your
25 parents' permission.

1 MR. PEELER: Again, one other
2 thing -- CARU actually monitors sites
3 affirmatively?
4 MS. LASCOUTX: I'm loathe to say
5 monitor because I consider what we do in the
6 television model to be monitoring, and over a
7 week and a half I think we see just about every
8 commercial that is out there for kids. We are
9 patrolling the Internet for kids, looking at and
10 starting with our supporter sites, then other
11 well-known marketers, linking up from there to
12 anywhere they may go.
13 We are encouraging people to bring us
14 inquiries about online practices that they feel
15 might not comply with our guidelines where we
16 take competitor challenges. We haven't gotten
17 any yet, but I suspect we will as soon as
18 marketers are as familiar with this venue as
19 others.
20 And in the Cyber Savvy guide, our name is
21 there as a source for complaints and
22 inquiries about Web practices. I would welcome
23 referrals from anyone in this room or any of the
24 organizations in this room to help us in our
25 monitoring of the Internet because it is a

1 daunting challenge. But we are patrolling sites -- this is
2 about what I can say now.
3 MR. PEELER: Pat, do you react mainly
4 in response to complaints, or do you go out and
5 look for sites?
6 MS. FALEY: It happens both ways. We
7 actually have someone on staff right now that has
8 been monitoring sites, contacting sites of our
9 members, contacting them if they are not
10 absolutely in compliance with our guidelines and
11 bringing them into compliance. We also have an
12 ethics process which has been described to you
13 before, and those complaints can be
14 self-initiated by staff or members or consumer
15 groups or, as Elizabeth said very often
16 competitors.
17 MS. LASCOUTX: I just want to add that
18 the other thing that we do is we will look at a
19 site before it goes out, while it's still in
20 beta. Advertisers, just as they have in other
21 media, will come to us either with something as
22 informal an as idea, we are thinking of doing
23 this at our site, would that be all right? Or
24 actually saying we are about to go live, would
25 you look at our site? So there are a lot of ways

that if we don't initiate it, sometimes the actual Web site initiates it.

MR. PEELER: Jill, does ISA have any type of enforcement of its guide?

MS. LESSER: Not at this time and that is because ISA completed the revamping of its guide about a month ago, and so one of the things that we are in the process of doing in the Privacy Subcommittee of the Online Policy Committee is figuring out, particularly because of the diversity of membership within the ISA, exactly how we can enforce those guidelines because they are comprehensive in the sense that they are guidelines for online marketers. They are guidelines for online service providers, which are different guidelines. They are guidelines for children's information and unsolicited mail. We are in the process of figuring out what the best enforcement mechanism is.

MR. PEELER: The relationship between the three sets of guidelines, I think starting with Jill, your guidelines refer to the CARU guidelines?

MS. LESSER: Right. Last year when we

1 came on to present, we presented joint guidelines
2 with The Direct Marketing Association, and we
3 have made some changes primarily for clarity
4 sake. There was some language we thought in last
5 year's last draft, which was obviously a draft,
6 that was not as clear as it could be, and I know
7 that The Direct Marketing Association went and
8 expanded a version for itself, so we have not
9 split ranks.
10 In addition, as I said before, because
11 we think that CARU has a lot of credibility in
12 the advertising arena and because they have done
13 a lot of the best thinking about children's
14 advertising in particular as distinguished
15 necessarily from marketing, we have asked our
16 members to refer to their guidelines rather than
17 simply reinventing the wheel.
18 MS. FALEY: I think Jill explained how
19 we developed our guidelines. We provided further
20 guidance for our members just for clarity sake as
21 much as anything. In terms of the CARU
22 guidelines, we were consulted at one point on
23 these guidelines, and our own guidelines do say
24 that marketers should follow the CARU guidelines
25 advertising practices.

1 MS. LASCOUTX: And not to sound like
2 the emperor of the world here, but if CARU in our
3 patrolling were to find a DMA member or an ISA
4 member who we thought was violating our
5 guidelines, we would after September initiate an
6 inquiry with them and enforce our own
7 guidelines.
8 MR. PEELER: Elizabeth, your guides
9 apply to children aged 12 and under?
10 MS. LASCOUTX: Under age 12.
11 MR. PEELER: I take it the DMA
12 guidelines are higher?
13 MS. FALEY: The DMA guidelines
14 apply to marketers. We haven't set an
15 age specific.
16 MR. PEELER: Is 12 the right age and how do
17 we know that for a child?
18 COMMISSIONER VARNEY: The age would
19 actually be 11.
20 MS. LASCOUTX: It's 11 and under for
21 the CARU guidelines. I understand that age was
22 set, and there may be someone here who knows, to
23 harmonize it with some, I think it may even have
24 been FTC legislation at the time, but I'm not
25 clear on that.

1 COMMISSIONER VARNEY: Commissioner
2 Starek said its probably a 900 number.
3 MR. PEELER: I think it was a 1974 FCC
4 guideline.
5 MS. LASCOUTX: So I understand that
6 that is where our age limit comes from, although
7 it may have predated that because we inherited
8 our guidelines essentially from the Association
9 of National Advertisers. But we felt comfortable
10 with that in the offline world.
11 There has been some very preliminary
12 discussion about the appropriateness of maybe
13 raising the age limit or having a secondary set of
14 guidelines for marketing to older children
15 online. But frankly in the last advisory, that
16 was tabled because we decided to address that
17 some other time after we had some guidelines in
18 place. So that is a discussion and a decision
19 that would be made by CARU's advisory committee.
20 MR. PEELER: A final question is, I
21 take it at this point it is too early for any of
22 you to have numbers on what percentage of sites
23 are following your recommendations with respect
24 to collection of children's information?
25 MS. LASCOUTX: It's too early to say

1 that. Our numbers may not be all that great, but
2 I will tell you that we have not contacted one
3 Web site advertiser who has said well, we don't
4 feel like following your guidelines. The
5 reaction has always been, oh, we weren't thinking
6 about that; gee, that is really an issue; how
7 can we address it? So that is why we are
8 spending this time working with the industry.
9 COMMISSIONER VARNEY: So maybe when you
10 tell us what you find out from contacting
11 the folks in the CME study, maybe they will have
12 had that reaction as well.
13 MS. LASCOUTX: Maybe so.
14 COMMISSIONER VARNEY: I want to say
15 again, although I may not end up in exactly
16 the same place as the three of you do in
17 your guidelines on some very narrow issues
18 I think the guidelines are extremely
19 important. They are a step in the right
20 direction and I hope that they are evolving and
21 that we will keep talking.
22 MR. PEELER: Thank you. And, Pat, you
23 mentioned some very interesting statistics during
24 your presentation. If you have anything you can
25 give us on that, we would love to see that.

MS. FALEY: Sure, I would be happy to.

MR. PEELER: And with that, I think we will close the panel. Thank you very much for your participation, and we will take a 15-minute break.

(Recess.)

PANEL VII - ROUNDTABLE: PERSPECTIVES ON SELF-REGULATION, TECHNOLOGICAL APPROACHES, AND THE ROLE OF THE FTC

"Recommendations for the future including the roles of industry and government.

Charlotte Baecher, Director of Education Services, Consumers Union

Leslie L. Byrne, Director, U.S. Office of Consumer Affairs

Gerald Cerasale, Senior Vice President Government Affairs, The Direct Marketing Association

Julie DeFalco, National Consumer Coalition

Mary Ellen R. Fise, General Counsel, Consumer Federation of America

Daniel L. Jaffe, Executive Vice President, Government Relations, Association of National Advertisers, Inc.

John Kamp, Coalition for Advertising Supported Information and Entertainment (CASIE)

Elizabeth Lascoutx, Vice President/Director, Children's Advertising Review Unit of the Better Business Bureaus (CARU)

William MacLeod, Outside Counsel, Grocery Manufacturers

1 Association
2 **Kathryn Montgomery,** President, Center for Media
3 Education
4 **Deirdre Mulligan,** Staff Counsel, Center for Democracy
5 and Technology
6 **Marc Rotenberg,** Director, Electronic Privacy Information
7 Center
8 **Shirley Sarna,** Assistant Attorney General, New York
9 Department of Law, National Association of Attorneys
10 General
11 MS. SCHWARTZ: If everyone will take
12 their seats, we will begin the round table.
13 My name is Teresa Schwartz. I'm
14 the Deputy Director of the Consumer Protection
15 and although this is the very last session,
16 it's my first day and time at the
17 table. But for many sitting around the table,
18 you have been here for days and days
19 participating and enriching this record, and we
20 appreciate everyone's staying power and we
21 welcome some to the table who have not been
22 participants but who have been in the audience.
23 The purpose of this round table is
24 really twofold. One is to give an opportunity to
25 react to the earlier presentations about the

technologies and the self-regulatory initiatives that we have just heard about and then secondly, to talk about the broader issue, where do we go from here in this area.

The way I would like to run this, we have got 13 people, so a quick mathematical calculation tells me that we have to stay under 10 minutes a person. To make it a roundtable and to make it interactive, which is where we are in our society this day and age, I want to start by calling on Mary Ellen Fise from the Consumer Federation to begin the discussion and give us her reaction to the industry's self-regulation and technological presentations earlier today, and then for those who would find something in her presentation that they might like to address, to put your sign on the end and I'll try to call on people, to keep the dialogue going and interactive. If no one has a sign on a side, I will just call on people randomly.

So Mary Ellen, would you like to begin the discussion? And keeping in mind that I know you have a good bit to say, but also that we have

1 some time limits.
2 MS. FISE: Thanks. I would like to
3 make comments in two general areas. First to
4 talk about the differences between the guidelines
5 that CME and CFA had asked the Federal Trade
6 Commission to issue and compare that to what we
7 just heard from CARU and also some general
8 comments about where do we go from here. But
9 first in comparing the two sets of guidelines, I
10 just wanted to kind of highlight because they
11 really are very different, and we have set this
12 all out in writing and submitted it to the
13 Commission, and at some point there were copies
14 outside.
15 First, on scope, the CARU guidelines
16 apply to children 11 years of age and younger,
17 and the CMA/CFA guidelines apply to children under the age of
18 16. But also, in terms of scope, CARU repeatedly refers to
19 advertisers and talks about things in the advertising concept,
20 whereas our guidelines refer to marketing. Our guidelines
21 would include advertisers, but it would also
22 include marketers and those who collect
23 information who may not be advertisers, and so
24 those performing market research, we believe, need
25 to be under the ambit of these guidelines.

1 With respect to consent, we have been talking
2 about this a lot over the last couple of days. The
3 CME/CFA guidelines call for valid parental
4 consent, meaning parental consent that can be
5 verified; whereas, the CARU guidelines talk about
6 making reasonable efforts. And we are greatly
7 concerned that those reasonable efforts
8 would implicitly condone a child saying that
9 they got consent when, in fact, they
10 haven't.
11 On disclosure, CARU appears to be
12 silent with respect to disclosure requirements on
13 aggregate and anonymous information collection,
14 whereas our disclosure requirements would apply
15 even in the collection of aggregate and
16 anonymous information. We want people to know, we want
17 families to know that, children to know that this
18 information is being collected even if it doesn't
19 include personally identifiable information.
20 With respect, though, to personally
21 identifiable information, we believe that the
22 CARU guidelines fall short. They don't address
23 things like the size, placement, audio. We in
24 the CME/CFA guidelines call for those disclosures
25 to be directly preceding collection. Also, the

1 CARU guidelines do not address contract claims,
2 it does not address allowing the correction of
3 information and they do not address prevention,
4 preventing further use of the information that
5 had already been disclosed.
6 And then finally, on enforcement, this
7 is a major difference, we are asking the Federal
8 Trade Commission, the federal government to issue
9 guidelines that would set a level playing field
10 and that would be enforceable if a company
11 violated those guidelines; whereas, CARU's
12 self-regulatory program calls upon the
13 industry to do it themselves, and the enforcement
14 wouldn't be by CARU.
15 And Elizabeth referred to patrolling
16 well-known marketers as, I think, the starting
17 place. And while that certainly is a start, it
18 is certainly not adequate in our estimation.
19 Now, more generally, kind of where do
20 we go from here? We have heard overwhelming
21 support through the survey data. We could not
22 have hoped for better response. Particularly, I
23 think one was in the 96 percent range and one in
24 the 97 percent range about the concerns that
25 parents have when marketers would violate

1 collection practices and the fact that they would
2 want there to be legal liability for marketers
3 who violate privacy policies.
4 In terms of the Federal Trade
5 Commission, our sense is that there appears to be
6 a growing consensus and we are very delighted
7 that there seems to be a majority of the
8 Commissioners who are truly concerned and believe
9 that it is possible that the collection of
10 information from children in certain
11 circumstances could be unfair, deceptive or
12 fraudulent. With that said, though, it's been
13 two years, and we have been waiting for
14 guidelines. We have been waiting for industry to
15 clean up their practices. And I think the data
16 that we provided yesterday clearly shows that
17 there is widespread collection of data or
18 information from children.
19 We believe that there is information
20 both through the survey data and from the current
21 practices that is sufficient that the Commission
22 could issue those guidelines today. And
23 we believe that they should go forward in
24 considering that as the response.
25 But in addition to that, we believe the

1 Commission needs to be looking at individual bad
2 actors and going after them for, again, deceptive
3 practices, fraudulent practices, unfair practices
4 aimed at children.
5 And I guess I'll close by saying that
6 more children are going online every day, and we
7 can't be waiting around for yet another year.
8 And so we will be looking to see and hoping that
9 the Commission will take action. But if that is
10 not the case, we will be seeking legislation on
11 Capitol Hill at least to motivate the Commission
12 to take strong action to protect children.
13 MS. SCHWARTZ: Elizabeth Lascoutx from
14 CARU.
15 MS. LASCOUTX: Thank you. I'm going to
16 try to respond to several of the points that Mary
17 Ellen made. I'm not sure I scribbled them all
18 down fast enough.
19 Let me start by just correcting a
20 couple of misapprehensions here. We don't just
21 address personally identifiable information. Our
22 first data collection, our first and second data
23 collection guidelines say before asking children
24 for information about themselves, advertisers
25 should remind children to ask a parent for

1 permission and the advertiser should disclose in
2 language easily understood by a child why the
3 information is being requested and whether this
4 information is intended to be shared, sold or
5 distributed outside the collecting advertiser
6 company.
7 The third one says that if information
8 is collected from children through passive means,
9 e.g., navigational tracking tools, browser files,
10 et cetera, this should be disclosed to the child
11 and parent along with what information is being
12 collected. So taken together, those guidelines
13 say that any time there is information collected
14 from children, that use has to be disclosed.
15 In terms of enforcement, it is true we
16 are a self-regulatory system, and some of our
17 guidelines have a legislative backup if we deal
18 with -- I'm talking about our preexisting
19 guidelines -- if we deal with deceptive
20 practices, we can certainly refer noncompliance
21 to this agency.
22 A lot of our guidelines have absolutely
23 no parallel anywhere else. They deal with things
24 like peer pressure, or inappropriate behavior or
25 prosocial role modeling, and there is

1 nowhere else for us to refer those if a company
2 won't comply with our request for modification or
3 discontinuance. We get an almost total level of
4 compliance on those guideline issues as well. In
5 fact, I think it was last year, the day that we
6 closed out a case against a series of Nintendo
7 commercials, we received a complaint about those
8 commercials referred to us from this agency
9 because we had jurisdiction and this agency did
10 not.
11 So I think the track record, the
12 23-year track record of CARU and its enforcement
13 is pretty darn good, and we don't operate in a
14 vacuum. We don't operate in the dark. The
15 results of our inquiries are published. I think
16 public opprobrium for advertisers really does
17 matter. They don't like being held up to bad
18 press. And we do publish all of our case
19 inquiries. And I think enforcement has really
20 not been an issue. And in the case of bad
21 actors, this agency does currently have
22 jurisdiction to go after them on all the grounds
23 that we have discussed earlier today.
24 In terms of your comment that you are still seeing
25 abuses that the industry isn't following our

1 guidelines, our guidelines have been out for a
2 month and a half, just about a month and a half,
3 and I think I addressed earlier that we are in a
4 work in process with the industry, and we are
5 seeing an enormous number of changes made
6 already. Companies that have never worked with
7 us before, like Microsoft, that they made
8 immediate changes to their sites as an interim
9 while they are doing their major redesign -- and
10 they intend to take into account our guidelines --
11 is an indication that we have some clout and that
12 we are getting cooperation.
13 In terms of our patrolling, I would
14 love to get -- we are starting where we can and
15 we are moving out. But we are going to be
16 relying, as I said, on other referrals, and I
17 would welcome referrals from you if you think
18 there are sites violating our guidelines.
19 I do have a question for you, though,
20 because I have not yet heard defined what CFA/
21 CMA means by valid parental consent or
22 verifiable parental consent. I don't
23 know what you mean by that, whether P3
24 would satisfy you. I haven't heard verifiable parental
25 consent defined.

1 MS. FISE: Our guidelines define verifiable parental
2 consent as in writing or an electronic means that assures
3 the veracity of that consent. I think Shelley
4 probably will be discussing P3 later.
5 But if you go back to the guidelines
6 that we submitted at hearings here one year ago,
7 the consent was laid out pretty explicitly.
8 MS. SCHWARTZ: In the order in which
9 the signs have gone up, Charlotte Baecher from
10 Consumers Union and John Kamp from CASIE.
11 MS. BAECHER: I want to expand. One of
12 the biggest flaws in the whole concept of
13 self-regulation, I think, is its extraordinary
14 reliance on the parent. It puts a tremendous
15 onus on the parent, and there are several things
16 that have to be taken into consideration. Let's
17 call it a reality check.
18 Let's start with the area that I'm most
19 familiar with. I'm dealing with kids themselves,
20 the subject of our concern day in and day out.
21 Telling a child to get parental consent is far
22 from getting parental consent. We have all been
23 children. You are only going to ask your mom for
24 parental consent if you know she is going to give
25 it. If you can go right ahead and go in, it's

1 not any kind of a deterrent at all to a child.
2 So even though we don't have an easily definable
3 method of getting verifiable prior parental
4 consent, that is really necessary, otherwise this
5 is really just show.
6 And I think that there are several
7 other things where the child him or herself is
8 being penalized because if a parent says "no" and
9 really enforces it -- using blocking software,
10 using privacy preferences, whatever technology is
11 available -- the child is going to be bearing the
12 brunt of whatever is going on, and the child is
13 not going to be able to go to a game the child
14 wants to because the child cannot reveal
15 personal information. Basically, the child's
16 options on the Internet are going to be limited by
17 this and rather than having it reinforced that
18 privacy is a good thing to protect, the reverse
19 is going to be happening where the child is going
20 to feel somehow slighted.
21 I think everyone here who has tried to
22 tell a child, "no," you can't have this; you can't
23 do this, has heard but Mom, everybody's got it; I'm going
24 to go over to Johnny's; I'm going to get it there.
25 There are a tremendous number of real life

1 reality checks, things to keep in mind.
2 Another problem with putting the whole
3 onus on the parent is, what I think we have seen
4 over these past two days, the lack so far of
5 parental use of the technology. And even though
6 there is very exciting technology coming in the
7 future, until we can say that we are going to
8 have 100 percent compliance, it's really leaving
9 children unprotected. And is it all right? Is
10 it all right that, say, 50 percent of the
11 parents comply? Is it all right that millions
12 and millions of children are left unprotected
13 because the parents are not taking an active
14 role?
15 I guess finally, probably one of the
16 biggest problems in expecting self-regulation to
17 take care of this problem is a very basic
18 marketplace fact that to do what is good for
19 children means making less money than you could
20 make if you weren't doing the honorable thing.
21 And somehow by requesting verifiable prior
22 parental consent, you are going to be penalizing
23 the Web sites that are going to be getting fewer
24 hits where the kids are not going to be able to
25 go until a parent says yes, and the site itself

1 will be forced to pay some of the consequences of
2 its privacy or nonprivacy policy. So I think
3 that it's very obvious that there is a very
4 strong role to be played by the Federal Trade
5 Commission in protecting children. So it's a
6 very important issue, and I don't think it's one
7 that we can continually put off.
8 MS. SCHWARTZ: John Kamp, then in
9 the order of signs, Shirley Sarna, Dan Jaffe,
10 Gerry Cerasale, Julie DeFalco, and back to
11 Elizabeth.
12 MR. KAMP: Thank you. I promise to
13 make it short. It has to be a little longer
14 given I have to respond, I think, to a couple
15 things that were just said.
16 First of all, I think you have to
17 understand that the business community as I
18 experience it through CASIE, my group and the
19 American Association of Advertising Agencies
20 doesn't see the treatment of children in
21 appropriate ways as something that is against
22 their business interest. The business interest
23 of the 4-As community and the business and the
24 community, the business community that has been
25 represented here, businesses understand that if

1 privacy is not protected in this country, in
2 whatever medium, that the American people won't
3 use the medium, and that would be a disaster I
4 think for all of us. So I just can't buy that
5 dichotomy.
6 I also was a little bit uncomfortable
7 with the need, the sort of notion just
8 expressed that we need to have sort of 100
9 percent compliance. I was raised Catholic, and I
10 know that the nuns that raised me thought that I
11 had to be 100 percent compliant. But even in the
12 Catholic Church we were allowed to go to
13 confession. When we occasionally made a mistake,
14 we had to confess it to the priest.
15 This is not a perfect world and to
16 expect or even call for or expect that the FCC,
17 the FTC or self-regulation or software or any of
18 these things that we are doing would sort of in
19 100 percent ways protect children, I think, is just
20 totally unrealistic. And in fact, even when we
21 were talking about the age differences,
22 in my own case, I knew that by the time my
23 children reached age 11, that I had absolutely no
24 power. By that time I had either sort of raised
25 them to do what they were going to do, but they

1 were going to do it actually from 11 on pretty
2 much in spite of anything that I wanted them to
3 do. So let's not pretend we have a perfect
4 world.
5 I also was a little concerned about the
6 opening. I do think there was some use to
7 the contrasts between what may be the
8 position of the CFA, an institution that I very much
9 respect, and the self-regulation of CARU. But we
10 are not talking about sort of one or the other.
11 We are not talking about will there be government
12 regulation. Clearly, there is and there will
13 continue to be a very strong Federal Trade
14 Commission in this country. And when
15 appropriate, action must be taken. It will be
16 taken.
17 What we are talking about is a whole
18 series of tools here that are being created
19 sometimes by the industry, sometimes by
20 advertisers or different kinds of marketers,
21 sometimes by the Internet service providers. We
22 hope most often by parents who are able to take
23 advantage of these tools, but it's not one or the
24 other. We clearly need it all, and we need to go
25 forward as quickly as possible.

1 MS. SCHWARTZ: Shirley Sarna with the
2 New York Attorney General's office.
3 MS. SARNA: Thank you. I want to
4 underscore something that John said, and I hope
5 that we don't lose sight of it. Through this
6 week and as we go forward, there is no 100
7 percent perfect solution. If nothing else
8 that we have learned in the last week, we
9 have come to appreciate to an exquisite degree
10 how incredibly complex this issue is. How
11 incredibly complex it is to think about a new
12 medium and try and get a handle on applying
13 concepts that really are core values in our
14 society and translating those core value concepts
15 in a new environment.
16 Deirdre at some point, invited us
17 to think about the online environment with
18 no preconceived notions. That is to say,
19 not to think by analogy, but to really
20 allow ourselves to be freer and think
21 creatively as we go forward. I want to
22 expand that by saying I agree, but at
23 the same time I wouldn't like us to
24 foreclose going by analogy.
25 There is much in the offline world that

is already in place that in many ways reflects the values that are part of our society, and many of those values are encompassed in the kind of ground rules of us as a society.

So this is what I would like to add to this discussion. I am, I remain, I have been for as long as I remember, a great advocate of self-regulation. It's been my observation that self-regulation works exceedingly well when there is something underneath it that defines a common baseline. I think, for example, the National Advertising Division, CARU does an extraordinary job. And what works particularly well is that from the baseline, you have provided something additional that you urge your members to participate in, that can give them a competitive advantage and that really looks to a public interest piece of the way that marketers do business. And I think that marketers are genuinely committed to trying to do that, but there are a lot of things to juggle all at the same time.

When push comes to shove and something doesn't get resolved, for example, at the NAD and a marketer and advertiser doesn't comply with an

1 ultimate decision, that file gets floated up for
2 the FTC to take a look at, for the Attorney
3 General to take a look at it, and there is kind
4 of a safety net.
5 When we are talking about privacy and,
6 for example, one of the issues was disclosure.
7 We have no problem when we are talking in terms
8 of enforcement arsenal. We have no problem where
9 we are talking about a deceptive statement. I
10 promise to do this and, in fact, I deliver
11 something different. I say that that is the easy
12 case.
13 I said the other day and I continue to
14 believe and because this is children we are
15 talking about, the issue is even more compelling,
16 where what we are talking about is a disclosure
17 that sets out privacy considerations, for
18 example. I don't think that there is an
19 adequate -- maybe there is -- safety net
20 as a matter of law.
21 The Federal Trade Commission, because
22 it has such a broad range of enforcement tools,
23 has in its arsenal the opportunity for
24 guidelines. Violation of a guideline does not
25 necessarily mean a violation of law. But

1 compliance with a guideline is a safe harbor.
2 Also, as in the environmental
3 guidelines, it's easy to build in a review
4 process. I wonder whether the Federal Trade
5 Commission might consider in this very important
6 area, where time maybe isn't as much our friend as
7 it is in other parts of our last four-day
8 discussion, whether it might be worthwhile to think about
9 adding the public interest point of view, the
10 normative point of view that says, take into
11 account what everyone has to bring to the table.
12 Here is what we would like to suggest
13 for the next three years as a way to proceed. It
14 would have the most notoriety. It would have an
15 opportunity for comment and input, and it would
16 have an opportunity for review.
17 I find myself amused with my own
18 reaction because I came in as such a staunch,
19 such a staunch defender of self-regulation, and
20 now at the end of the day, I wonder why whenever
21 I want to think government, I have to whisper
22 because that has become an unacceptable concept.
23 I think when we are talking about issues like
24 privacy, like providing information and asking a
25 particularly vulnerable group to provide

1 information in an imperfect world of
2 understanding, why shouldn't there be a forum for
3 a bigger picture point of view for some guidance
4 that doesn't look only to what becomes how far
5 the leaders, as AOL mentioned this morning, how
6 far the leaders can bring along everyone else,
7 but sets a standard and says this seems to make
8 some sense. I think we should go with this. See
9 how it works and then come back for review.
10 MS. SCHWARTZ: John, we have a
11 convert. Here we started with a Catholic. Now
12 we have a convert.
13 MS. SARNA: But wait, the day hasn't
14 ended.
15 MS. SCHWARTZ: We're still in this
16 process. Let me see where I am on the list. Dan
17 Jaffe from the Association of National
18 Advertisers.
19 MR. JAFFE: Thank you. I'd just like
20 to echo a couple of things that John said that I
21 thought were important. Our industry, the
22 advertiser industry and the agency industry
23 believes that if we cannot resolve this issue
24 appropriately, in other words, to the
25 satisfaction of the general public and to the FTC

1 and other groups, that we will fail in the
2 marketplace. That if the public does not feel
3 secure in the Internet, they will not purchase
4 products, and that will obviously be to the great
5 detriment of advertisers and the great detriment
6 of their agencies that they use in trying to make
7 sales, and so we think there is an enormous
8 economic incentive to move forward.
9 We believe the FTC in last year's workshop
10 and in this workshop has moved the ball forward.
11 It has taken quite some time for our industry to
12 come up with rules but we now have rules for
13 children's advertising on the Internet, something
14 we did not have at all when we met last year.
15 And this has just come into effect, but it is my
16 strong belief that these rules will be widely
17 complied with.
18 This is not a passive approach. CARU
19 goes out and talks to people, but afterwards
20 starts to bring cases and this will be very
21 public. And so I think that will create a major
22 pressure for many people to move forward.
23 But we have never believed, though we
24 thought self-regulation was important, if we came
25 out with CASIE guidelines and CARU proposals in

1 this area, that that would be enough. We felt
2 the only thing that would really make a
3 difference is if we gave parents the power to
4 bring economic competition into the marketplace.
5 And that is why most of the business groups that
6 you see here and who have spoken to you in the
7 last few days have joined in the P3 program
8 because we believe until you had an easily
9 manageable information policy, the parents could
10 set beforehand whether the kid wants it or not,
11 whether they come to ask for consent from the
12 parent or not, that they could state their
13 policies and control their policies, that this
14 would not work. So we are not just merely
15 saying, do good. We are trying to create the
16 tools that will lead to good behavior in the
17 marketplace.
18 As I said at the beginning, we believe
19 there is a tremendous economic incentive to do
20 the right things. If we give parents the right
21 to be able to set their policies and to block
22 people from going to sites that are not stating
23 policies or not stating adequate policies, that
24 this will become a very important effect, as the
25 CARU approach will start getting more groups to

be online without evolving technology.

One other thing I think that has been discussed at various times during this process but some of us are acutely aware because we have gone through the whole CBA experience is it's not as easy as people say to know whether you have a kid online. Two federal courts in this country have said that it's not possible to know exactly who businesses are dealing with and that is why they struck down the CDA Act. We will see what the Supreme Court does. That should happen within this month and so we will get further conclusions, but it's certainly not a simple thing.

It's particularly not a simple thing when you start talking about kids up to 16 years old because then there is going to be nothing that is going to cue you or key you to the fact of whether you are dealing with a kid. I told the story last year, I think it's worth repeating here that when my nine-year-old went on the chat line and said he was 18 years old, I mentioned to him that it might help that he learn to spell. At some level, people will be on notice.

But when you start dealing with a

1 16-year-old, though some of them may not know how
2 to spell either, generally that doesn't work any
3 longer. And so also what we found in the CDA
4 area is that most sites are not simple sites.
5 They are mixed sites. My child, for good or ill,
6 is just as interested as any 18-year-old or
7 20-year-old or 25-year-old in all the alternative
8 rock sites. He is very interested in all the
9 movie sites. And so how is the advertiser, if he
10 is given a demand to have clearance, going
11 to know that there is a kid there. And
12 so this is not a simple problem to get around.
13 There may be some limited sites where
14 you could have a pretty high degree of
15 confidence, but I think those are quite a limited number
16 of sites and the question is are you going to be able
17 to set up rules that are so narrowly focused as
18 to deal just with those sites. My personal
19 belief is that the technology is the way to
20 handle those sites as well, but you are certainly
21 in a different situation when you are dealing
22 with a five or six-year-old than you are when you
23 start dealing with older kids.
24 COMMISSIONER VARNEY: Dan, would you
25 give us your thought -- maybe you can't without

1 committing your association. Because of the
2 complexity of this area, would you comment on
3 Shirley's suggestion that the FTC ought to
4 consider convening you all for a development of
5 voluntary guidelines akin to the Green Guides,
6 precisely because it's so complex and difficult
7 and the rules aren't clear? If you can't
8 comment --
9 MR. JAFFE: I cannot comment for the
10 association because we have never discussed this
11 issue directly. What I can say is that we have
12 been certainly thinking about this issue, and our
13 approach is a staged approach up until now and
14 first to have set up voluntary policies and what
15 we call goals. The case of goals for adults and
16 then get the CARU guidelines for kids, and then
17 to try and develop the technology to put money up
18 front because we felt that there was a gap; that
19 it was not enough just to tell companies to do
20 right, but we felt we needed to create major
21 incentives for them to do right by giving
22 easily usable technology to allow the parent
23 to act on. If, in fact, 97 percent of the
24 parents are concerned, I don't
25

1 think you are going to find 50 percent of the
2 parents who are not going to do something if they
3 have something that easy to step in. And
4 certainly I believe that is the case in the
5 younger age group.
6 What we did hear from this Texas group
7 that did a study is that for the younger kids,
8 and I'm glad to hear this, parents are usually
9 sitting there. It's not a situation where they
10 allow kids -- the kids can't type, but you see,
11 that is of some comfort. So I think the most
12 vulnerable, the ones who have the least
13 knowledge, will probably be protected. There may
14 be some five-year-old going all around the
15 Internet. I think that is a very exceptional
16 situation. Let others bring statistics to bear
17 on that.
18 But once you get to a slightly older
19 age, I think knowing whether you are dealing with
20 a kid and being able to set rules that are going
21 to work may not be as easy as has been
22 suggested. And I think there has been a great
23 underestimation of the FTC's role in here. I
24 think we are going to see cases from you where
25 people are treating people unfairly or falsely or

1 deceptively, and that is going to be productive
2 as it has been in all the other areas of
3 advertising. We have always been champions of
4 the FTC and a strong FTC, and so we expect the FTC
5 to play its role.
6 I think all of these things together
7 are going to lead us in the right direction. I
8 think we are heading in the right direction. We
9 have a commitment that you will head in the right
10 direction and that there will be strong
11 enforcement.
12 Elizabeth, as we were having lunch and
13 were talking about as soon as we have had a
14 chance to talk with all these groups, we are
15 going to be going out and bringing cases. We
16 were saying hallelujah because we want to have
17 the marketplace work for consumers. The
18 religious theme continues with my hallelujah.
19 COMMISSIONER STEIGER: Dan, we haven't
20 gone into this in any depth at all, but over the
21 hearings several mentions have been made of the
22 fact that the revolution really just begins.
23 Schools are being wired now for interactive Net
24 educational purposes as are libraries, which
25 probably opens up a whole other question of the

1 interaction between children in particular and
2 the Net.
3 Have you folks given any thought to
4 that? Do you presume this will also be an
5 advertising media, or have you given any thought
6 to it? I know it's a recent, quite recent
7 phenomenon and one that will be upon us more
8 rapidly than any of us realize.
9 MR. JAFFE: I can't answer about
10 whether the school medium will be an advertising
11 medium or not, but the P3 approach where the
12 schools as well as anybody else could set
13 limitations on where people would go and what
14 they would see and what they would do would be
15 available for schools or libraries or churches or
16 anywhere else where there are kids and the Net.
17 COMMISSIONER STEIGER: I guess that's
18 what I was getting at. You think the P3 approach
19 is robust enough to cover emerging uses of this
20 technology?
21 MR. JAFFE: That's our intention. That
22 was our intention, that anybody would be able to
23 use it and use it easily, use it effectively and
24 not be dependent on coming to the kid; that the
25 parents play the parental role that we have

always had.

One of the things we always thought was hopeful about the Internet is that technologies that create the dangers also give us the power to have more control. We have more control when the parent is out of the house, if these systems actually work, than parents would with the television. When I step out of my house for a minute and go shopping, if I leave my kid alone, I'm not going to know where he is going to be on the television. I don't know what he is going to do. That doesn't necessarily have to be the case with the Internet. Maybe once we get the V chip that may not be true for the television either. But technology may be giving us more control, rather than less control in the long run.

I think you raised a point that goes back to the question that Commissioner Varney asked which actually was a good one, which is there is a really serious question in my mind whether any of us are ready to lock things into place, whether we are ready for guidelines let alone law until we have had a little bit more time down the road. I mean you can say this forever, but I think within a year or so we will

1 really have gotten to the point where we'll know
2 what technology can or cannot bring to us; that
3 I'm sure there will be plenty more to come. We
4 will have a much better idea.
5 We heard very interesting things
6 just before lunch about all these technologies
7 that are quite eye opening. I just don't know
8 whether those will all fizzle on the launch pad,
9 or whether they will really give us tremendous
10 power to know who and what we're dealing
11 with.
12 COMMISSIONER VARNEY: It's a little bit
13 of a cart and horse question. I guess what I
14 would like if you can and maybe John also, after
15 today while the record remains open, if you
16 could give some thought if we should undertake
17 voluntary guides in connection with other people
18 because it seems to me that guides have the
19 advantage of, in some ways they have the
20 advantage of not having the force of law but of
21 creating kind of the level playing field during
22 the period while we are still waiting for the
23 technology to become pervasive.
24 On the other hand, if such guides would
25 in your view stymie the innovative process, I

1 would want to know that, too. I guess I would
2 ask you to mull it over and think it through,
3 John and some others at the table.
4 MR. CAMP: Well, clearly, you all may
5 remember the 21 trade associations came and asked
6 for guides in the environmental area and I think
7 all of us clearly think that they work very
8 well. But I know that you and clearly we are not
9 naive about the fact that guides in effect have
10 the force of law and they do have some of the
11 same problems inherent in them about freezing the
12 technology because you have to change them. But
13 I'm not at all ready to say that guides are not
14 appropriate here. They may very well be in some
15 cases. As we get further down the road, there
16 might be a lot of uses for guides for everybody's
17 concern.
18 MR. JAFFE: We will certainly get back
19 to you.
20 MS. SCHWARTZ: I'll turn next to Jerry
21 Cerasale from The Direct Marketing Association.
22 MR. CERASALE: I'll try to keep this
23 short because Dan went on and pretty much said
24 quite a few of the things that the DMA agrees
25 with.

1 I think one of the things that I
2 want to emphasize is that we heard about some
3 surveys and lots of surveys, but we heard some
4 surveys that say yes, parents do know what their
5 kids are doing on the Net, which to me was a
6 little bit -- the size of that was a little bit
7 surprising. A lot more parental knowledge than I
8 thought.
9 And I think some of the statements here
10 today have basically given parents a bad name. A
11 lot of us are digitally challenged. I can't even
12 say the words, but whatever, a lot of us are
13 challenged with that but we need the tools. I
14 think the key is that parents want to be parents,
15 and we want to give them the ability to be the
16 parent and give them those tools. And I think
17 that the DMA has put a lot of effort and time in
18 education, which is important, but also a lot of
19 effort and resources into the P3 program too
20 which we think is a good solution. Parents put
21 in the solution and it's there whether the parent
22 is at home or not at home at the time, or whether
23 the parent is sitting next to the child or not.
24 One of the things to remember about the
25 Net is it requires a computer, a telephone line,

a modem and some means to get into the Net, and an eight-year-old child doesn't have the ability to do that. I think the school situation that Commissioner Steiger raises is a potential problem, but we think that the P3 platform would work there in the library.

Protecting children is all our jobs. As a parent, as marketers, as Dan has said we need to have confidence in the Net in order to have anyone purchase anything over the Net. And so it's important for us to get that confidence. And I think it's our job, it's the government's job and so forth.

One of the big things for the government is what you have done here. You have brought us all together. We are moving forward. We are much further along than we were last year.

Where do we go from here? We keep moving forward. And technology which brings the horrors, also can bring the safety from those same horrors, and I think that you want to allow this medium to mature a little bit.

If you do put in laws, or if you do put in guidelines which really do bring the force of

1 law, you will tend to stifle some of the
2 innovation here. I think that you have seen not
3 just today, but early on in the individual
4 reference services and what they're trying to do
5 and what they're doing vis-a-vis children and all
6 of us as we go along. It's a changing process.
7 And the interesting thing for us is that the DMA
8 has taken the opportunity to start calling and
9 contacting Web sites that we don't think are
10 meeting our guidelines, and the initial reaction
11 is, oh, let's fix it. I mean, you have seen what
12 time has done. You have heard what Microsoft
13 did. We just contacted Microsoft this week as a
14 matter of fact, and immediately they call and
15 say gee, we are making some changes.
16 And I think from the self-regulation
17 standpoint, our members and marketers do not want
18 to violate our guidelines. They don't want CARU
19 to come after them. They don't want the DMA to
20 have a complaint against them and our new policy
21 of eventually publicizing the names of people who
22 do not follow our guidelines -- they don't
23 want that.
24 And you have to give, I think, us a
25 little more time to get our self-regulation

1 really rolling, and I think you need time for the
2 Internet to become much more mature as a
3 marketplace. It is not at the moment a mature
4 marketplace, and we have to have time to watch it
5 and see what is happening.
6 And we don't say the FTC does not have
7 jurisdiction to go after the bad guys. Our view
8 is you do, but it's not just you do and do
9 something about it. It's go get them. Go get
10 them. Put them out of business because it hurts
11 all of us. It hurts our kids, it hurts parents,
12 and it hurts marketers. So if you have people
13 who are fraudulent and deceptive on there, get
14 them off. Close them up and get rid of them.
15 But the self-regulation can move much
16 more rapidly than government laws and so forth,
17 and we can move internationally, and as we go
18 forward and try to get compliance and not have to
19 worry so much about the conflict of laws, whose
20 law applies here. So I think it's still an
21 infant enough medium that we need a little more
22 time to go forward and keep the fire, keep the
23 pressure on us to keep our word.
24 COMMISSIONER STEIGER: Jerry, you've
25 just said a word that we haven't heard a great

1 deal about and that is internationally.
2 Certainly you folks, the advertising community,
3 the legal community here are extremely active in
4 and current with the European Union. And I am
5 interested to know whether you think their
6 Privacy Directive will have an American impact.
7 I don't mean in the sense of what you may be
8 doing in marketing or advertising abroad. But
9 will it impact the U.S. market? I realize this,
10 too, is in its infancy and not yet in force, but
11 I think it might be useful to hear if anyone has
12 any wisdom about the impact of the EU privacy
13 standards.
14 MR. CERASALE: Well, I guess that is a
15 question first directed at me. We are in the
16 process -- I think the government is going
17 forward to try and say that the American standard
18 in the notice and opt-out standard from our
19 understanding would meet the EU guidelines, and I
20 think that that is clearly our position at the
21 DMA in pushing forward for that.
22 One of the things that for us, I think
23 I said in the first day as we opened the
24 hearings, these set of workshops or hearings, is
25 that the policy and principle that overlays

traditional media, the telephone, the mail and so forth and commerce that we use, should also apply over the Internet in cyberspace, in whatever form that commerce takes in cyberspace, whether it's E-mail or through the Web. And I think that that is the push that we have that the DMA is going forward with to bring those policies to bear in this new medium. And I think that that protection, especially with P3 and so forth in this new medium, will work and will most likely meet the European directive.

The Internet is becoming a very interesting place. In sales we know of many stories of some small company putting up information on a Web site and suddenly their volume of sales grows fourfold and not any of those sales are in the United States. They are coming from Malaysia. There is a story that Senator Leahy likes to talk about the Bow Tie Pasta Company in Waterbury, Vermont, which is just being inundated with Malaysian requests for their pasta and is sending that out.

So I think that we have to set up guidelines to protect privacy that keeps the Internet open. The guidelines go across

1 international boundaries, and we have to, through
2 our self-regulation, and the DMA's got a group of
3 other nations' DMAs together to try to get those
4 guidelines set internationally so that we can
5 have a common base, and it can be done very
6 quickly without worrying about different forms of
7 governmental intervention in numerous countries.
8 COMMISSIONER STEIGER: John, do you
9 have anything to add? I know you've been
10 interested.
11 MR. KAMP: Jerry's very optimistic
12 about those guidelines. I must say to you very
13 directly that I think that the European
14 guidelines that I have seen are very scary
15 because I think they are not appropriate for the
16 United States. I don't think that they would
17 work very well even in Europe.
18 We are working with others in the
19 government. We think the Magaziner-type process
20 that is working for the GII generally might be a
21 process that we will have to create and do that.
22 Unfortunately we are sort of one step at a time.
23 We are in New York working with CARU trying to
24 get the CARU guidelines out in time, and we are
25 clearly not ready. I hope Jerry is right that in

effect whatever happens in the U.S. becomes the standard because I'm very nervous about those EU guidelines.

COMMISSIONER STEIGER: Thank you.

MS. SCHWARTZ: Anyone, as we go around the table who wants to also address that issue, of course please do so, but Julie DeFalco, National Consumer Coalition.

MS. DeFALCO: Thanks very much. I'm happy to be here. I think I would like to start out with a question. Are these companies that are violating privacy on the Net sinister or just clueless? I think the answer affects what your policy prescriptions are.

I personally think that a lot of these companies that are doing this stuff, as it's been pointed out by a lot of industry groups, just really didn't understand that there was initially a problem, and they acted to fix it.

I think that something that the survey data show that we heard yesterday, some people are responsive to emotional representations of this issue, which we have seen in the Wall Street Journal on Monday and the New York Times on Wednesday. And it doesn't help when this issue

is examined in sort of a hysterical manner as in people's privacy is being violated. I mean if the worst thing that's happening to children on the Internet is that people are trying to sell them products, then I think it says a lot about our society.

I think the real question is what can the FTC do that industry and other organizations cannot do better? A lot of talks have been about educating consumers and only just now have I been hearing who is educating consumers. It's mostly been in the passive voice.

I think the DMA booklet is great, and I'm sure Consumers Union and Consumer Federation of America and other groups will come up with similar items like that, if they haven't already.

I think the worst thing that could happen is the government educating consumers, imagining a pamphlet, "Your Government Explains Encryption," "Your Government Explains Anonymity," is kind of scary. I think it gives people a false sense of security to put the emphasis on a restricting only what marketers do.

And actually I think that marketers and

1 advertisers on the Internet should act
2 appropriately and follow their guidelines, and
3 they shouldn't do anything that violates any of
4 man's or God's laws, I suppose. But the idea
5 that children will feel slighted or be
6 unprotected because they are restricted from
7 going on a page, parents are supposed to set
8 limits for their children. They are supposed to
9 let children know that there are certain things
10 that they cannot do and when they get older, they
11 can do. If you don't trust parents to do this, I
12 don't know what makes you think that an anonymous
13 businessman or a government bureaucrat would.
14 I think the best thing for the FTC to
15 do on this issue is instead of standing up and
16 doing something, sitting down and not doing
17 anything right now, just sort of hanging out as I
18 said the other day. I think the FTC should
19 pursue outright fraud such as violations of what
20 companies say they are going to do online. I
21 think that is an implicit contract, and I think
22 there is plenty of room there to use laws that
23 are already on the books.
24 I think another thing that would be
25 good, which no one really talked about, would be

for the government to also come up with similar guidelines to the industry, for how the government is going to handle data online and what opt-in/opt-out options citizens have. Maybe we give out information to the government that might have potential to do harm. I heard yesterday that the FBI has been going undercover in chat rooms to catch child pornographers, which I think we can all agree is a good thing, but I kind of wonder what other kinds of things the FBI might go undercover on, on the Internet.

So that's all I wanted to say. Thank you very much.

MS. SCHWARTZ: I'm going to ask Shelley Pasnik from the Center For Media Education, I want to come back to you. I want to give everyone a chance to speak who has not yet spoken.

MS. PASNIK: It's been a long week and everyone's worked really hard, so I want to invite everyone over to my office in about three to four weeks when my Jelly Bellies arrive and all my other loot that I'll be receiving as the result of giving out personally identifiable

information, so come on over.

The title of my remarks are The Two Faces of Advertisers or A Name is A Name is A Name. Now, we heard Dan speak earlier that there is nothing to cue you to indicate what would appeal to a child on the Internet. Among the sites that I examined, Colgate Kids World, Ingenious Kids Station, KidsCom, Kids Star, MacDonald's Kids, Microsoft Kids, Nabisco Kids, Pathfinder For Kids. How much of a cue do you need? These sites are clearly designed to appear to youth, to young kids.

Secondarily, I attend a lot of marketing to kids conferences. They go by Digital Kids or Kid Power. I read, among other publications, Kid Screen and Selling to Kids. This is a huge market. In fact, it's a $200 billion market in terms of the amount of money that children are spending or the amount of money that they're influencing their parents to spend, so let's keep that in mind as well.

At these marketing conferences, though, you should keep in mind the types of language or the kind of language that advertisers use. It's one thing to come to a formal proceeding, such as

1 this one, and put on the face for the Commission,
2 but it's another in the way that their practices
3 are discussed at these marketing conferences.
4 They talk about "cybertots" or the "clickerati."
5 That is the new generation that is growing up
6 right now. They talk about wanting to create
7 impulse tantrums similar to what you see children
8 having when they are in line at a supermarket.
9 That sort of notion of having a tantrum because
10 they want something so badly. That's their
11 goal. And also, they want to capture kids'
12 attention, their mind sharing, their loyalty.
13 And I invite you to read many of the transcripts
14 from some of these marketing to kids
15 conferences. I think it will give you a far
16 different perspective than perhaps the one that
17 you are getting today.
18 In terms of the blocking technology
19 that we have seen demonstrated or that we have
20 heard discussed over the course of the last
21 few days as well as the last year, I think
22 these companies should be commended.
23 Everyone should be trying to address the
24 important issue of privacy.
25 We heard some question about

1 blocking softwares' effectiveness, but they have
2 the potential to be very effective when it comes
3 to fair practices and practices that aren't
4 deceptive.
5 But what we are talking about today are
6 those practices that can be defined as unfair or
7 deceptive. For example, collecting personally
8 identifiable information from children without
9 verifiable consent is an unfair practice. We
10 also heard Jerry talk about let the medium
11 mature. How long, though, will it take before
12 parenting or parental involvement becomes
13 obsolete? Right now to involve parents before
14 personally identifiable information is collected
15 is a good practice, and one that all companies
16 should subscribe to.
17 Secondarily, collecting information for
18 two purposes but only disclosing one is a
19 deceptive practice or not disclosing at all is a
20 deceptive practice, and I would encourage the
21 Federal Trade Commission to use the jurisdiction
22 that they have in these two areas.
23 Also, we have heard the demonstration,
24 we saw a little bit of the demonstration from P3,
25 and they, too, should be applauded. Again,

1 everyone should be looking at ways to protect
2 children's privacy. However, I've heard many
3 others say the proof is in the pudding or the
4 devil is in the details or we're going to have to
5 drill down. And that's just it. There have not
6 been enough details forthcoming about exactly how
7 this will be implemented. Instead, I've heard
8 those participating in the coalition talk about
9 the need to protect the status quo, the status
10 quo being an opt-out system, and certainly this
11 is not going to be an effective way to protect
12 children's privacy.
13 Also, privacy is narrowly defined, that
14 we must consider the context in which personally
15 identifiable information is collected from
16 children. Is it simply the form that you see on
17 one screen or is it the solicitations, the
18 enticements, the encouragements that exist on the
19 preceding screens? For these reasons, I again
20 would encourage the Commission to please act in
21 this area. Children's privacy is too important
22 to allow it to be threatened again and again as
23 we have seen and as the research will continue to
24 show.
25 COMMISSIONER VARNEY: Shelley, I think

1 you brought up a very important point that we
2 have not discussed here at all. You know,
3 Jupiter Kids sent me a flyer. The flyer was,
4 come to our Digital Kids Conference. Find out
5 where the kids are, who they are, how you can get
6 information from them to increase your marketing
7 potential.
8 I think there is a real dichotomy
9 between what one would guess goes on at those
10 conferences and what's happened here. And I
11 would very much appreciate anybody submitting for
12 the record, if they have attended the conference,
13 what their views were, if there are transcripts
14 of these kinds of conferences, because you have
15 this whole industry evolving that is teaching
16 people how to find kids online and how to get
17 information from them and how to market back to
18 them, which is somewhat inconsistent with all the
19 good intentions we have heard expressed here. So
20 any information that the Commission can get on
21 that for the record I think would be very
22 helpful.
23 By the way, when I tried to register
24 for the conference, they told me they were full.
25 (Laughter.)

MS. SCHWARTZ: Deirdre Mulligan for the Center for Democracy and Technology.

MS. MULLIGAN: I want to make, I guess, four kind of prefatory comments and then I actually want to try to answer Christine's comment that was asked earlier in one of the preceding panels.

I think I want to kind of respond or make a rejoinder to Shirley's comment about old paradigms, new media. I think what I was trying to say, the values remain fairly constant. However, technology, be it our ability to clone humans, which we recently have been struggling with, or the ability of children to interact with others in a very unmonitored environment, which is what we are presented with, that is what distinguishes the Internet from the TV or from the telephone even. In some instances the range of interactions challenges us to figure out how we implement those values in a new medium.

And I guess what I'm asking for is that in thinking about how to preserve the values that we not react, but that we reflect and then proceed thoughtfully because I think it's in that way

1 that we are going to be able to minimize the
2 risks, but more importantly because of the role I
3 think the Internet is going to play in our lives
4 in the future, maximize the benefits, and I think
5 there are many.
6 I want to make one comment in kind of
7 talking about the CARU and the CFA/CME
8 guidelines. I am very anxious with us treating
9 children between the ages of 12 and 16 as though
10 they are 12. I think that if our psychiatrist
11 friend Michael Brody were here today, he would
12 tell you that between the ages of 12 and 16,
13 which is when sex education begins in schools,
14 which is when children begin to take out library
15 books that they don't want their parents to know
16 about, that kids are very often seeking out
17 information. Sometimes that information requires
18 them to turn over information because they want
19 to get something in the mail and perhaps they
20 don't want their parents consenting. Perhaps
21 they want to get that on their own and that
22 children do have privacy interests in some
23 context that are distinct from their parents.
24 I think particularly when those
25 children are between the ages of 12 and 16, I

1 don't know about you, but having been 12 and 16
2 once myself, there were many things that I might
3 have shared with you that I wouldn't share with
4 my parents. So I would really hesitate to treat
5 those children as though they were all the same.
6 Finally, I think that in responding to
7 your question earlier, Christine, about what do
8 we do now when the technology is not yet
9 available to give us verifiable parental consent
10 or some idea of what parents want to choose for
11 their children, I think that we can't just fixate
12 on the age of the child. I think that some
13 combination of the age of a child, but probably
14 more a reflection of what Shelley talked about is
15 what is the age of the child -- what is the age
16 of the person that the Web site is trying to
17 attract.
18 And I think that there probably is some
19 room for the FTC to say that until we have a way
20 to act responsively, since everyone at the table
21 has said that's what their goal is to do, that
22 perhaps there can be some guidelines in the
23 meantime that say well, until you can get
24 parental consent, that perhaps you should refrain
25 from certain activities at sites that are

1 directly targeting a very young population.
2 And I think that while that encourages
3 the market to respond by saying, we are not saying
4 you can never do this. We are saying that you
5 need to do this responsibly. And we are trying
6 to put some fire behind the development of that
7 technology. And so I would consider something in
8 those lines.
9 MS. SCHWARTZ: I'm going to ask next
10 Leslie Byrne, who is Assistant to the President
11 and head of the U.S. Office of Consumer Affairs
12 and then Bill MacLeod.
13 MS. BYRNE: I was going to say
14 something else until Deirdre started. We don't
15 allow 16 year olds to sign contracts to lease a
16 car. And now that we have invented contractual
17 privacy, to enter into a contract to negotiate
18 your privacy rights away, I doubt very seriously
19 if we can hold any minor to a contract that it,
20 in essence, says that they can negotiate these
21 rights.
22 When we started talking about privacy
23 preferences instead of privacy rights, we have
24 created this quagmire. And that is basically
25 what we are talking about here. We have got

1 marketing companies who are data mining. And in
2 the effort to data mine, they are setting up
3 contractual privacy and they are doing this with
4 children. And a child, as far as I know, in this
5 country cannot be held accountable for a
6 contract. And I would hope that the FTC would
7 address that specific issue. If we are going to
8 engage in contractual privacy, how can we enforce
9 that on a minor? That is my first point.
10 My second point is that John had
11 mentioned that by setting up some framework, we
12 may freeze technology. I think that without a
13 framework, technology is going to shoot off into
14 1,000 different directions. There is no focus to
15 the technology. The technology has 1,000 good
16 ways to do everything but no framework, and that
17 is why I think we definitely need some kind of
18 framework to focus the efforts of all these
19 wonderful technological advances that we have
20 heard about today.
21 And Commissioner Steiger made, I think,
22 two really excellent points; one is about
23 libraries and schools where parents don't have
24 control, where parents can't watch, where parents
25 can't put preferences on them. Every school in

1 this nation is supposed to be wired by the year
2 2000 whatever. I know that in my home county of
3 Fairfax we have an ongoing debate about what
4 libraries are doing in oversight of children on
5 the Internet. And to pretend that this is only a
6 home-based issue, I think, misses a tremendous
7 audience for who is getting this material.
8 Commissioner Steiger also mentioned the
9 EU directive, and I had the OEC delegation on
10 privacy from the United States, and I will tell
11 you that I am not as taciturn as some of the
12 other speakers that our industry is not facing
13 self-imposed trade barriers unless they deal with
14 this issue in a real way. We not only have the
15 EU directive, we have the potential of the
16 International Standards Organization doing
17 privacy directives. We have a whole list of
18 Canadian directives that are being looked at.
19 And none of them, whether the ICO, Canadians or
20 the EU are as market driven as ours. And without
21 our recognition that we have got to come to some
22 kind of harmony, I do think we have a real
23 potential for self-imposed trade barriers in our
24 idea of how to, for example, set up contractual
25 privacy with children. And so those are my

comments.

MS. SCHWARTZ: Bill MacLeod, as I read this, Bill, you are appearing today on behalf of the Grocery Manufacturers.

MR. MacLEOD: That's correct. And perhaps as an example, I might mention a company that is not a member but a company whose product has been mentioned already and that is, I am not aware of any Federal Trade Commission case that would support the proposition that sending a free package of Jelly Bellies through the mail is an unfair or deceptive act or practice.

I think it is important to remember what it is that the Commission can and should do and what it is that can be achieved by private practices and voluntary guidelines. I think to Shirley Sarna's point that perhaps this is an area where the government might be worthwhile moving in, I would suggest that if we take that step now, we are more likely to not only impede technical progress, but also to impede the ethical and the moral progress that we have seen over the last year with the voluntary efforts that have been undertaken.

There is no question, I think, in

anybody's mind that the FTC could pass and enforce guidelines or rules that go as far as have been accomplished in the various guidelines that have been proposed and that companies can now adopt voluntarily on their own.

GMA was also an association that supported wholeheartedly the Federal Trade Commission's efforts in publishing the Green Guide several years ago and then in revising those guides just recently. And let us remember what it was that led to the call for and the issuance of the Green Guides. It was a number of FTC investigations. It was a number of FTC cases which now number in the dozens. There was a very long track record of FTC law enforcements against unfair and deceptive acts or practices in that industry which led to a call for some guidance for the industry as a whole to follow.

That is the kind of pattern that I would suggest would be appropriate to follow here. Before we get to the point at which we are deciding whether it is appropriate for government action as opposed to continued voluntary action, let's ask the question whether the worst that we can see here is getting a free package of Jelly

1 Bellies through the mail.
2 COMMISSIONER VARNEY: Bill, I have got
3 to interrupt you on this, I'm sorry. I would be
4 very interested to know if all of the other
5 industries that have been participating in the
6 last four days would agree with the proposition
7 that it is better for us to go ahead and
8 prosecute prior to establishing guidelines as to
9 what we think is actionable behavior. I cannot
10 accept that that is a universal view of the best
11 way to go.
12 Secondly, I don't believe that
13 characterizing sending Jelly Bellies through the
14 mail is an offense of any kind. I think the
15 question is the amount of information that is
16 being solicited on Web sites that are targeted to
17 small children without their parents' knowledge
18 and consent. Is that a practice that we should
19 be considering investigating? Self-regulatory
20 approach, government approach, what is the
21 answer? I think to characterize that as sending
22 jelly beans to kids, and you know what, maybe
23 there is some harm from sending jelly beans to a
24 diabetic kid. There might be a problem there.
25 MR. KAMP: I don't want to take on the

1 second, but since he was asked if any of the rest
2 of us agreed, the jelly bean one is too
3 complicated for this late in the afternoon. I
4 think my blood sugar is too low or something.
5 But on the first one, I clearly think
6 that if there are cases, and I presume there are,
7 will be, have been, Shelley has pointed out some
8 stuff that troubles me, at least on its face. If
9 there are cases of fraud, for example, that are
10 clearly within the agency's jurisdiction and
11 there is serious harm to families, it's the right
12 and the responsibility of the FTC, and I can't
13 imagine any Commissioner at this agency not
14 bringing the appropriate case, and I can't
15 imagine any of our trade associations, at least
16 my trade association standing up and saying you
17 are doing the wrong thing.
18 COMMISSIONER VARNEY: I'm not sure that
19 we are talking about fraud and deception. I
20 think we might be talking about unfairness and,
21 Commissioner Starek, you mentioned unfairness
22 this morning, I believe, and I would like you to
23 correct me. I believe you said that perhaps
24 collecting information for one purpose and using
25 it for additional purposes may be an unfair

practice.

Now, I don't pretend that that is a majority of Commissioners' views, but I just cannot believe that industry would want us to start bringing cases without some sort of dialogue whether it amounts to voluntary guidelines. I mean, I think, yes, we are going to enforce fraud and deception. There is no question about that. But what about those cases that don't fall in fraud and deception.

MR. MacLEOD: Was that a question?

COMMISSIONER VARNEY: No. It was whatever you call it.

MR. KAMP: Rhetorical question.

MS. SCHWARTZ: We have been almost completely around the table except for Marc Rotenberg. Do you want to step in now or wait?

MR. ROTENBERG: I'll step in.

I just wanted to take a step back and try to put our discussions in some context because not only do I advocate for privacy, I also teach and study privacy. And I don't think there is any question that this is one of the most historic events on the privacy time line. I think we can say probably not since the 1973

1 study undertaken by HEW has there been a more
2 comprehensive effort to understand the challenges
3 that we face with new technology. And for this,
4 I think the FTC is to be commended for the very
5 good work.
6 But at the same time, I have to share
7 with you a concern because we have spent much of
8 the time this week and even today talking about
9 the adequacy of self-regulation and how
10 self-regulation can be made to work, and I have
11 to tell you, this is not the way we have
12 generally done privacy in this country.
13 It is not.
14 It was our country which in the 18th
15 century established the right of a citizen to
16 private home and private correspondence against
17 the government, and it was our country at the end
18 of the 19th century which first suggested that
19 individuals had a right in their good name when
20 it was misused by others.
21 And through the course of the 20th
22 century, we have developed the most comprehensive
23 set of privacy safeguards and rights of any
24 nation in the world. You have privacy rights in
25 your credit records, in your banking records.

1 You have them in your cable subscriber records,
2 your E-mail, your video rental record. And yet,
3 today, when we confront one of the greatest
4 privacy challenges we ever had as a nation, for
5 some reason, we turn away from government. And
6 we say let's see what solution we can reach
7 without the assistance of the government, which
8 is, of course, us.
9 Now, let me try to explain why it is we
10 have rights in law to protect privacy and what
11 that means. You see when you establish a right
12 in law, you give everyone a claim, not just the
13 rich, not just the technologically sophisticated,
14 not just those that can withstand market
15 pressure. Everyone has a claim to get access to
16 their credit report when a loan application is
17 denied, to be assured that the high school
18 records of their children will not be disclosed
19 to strangers. And like many rights, most of us
20 rarely care about these things until we need
21 them.
22 Someone who I respect very much wrote a
23 column this week talking about privacy as a
24 preference, and he said what is neat about these
25 new techniques is they allow people to act on

1 privacy to the extent of their preference. As
2 much as I like this fellow, I disagree. We are
3 not talking about the color of your shirt, the
4 size of your shoes, what kind of car you like to
5 drive. We are talking about basic rights.
6 The majority of people in this country
7 don't vote. They exercise a choice not to vote.
8 But they never give up that right. They never
9 sell it and they never lose it.
10 Now, let me just say briefly what I
11 think the challenges will be for us as we go
12 forward in this area.
13 People need a right, the legal right to
14 get access to their information, not to a policy,
15 not to a statement of the type of information
16 that is collected, but to be able to see that
17 information, and we have done that with virtually
18 every privacy law in this country. I see no
19 reason why we can't do it in this discussion.
20 People should have the right to be
21 anonymous, particularly in commercial
22 transactions. Alan Greenspan will tell you that
23 the majority of consumer transactions in this
24 country are cash based. They are anonymous.
25 When you go to a store to buy a product or a

1 good, you don't need to say who you are. You
2 don't need to disclose your preferences. If you
3 are interested in what they offer and you can pay
4 for it, they will give it to you.
5 I don't see what the rush is to collect
6 all this personal information. I don't see why
7 we need techniques to facilitate the collection
8 and sale of personal data. We need the
9 opposite. We need techniques to limit the
10 collection and sale of personal data.
11 We have a very real problem, and I
12 just -- I wish to convey to you some sense of
13 urgency about this. There is some sense of
14 urgency because people across this country are
15 concerned about loss of privacy and they should
16 be.
17 And I'm sorry if in the course of this
18 week I've been somewhat critical of industry. It
19 is the case of the people participating in this
20 process that are probably doing their best, but I
21 got to tell you something, you are not doing
22 enough. You are just not. It is not enough to
23 say to someone we have got your permission to use
24 your information. Thank you. Now go away. You
25 have to give people rights in that information.

They have to know how the data is being collected, and I think that is going to be the challenge. And I'll tell you something: If you don't meet that challenge, if it doesn't happen, we are going to start to see some real privacy protests in this country. Those things happen and they will happen here.

MS. SCHWARTZ: We have been around the table once now. I want to give an opportunity if you wanted to ask some questions.

COMMISSIONER STAREK: Well, maybe one. Actually, I would kind of like to follow up on the last point that has been made. I stressed, and Christine mentioned, that we have unfairness authority here. Our statute gives us the authority to take action when there is an unfair act or practice in the market. And we have a statutory test to determine what is unfair. And maybe you can explain to me how the collection of information when there is consent given is unfair to anybody.

So, in other words, while protecting people's privacy is truly important, it doesn't have a lot to do with our jurisdiction. Because our jurisdiction deals with deceptive acts and

practices and unfair acts and practices.

MR. ROTENBERG: Well, Commissioner, I appreciate your point, and I think part of what this means, of course, is that the FTC has some role in addressing the privacy issues, but other groups will need to step in as well. It may be a role for Congress and a role for other agencies. I don't think there is any disagreement on this.

But to go a step further, you asked the question what is the concern. As strong as I feel about this issue, I'm not going to sort of wave worst case scenarios in front of you. I don't think the evidence is there, that there have been many of those incidents. There have been some to be sure, but not many.

I guess the question really that all of us have to answer as we think about our future in this information age and the future of our children in this information age is, do we really want to create an environment where before our kids can get access to information they have to say who they are? They have to disclose their address. They have to answer some questions about their family's income.

I mean, I can tell you growing up, I

had wonderful opportunities and libraries and bookstores and I mean it was just a world of information, and I don't remember filling out forms. I don't remember getting on all these lists. I think this world has changed much more dramatically than we realize. And it concerns me. It concerns me that strangers would know more about my family than I know about my family.

MS. SCHWARTZ: Thank you.

Elizabeth, it's been so long since you put your sign up, I don't know if you want to now have your opportunity to speak the second time around.

MS. LASCOUTX: Jerry and Dan and John made a lot of the points for me. I'll do it, although I really just did want to respond to one thing that Charlotte said that the burden of this whole self-regulatory system is on the parent. I think the burden is very much on the advertiser, the one that we are going to hold to our guidelines. But one of our guiding principles is that the primary relationship in a child's life is that between the child and parent and the advertiser should do everything they can to foster that. And all of

1 our guidelines kind of speak to that, and that is
2 why we encourage and are working towards
3 effective notice and choice for parents.
4 But I really just wanted to make sure
5 that I got to refute that it's all on the
6 parents. Parenting is hard. Saying no to your
7 child is hard. I have a child. She is old
8 enough that it doesn't matter if I say no to
9 her. But that is part of parenting. So we all
10 have to deal with our children's anger because we
11 won't let them go on a site that collects
12 information that's private. You have to deal
13 with your kid's anger if you won't let her go to
14 the park at night. I mean, I don't see that
15 there is an undue burden on parents if some sites
16 collect information and some parents won't let
17 their children go there.
18 Since I've got the mike, let me just
19 say that I really want to reinforce what John and
20 Dan said about it being in the best interest of
21 industry to act responsibly. Every single group
22 that's here is showing that that is important.
23 If we don't have consumer confidence, there will
24 be no use of the medium. All of the people, and
25 they are major players who contributed both ideas

1 and funds to the P3, have demonstrated the
2 importance of that commitment.
3 My own parent organization online has
4 just collected lots of money from major players
5 to launch a program called BBB Online which is
6 specifically to help foster consumer confidence
7 in online commerce. Advertisers all know it.
8 Nobody with the slightest bit of forethought is
9 going to contribute to bringing the whole Net
10 crashing down around advertisers' ears.
11 MS. SCHWARTZ: Thank you. We are
12 coming close to the end. Jerry has his sign up,
13 and Deirdre indicated she would like to speak.
14 MR. CERASALE: I just wanted to respond
15 to a rhetorical question from Commissioner
16 Varney.
17 COMMISSIONER VARNEY: Oh, I always get
18 in trouble.
19 MR. CERASALE: Hopefully, I won't get
20 into trouble responding.
21 I think if I have received information
22 from you telling me you're going to do X and then you
23 go and do Y, I have received that information
24 from you falsely. You have deceived me. And I
25 think that and we agree with that and I think

that that says something about these guidelines. Our guidelines say, give notice of what you are going to do. And give you an opportunity to say "no." So if you give me information and I tell you what I'm going to do with it and I do something else, I have deceived you and that brings in a whole realm of FTC powers.

If I give you the option to say no, and you do say no and I don't follow that, again I've given a whole realm of opportunity to the FTC that is right in your current jurisdiction. You need no laws, no further guidelines. So I think that it's really important as we look at what we do and we work together on this that our guidelines do say you got to give notice, and they have to give notice and they have to be truthful in the notice that they give and give you the opportunity to say no. So I think that is important.

And I would say to your rhetorical question, yes, you do have the authority from that to move forward under your current jurisdiction and you should do so. If people are deceiving, we want to stop them.

COMMISSIONER VARNEY: I guess, Jerry,

1 my question goes a little bit beyond that. I
2 think in the not too distant future we will be
3 faced with a question whether in the case of
4 specific transaction presenting itself as an
5 enforcement action or the case of a policy issue,
6 I think the Commission will have to squarely
7 address whether or not the intentional collection
8 of detailed personal information from small
9 children is an unfair practice.
10 I think that is going to be something
11 we have to face. I don't think any of the
12 guidelines have yet resolved that. Maybe they
13 will. Maybe we need to keep talking. Maybe in a
14 week, two, three weeks we will be able to get a
15 clear sense of that.
16 As far as we have gone, I agree
17 completely. We agree on this stuff that it's not
18 easy, but we agree on the easier stuff. It's the
19 hard stuff. It's the policy. It's the social
20 questions. It's the questions Mark has raised.
21 MR. CERSALE: I think we are at the
22 situation where we are in the process if I
23 collect something from an eight-year-old child
24 with the intent to distribute it or I do
25 distribute it, I think that even the DMA

goes and says yes, we have got to have some consent. But I think you have to look at collection and use together. You have to look at those two things together as we go forward and through this difficult time, and I mean there are a lot of things that everyone raised here. What kind of consent as we try and look at tools in the new medium to try and see if we can get parental consent? That is really where a lot of us are moving, I think, in response to that question as we look at collection and use together, and I think we are probably closer than it may seem through our discussions today this afternoon.

COMMISSIONER STAREK: Well, I just wanted to add that some at the table here are very familiar with our statute regarding unfairness and, of course, you know we have established that there be some sort of injury involved here that was reasonably unavoidable. And I'm not so sure that that's the kind of use that's put to some of this information that's collected constitutes injury. It may in certain cases, but not in other cases.

MR. CERASALE: True point.

1 MS. SCHWARTZ: Deirdre, I think you may
2 have the final word as a panelist. My boss has
3 the final word, though.
4 MS. MULLIGAN: I didn't think I was
5 going to hold up under that heavy wave.
6 I wanted to agree with Mark on almost
7 all of his comments except maybe one little
8 example that when you say that you never had to
9 sign a form or fill out anything to get
10 information, and I think that your Web site and
11 my Web site today prove very differently that
12 people can come to my Web site and seek out lots
13 of information, and they can also put their name
14 on a distribution list to get our alerts. And
15 there are many kids between the ages of 12 and 16
16 who choose to do that, and there are many, many
17 other ways in which kids are participating in pen
18 pal programs, they are seeking out that
19 information. There are Web sites that actually
20 operate areas where they try and limit it to
21 kids under a certain age or to girls because they
22 are trying to create safe environments. And I
23 think that there are serious privacy questions
24 there but that this medium has enabled people to
25 engage, as we have said so often in the First

1 Amendment area, we can all be publishers of
2 information. We can all be advertisers, I
3 suppose in some sense, and we can all be
4 recipients of information. And that some of the
5 ways in which people are seeking out information,
6 they are giving out things like an E-mail
7 address, which I think all of us would argue are
8 personally identifiable information.
9 And so that all I'm asking is that when
10 we look at this, you know, perhaps it's
11 information of someone who is identified as a
12 child so, for example, it's at a child's Web
13 site. They have collected information, or it's at
14 a Web site where they're collecting information
15 about how old people are because I think that we
16 want to be sure that we put rules that mesh with
17 the medium. And that would be it.
18 MS. SCHWARTZ: Well, I thank everyone
19 around the table. We have 13 panelists, and I
20 must say I thought this was going to be a
21 daunting task to try to conduct a conversation,
22 and the caliber of the conversation and the
23 amount of thoughtful contributions that we've had
24 to our record has been marvelous, so I thank you
25 all.

1 And with that I turn to the Director of
2 the Bureau of Consumer Protection, Jodie
3 Bernstein, for some closing remarks.
4 MS. BERNSTEIN: Thank you very much,
5 Teresa, and thank all of you.
6 I must say and it has been my assigned
7 task here to try to wrap up a truly extraordinary
8 week. No small task, I might add, because it has
9 been one of the most extraordinary events that
10 I've ever had the pleasure of participating in,
11 and as I thought about it and was particularly
12 struck that the number of people who managed to
13 still be here at the end of this intense week, I
14 don't know about all of you, but I sort of felt
15 like, and this is consistent I guess with our
16 parent child theme, I think we have all bonded
17 here. And I was thinking to myself how am I
18 going to thank these people truly for bonding
19 with us as they have, and so I'm going to tell
20 you about what I've got in mind for your reward.
21 It will come in the mail, and it's a T-shirt that
22 is going to say on the front of it, I was a
23 Doobie at the FTC Privacy Camp.
24 Now, you only get to keep your T-shirt,
25 if you fill out a form. And you have to check

one of these boxes. The first one will say I loved it and think it was the best thing I ever did in my life. The second will say I'm exhausted and I never want to hear from any of you again. And the third one will say I loved it and I want to receive at a minimal cost the newly published camp song as soon as you have it ready. So I expect all of you to respond. And in the event you are going to reject your T-shirt, which you may very well do, please let me at least in a more serious note express our thanks to all of you who participated in this extraordinary way all week. You have truly created an enormously rich record for all of us to consider.

I also want to thank particularly the Commissioners who took part in these sessions all week. Their active role I think here certainly underscores their commitment to addressing and responding to these privacy concerns.

One more thank you, if I may, and that I do with some pride because I would say that our staff and particularly the folks who made the events run and did so effectively were about as extraordinary a group as I've seen in a long

time. My fear is that Time Warner or somebody else is going to steal them away because I've never seen such a terrific performance. Let me just say one small applause for you. Thank you very much.

(Applause.)

Now, let's just reprise the week if we can briefly. We began on Tuesday, as you all know, hearing about the astonishing variety of personal information being collected and stored in databases and in some cases made instantly available to anyone with access to the Internet. At the same time, however, we saw that industry appreciates and is addressing the serious privacy concerns raised by these databases. Many are now considering ways to restrict access to sensitive information and to provide consumers with access to their own information and the ability to correct it.

Further, key industry members came together -- you will find this a consistent theme, I think, through the week -- and offered a comprehensive self-regulatory proposal, a very positive initial step. We look forward to continuing the dialogue with them to respond to

1 some of the concerns that were raised as they
2 articulated their proposal. We are optimistic;
3 we, the staff, are optimistic that these concerns
4 will be met by the time the Commission reports to
5 Congress, as Congress has requested.
6 The next two sessions concerned online
7 privacy. These are issues that the Commission
8 and several of the people have noted that we have
9 been concerned with, the Commission has been
10 concerned with for some time. And of the many
11 things that we learned this week, the most eye
12 opening, I think for some of us anyway, came in
13 sessions two and three when we saw just how
14 strongly consumers care about the security and
15 confidentiality of their personal information
16 online. This concern has led consumers to look
17 for greater protections, preferably,
18 from voluntary effort by industry, but if
19 necessary from government.
20 Now, industry may not yet have been
21 aware of consumers' strong preference for an
22 industry response but coincidentally one of the
23 leading industry members and a number of key
24 trade associations put forward new, innovative
25 and promising self-regulatory policies and

1 procedures.
2 In addition, three significant
3 technological proposals were unveiled. Together,
4 they were an impressive beginning in addressing
5 consumer privacy concerns, and the technology
6 particularly will play a critical role in a
7 resulting comprehensive self-regulatory
8 solution.
9 In addition, all participants committed
10 to, and I think this is very important to us and
11 all of you, consumer education projects to
12 continue to alert consumers to the uses of these
13 tools. Perhaps nothing came through as clearly
14 as the recognition for and the need for consumer
15 education now and in the future. We look forward
16 to partnering with industry groups and consumer
17 groups in that aspect in resolving consumers'
18 concerns.
19 In the area of unsolicited commercial
20 E-mail we saw the benefits, and this is one of
21 the benefits of this kind of workshop session, I
22 think, of bringing all sides of a problem to the
23 table to engage in a very civil discussion of a
24 difficult problem. We are very much encouraged
25 that this disparate group has committed itself to

1 work on developing a voluntary solution and will
2 report back to the Commission in six months.
3 Finally, together, this is the final
4 part of this session, we addressed children's
5 privacy in the online environment. One of Dr.
6 Westin's most striking findings concerned that
7 topic. As you will recall, Dr. Westin informed
8 us that consumers are almost unanimously, 97
9 percent, in their belief that Web sites should
10 not collect personal information from children
11 and sell or rent that information to others. In
12 other words, consumers wanted, Dr. Westin's
13 phrase, law and order on the Internet.
14 On the other hand, or perhaps
15 consistent with that, we heard from the Center
16 for Media Education and others that a great many
17 children's Web sites are compiling detailed
18 personal information about the children who visit
19 them and giving parents no meaningful notice
20 about these practices and no opportunity to
21 control them. We also heard from the FBI and
22 Department of Justice about the frightening
23 consequences when children's names, addresses or
24 E-mail addresses fall into the wrong hands.
25 We are encouraged by the many efforts

1 we have seen in the past year to address consumer
2 privacy concerns as they relate to children. We
3 have heard from some responsible industry members
4 about improvements in their own privacy policy.
5 We have also learned about exciting efforts to
6 design tools that will enable consumers to use
7 the technology to exercise control over how their
8 personal information and their children's
9 information is used online.
10 But we also heard that technology alone
11 cannot solve problems without a strong
12 self-regulatory commitment by industry to abide
13 by privacy policies and to honor consumers'
14 private preferences. Given the findings of the
15 Harris-Westin study and the other studies we
16 heard about this week and what we believe was an
17 emerging consensus that effective self-regulation
18 is the preferred solution, we think there was a
19 consensus that more protections are required to
20 meet parents' expectation for the protection of
21 their children.
22 Our task now, I think, is to put
23 together all these pieces, to try to put them
24 together and fit them together and try to answer
25 the following questions: Will these efforts be

enough? Will they happen quickly enough?

Industry has committed to get back to us on a number of initiatives and we look forward to that response. All of the participants here emphasize the need for education, and we will work with them on that.

The record, as noted earlier, remains open for additional comments which we would welcome. Finally, and as all the commissioners have indicated throughout this week and otherwise, we, staff, will review all of the information you have provided and additional comments as they come in and report to the Commission as to what other actions are appropriate. Again, our most sincere thanks for a marvelously beneficial week for us at the Commission. My thanks to one and all, and now you may all go home and await your T-shirt which is coming in the mail. Thank you.

(Whereupon, at 4:34 p.m., the taking of the instant hearing ceased.)

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P954807

CASE TITLE: Privacy Workshop

HEARING DATE: June 13, 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:

_____

PAULA GRIDER

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

_____

SARA J. VANCE