FEDERAL TRADE COMMISSION

I N D E X

DOCUMENTS APPENDED	DESCRIPTION
Number 6	Verifiable Parental Consent...A Snapshot of The Child Internet Industry's Experience Parry Aftab
Number 7	Center for Media Education (CME) Surveys of Children's Web Sites
Number 8	Disney.com registration page
Number 9	CyberSmart! Statement
Number 10	TRUSTe web page regarding privacy
Number 11	Privacy Times, Volume 19, Number 14, 7/20/99
Number 12	KidsCom Fact Sheet
Number 13	CARU folder of information

FEDERAL TRADE COMMISSION

CHILDREN'S ONLINE PRIVACY PROTECTION RULE

PUBLIC WORKSHOP

JULY 20, 1999

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

ATTENDEES:

FEDERAL TRADE COMMISSION:

Jodie Bernstein, Director, Bureau of Consumer Protection

Lee Peeler, Associate Director, Division of Advertising Practices

Toby Levin, Team Leader, Internet Advertising Group, Division of Advertising Practices

David Medine, Associate Director, Division of Financial Practices

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

ATTENDEES (cont.):

Jill Samuels, Attorney, Division of Advertising Practices

Jessica Rich, Assistant Director, Division of Financial Practices

SESSION I PANELISTS:

Parry Aftab, Cyberspace lawyer

Kris Bagwell, MTV Networks Online

Paula Bruening, TRUSTe

Jorian Clarke, Circle 1 Network/KidsCom

Caroline Curtin, America Online, Inc.

John Kamp, American Association of Advertising Agencies

Kathryn Montgomery, Center for Media Education

Charulata Pagar, Promotion Marketing Association, Inc.

Rebecca Randall, MaMaMedia, Inc.

Jeff Richards, Internet Alliance

Cassidy Sehgal-Kolbet, Council of Better Business Bureaus

ATTENDEES (cont.):

SESSION II PANELISTS:

Eric Aledort, Buena Vista Internet Group, Walt Disney Company
James Brandt, VeriSign, Inc.
Jason Catlett, Junkbusters Corporation
Mary Ellen Fise, Consumer Federation of America
Leslie Harris, American Library Association

SESSION II PANELISTS (cont.):

R. Paul Herman, iCanBuy.com,inc.
Daniel Jaffe, Association of National Advertisers, Inc.
Katharina Kopp, Center for Media Education
Leanna Landsmann, TIME for Kids
Sheila Millar, Mars Incorporated
Ronald Plesser, Direct Marketing Association
Jim Teicher, CyberSmart!
Eric Wenger, New York State Attorney General's Office

ATTENDEES (cont.):

SESSION III PANELISTS:

Oscar Batyrbaev, eOneID.com

Evan Hendricks, Privacy Times

Austin Hill, Zero-Knowledge Systems, Inc.

Jeffrey Johnson, Equifax Secure, Inc.

Steven Lucas, PrivaSeek, Inc.

Deirdre Mulligan, Center for Democracy and Technology

Kevin O'Neil, KPMG LLP

Priscilla Regan, George Mason University

P R O C E E D I N G S

- - - - -

OPENING REMARKS

- - - - -

MR. PEELER: If I could have the panelists take their seats, please.

Can we get the first set of panelists to take their seats, please?

MS. BERNSTEIN: Good morning, everybody.

Nobody answered me back. Good morning.

THE AUDIENCE: Good morning.

MS. BERNSTEIN: There, that's better. We have to get this crowd going this morning.

So many of you have been wonderfully cooperative and helpful to us over these many, many workshops that we have held that I really do want to just thank you for working with us once again, because this is an important opportunity for all of us to try to obtain as much input as we need to have the result be a super one.

That is, a flexible rule that will strike the right balance that we all know we're going to try to obtain to protect children and put parents in a position to be able to make those choices and at the same time not impose barriers that will have a chilling effect. So, that's our goal today, and I know you will all

participate as fully as you have in the past.

We have had a lot of comments on rulemaking generally and particularly on this subject. I did want to mention that, you know, it was so unusual last year that we all worked together, I think, to work with the Congress to pass the Act last year. It was a record record, I think, in terms of the length of time that was used in producing the statute, which we all worked on.

And rather than the Congress saying, Okay, well, we are just going to move along now, last week when the Commission was testifying before the House Committee on Privacy and issued a report, there were a number of questions for members of Congress asking about what progress was being made in implementing this statute. I thought it was an important inquiry and one that we will certainly follow up on, because in response we said that we were learning a good deal in the context of this rulemaking and would be happy to provide that learning to members and other committees as we move along.

So, the issue today is one that, of course, everybody is aware of, and that is what -- how do we effect consent. How do we arrive at ways in which parents can be certain that their consent is the one that goes and really is, as I say, verifiable in the language of the statute.

We have a closely, closely organized group of panels today. There are three of them, and you will all get a reward if you stay awake through the whole thing, and not only that, work with us and provide us with additional comments afterwards. So, Lee Peeler will head the first panel this morning, and we'll get -- we'll get started right away.

Again, thank you all for coming, and let's get going.

- - - - -

SESSION I

- - - - -

MR. PEELER: Thank you, Jodie.

Before we start on the substance today, let me just take care of a few housekeeping issues. The first is to acknowledge that the food and drink outside the room today have been furnished us by the American Association of Advertising Agencies. John Kamp, we appreciate the donation.

There's also a cafeteria upstairs on the seventh floor if people need coffee or food in addition during the course of the day. Outside on a table is a list of area restaurants, and, you know, we have scheduled a hour and 15 minute lunch break for you from 12:30 to 1:45.

There's also a message board outside the lobby of the room, and rest rooms are outside the door. Men's is the first left, women's is the second left.

We have some procedural rules that we'd like people to follow today, make the workshop move along as well as it can. The first is fairly simple. Please identify yourself every time you speak, and the first time you speak, if you could also list your organization.

We're asking the panelists not to reiterate their written comments. We have had your written comments. We have given them close and careful consideration, and the goal today is really to go beyond that and have a dialogue about the issues raised in your comments.

We hope that you will stick to the issue that we're asking you to address, which is mechanisms for verifiable parental consent, and along those lines, of course, don't be offended if I cut you off if you start to stray into other areas.

There are a lot of very interesting additional questions that are raised in this rulemaking that I find fascinating. In fact, I probably won't even notice if you wander off, but Toby will, and she'll kick me. I don't want to be kicked.

Just as a convention, if you want to speak, why don't we just turn the name tags on the side, and I'll try and keep track of those. I may call on people out of sequence, but I will try to keep as close a track of your request as I can.

MS. BERNSTEIN: I think we have had a real technological breakthrough here, Lee, because this is the first time we had the names on both sides. So, we've learned from all of you as we've moved along, and we will continue to do that.

MR. PEELER: Every year we get better and better.

We're going to try to stick on schedule today, and we're off to a very good start. I would also point out that at the end of each session, there will be an open comment period for 15 minutes in which people in the audience can comment on the issues that have been raised by the panel. For that comment period, again, identify yourself by name and affiliation, and also it would be very helpful if you could simply spell your name the first time you speak.

And the final item is to remind you that the record for this workshop will remain open until July 30th, so you have until then to present additional information or to follow up on information that's

presented here.

Our goal for this -- for the overall workshop, of course, is to address the question of what constitutes verifiable parental consent given existing technology under COPPA.

We have three panels today. The first panel, which will begin in a couple minutes, will address what's going on right now and what we can learn from the methods and techniques that are being used right now to get parental consent.

The second question will look at the question of e-mail and electronic-based methods of getting parental consent, and we will look at those in some detail. The third panel will look at the role of intermediaries in providing consumer consent.

We are not looking for one way of providing parental consent. The statute doesn't contemplate that there will just be a single method, and that's not our goal today. Our goal today is to develop the guidance we need to give industry as to what range of approaches will be acceptable.

Again, we will be starting from the statute, and the statute says that verifiable parental consent is any reasonable effort taken in consideration of available technology that is designed to ensure that a parent of a

child receives notice of an operator's personal information collection use and disclosure practices and authorizes the collection, use and disclosure, as applicable, of personal information and the subsequent use of that information before the information is collected from the child.

I would also point out that on the board to the room's right are a list of exceptions to that requirement, and those exceptions were placed in the statute in order to facilitate the interactivity of the Internet. One is very straightforward, and that is to obtain information from the child that's needed to obtain parental consent.

A second exception that is designed to facilitate the interactivity of the Internet is -- allows a site to respond to a specific request of a child on a one-time basis. And a third allows a site to respond to multiple requests of a child, for example, for a subscription or for a contest, as long as the site gives notice to the parent and an opportunity to opt out.

There are a number of other exceptions that are designed to ensure that sites can protect the safety of children and prevent fraud. And in the course of our conversation today, I hope people will keep in mind

these exceptions and address them where applicable.

Now, the goal of this first panel, as I said, is to review the practices that are being used right now, with the objective of first off finding out what sites are doing, how that's worked, and most importantly, what we can learn from existing experience that will help us in our efforts to formulate guidance for the industry.

There are two panel members who have done surveys of existing mechanisms, and I'd like to start with them and ask them to sort of briefly summarize the results of their work.

First, Parry?

MS. AFTAB: Good morning. Thank you, Lee. I'd also, before I begin, I'd like to thank the FTC, not only for doing this but for being perhaps the most accessible and helpful agency out of all of the federal agencies in this government. They have worked shoulder to shoulder with all of the members of the Internet industry in helping us fashion something that works and continuing to help us make something that will work for both parents and the industry. So, I wanted to thank you.

I'd also just to formally like to enter my comments, marked Verifiable Parental Consent, a Snapshot of the Child Industry, Internet Industries Experience,

into the record formally.

I represent a lot of members of the children's industry. I also work quite closely with others, because I'm the author of A Parent's Guide to the Internet and a new book that comes out in October, as well as running CyberAngels and heading up UNESCO's new effort for help for children on the Internet. So, I know what a lot of people are doing, because I'm one of the first people they complain to.

The clients and people I know have used several means of obtaining verifiable parental consent. They use snail mail, regular mail, they use fax, and they use 800 numbers. What we have learned is that it is costly.

There are three types of groups involved on the Internet with children, mom and pop sites that, you know, work from their living room; mid-size companies that, frankly, control a great deal of the children's market, Headbone, Freezone, KidsCom, Bonus, these types of sites; and then there are the corporate giants, Disney, AOL and the others.

The ones in the middle are the ones who are struggling to provide verifiable parental consent, care a great deal about it, who are the subject of scrutiny often by watchdog groups, and they have found that it's

costing them roughly between $50,000 and $60,000 a year in hard costs, that means staff costs. There's a substantial soft cost involved that they have not yet attributed that would be rent and phones and all of these other type of costs, as well as the cost of administration and opportunity costs on different things that they're doing.

So, it's costing a great deal of money, and a lot of them, notwithstanding all the IPOs that we're hearing about, don't have substantial funding. So, it is something they have had to grapple with.

We have learned that parents, to the extent they have 800 numbers available to them, prefer using an 800 number. It's the most immediate way of providing verifiable parental consent, although our experience has ranged from, "Hi, I'm my father," to knowing that the only perfect response is one given by a child. Most of the time when the parents call, they leave something out. Well, we know that if everything's done quickly, in time, within the 125 seconds they're allotted, you know it's a child who's practiced doing this for a substantial length.

There have been issues about language capacity, economic range, people who don't read as well as others and trying to get those consents in, and as we look for

universal access, that's something we should be paying attention to. But it's costing a lot of money, and so a lot of the sites are hoping that there's an electronic means of doing this, that they won't have to have fax and letters, 800 numbers that then have to be inputted by someone with a two-day lag often.

Headbone in particular has added a credit card capability, that there's a $2 or $3 charge, a processing fee, that you can use, and that gives you immediate connection for your child, but a lot of children are frustrated by the administrative delays and getting this information inputted. So, that's something we need to address, is the kids' concerns as well as the parents'.

In a parental advocate capacity, I've learned that the parents are thrilled that somebody cares if they're giving consent about what their children are doing. They are very appreciative, and I think that this experience will move across the table as other people talk about what they're doing. They love it.

Do they care that it's offline or online? No. When I talk to parents and when I call parents, they are as comfortable giving online e-mail consent as they are in the other forms, and in my comments you'll see that there's a suggestion that a nonprofit that we're forming can be a way of substantiating that.

But it's costing them money, it's costing them time, and it's costing them the ability to do other things that they would do, and that's something we need to address, because some of these sites, the ones in the middle ground, are the ones that are providing the best and most proactive, innovative content for children, and I don't want to drive them out of business because we're not being realistic.

So, they want to do the right thing, but their experience is it's costing them a lot of money and in many cases very difficult to do.

MR. PEELER: Thank you, Parry.

The Center for Media Education recently completed a snapshot of how all of this fits into a bigger picture, and I'd like Kathryn to update us on the results of their survey.

MS. MONTGOMERY: Okay, thank you, Lee, and we do have a press release and other material that we have handed out today that's available.

MR. PEELER: And Kathryn is going to identify herself as Kathryn Montgomery, please.

MS. MONTGOMERY: I'm Kathryn Montgomery, and I'm president for the Center for Media Education, and we're very pleased to be here, and I'm going to say that it's heartening to see that we've come a along way since the

1996 report that my organization put out documenting that there were problems with data collection and marketing to children online. I'm pleased with the direction all of the policy has been going in and to work constructively and expect to continue working constructively with industry to create rules that will be effective.

And I think it's going to be very important right now for us to work very carefully and cautiously to create a very good framework to guide the development of this new electronic commerce economy that is moving online. That's going to be very important in children's lives and will have, I think, a very significant influence over children.

I commend the Commission for all its wonderful work, and I also want to say that the people who are here representing industry today are in many ways the good guys. These are the ones that have come forward to share their experiences, to work constructively, to act responsibly, and I very much appreciate that.

However, one of the reasons we realized there needed to be a law is that not everybody is responsible, and the law is intended to create a level playing field and create a safe online environment for children. So, let me just briefly share with you some findings that we

pulled together in preparation for this workshop.

We did two different analyses. One was doing a random survey of children's websites, kids' websites. The other was looking at the most popular websites, and that information, as I said, is available in the handout, so I won't go into the detail. Let me just give you what we found.

It's a little disheartening, because -- do we have the slide? I don't know if you can see that. You may be better off just reading it in the handout.

Of the random sites that we looked at, 95 percent of them -- while 95 percent are collecting personally identifiable information from children, three-quarters of them -- nearly three-quarters of them post no privacy policy at all, and less than 6 percent make any attempt to notify or get permission from the parents. And of those, just about 3 percent do it in a way that is truly verifiable.

You would expect, of course, that the popular and more prominent sites would have a better track record, and they do; however, I'm still concerned about what we found there. While 88 percent of the popular sites collect personal information from children, around a quarter still don't post any privacy policies, and less than 26 percent that are collecting information

make any attempt to get permission, and of those only about 13 percent verifiable methods.

I just want to underscore, there's a lot of work to be done here, and I think it's going to be very important for us to have meaningful, effective policies that will truly enable parents to be involved with the process, allowing their children to go online and provide personal information. So, I look forward to working with everybody today.

MR. PEELER: Thank you, Kathryn.

One of the things -- first thing we want to do as a panel is just try to put together a list of what types of authorizations are currently being used, and we have a number of companies with us today who are pursuing different strategies to get authorization, and I'd like to just briefly get those companies to give us an idea of what they're doing to obtain consent. And then we -- after getting that list put together, let's try to move to a discussion of the costs and benefits of those mechanisms.

Jorian, KidsCom is using print and fax?

MS. CLARKE: Yes.

MR. PEELER: Can you describe what you're doing?

MS. CLARKE: Yes, yes, and again, I'd like to

echo, thank you very much for inviting us. We find these forums very helpful in getting new ideas and exploring new methods.

We currently, unlike what Parry had mentioned, we have used fax and snail mail. We have not gone in the direction of phone right now, but it will be interesting to hear more about it. We have learned -- I know you said you didn't want to go into details with this -- we have learned that it costs about $2.81 per child to do the processing required in collecting fax and snail mail.

We also have found most important for us has been a new area that we have been going in since '97 where we have been trying to get parental involvement by getting parents more involved, and we call it simply a development of using natural inclinations to pull parents in the site.

For example, in research we've done in both focus groups and online surveys, as well as all of you who have children will verify, that there is a watch-me phenomena that comes with a child under the age of 12. They very much want their parent to see what new discovery that they've done, what new skill that they have built.

Also, the important thing with children is the

whine factor. "Mom, mom, mom, can I have this?" So, part of what we've done is utilized our content both in our kids site and we're also the only children's site out that has an active parents site, too, and that's Parentstalk.com, where we involve parents in content that's appropriate for them as well as having their children pull them onto the kids site, where we've provided content that helps them understand what their children are doing.

And that goes from as far as simply saying throughout the site, in areas, to have the kids challenge their parents to a game or print this out and show your mom what you have done or share these facts with your parents or be sure to share these great stories, et cetera. And that we found very effective in helping parents become more aware of what their kids are doing online.

Then when we have the parents' attention, we also take them into areas on our parents site where we teach them technology tips, we call it Tips for the Technologically Challenged, so that they have a better understanding of what it is possible to do online so that they're able to increase their skills in this medium.

We also have provided experts on the site which

give them guidance and counsel on information on parenting and information on parenting in this new generation of Internet. We found this very helpful.

Now, in our go-forward plan, we're also doing additional research with parents to get from them directly what are issues important to them, and while it may be hard for all of us to face, in our experience in the last four and a half years of working with parents and with kids, we have learned that not all parents read or write English, not all parents have a credit card, and, of course, not all parents understand the power of technology and what they can do in helping their children make decisions.

And I think it's important for the Commission to be looking at these nontraditional families in helping to decide how can we make sure that the Internet doesn't begin to fall into a "have and have not" category and we make it difficult for the have-nots to be able to reach this powerful information, whether they are doing it through schools or doing it through public institutions, like libraries.

MR. PEELER: Thank you, Jorian, and just to reiterate, your basic business model is a print and send authorization, the child prints it out and sends it in to you; and also a fax authorization, the child prints

it out and the parents fax it to you.

MS. CLARKE: Correct, correct.

MR. PEELER: Okay.

Rebecca Randall for MaMaMedia.

MS. RANDALL: We are known for turning things on its head. I guess what would be most helpful is to characterize the nature of our content, because it's a little bit different, and I think sometimes that can illuminate how we need to think about the framework that Kathryn was describing in a different way.

So, one of the things I would submit is that we broaden our traditional understanding of the word "data" and "data collection," because if you think about the world in which kids are now growing up, data can be a report card that a teacher collects and sends to a parent; data can be a story the child writes. So, often times, because of the associations we have with those words, we -- we kind of narrow our thinking. So, I'm proposing that we broaden our thinking a little bit.

The nature of MaMaMedia's content -- we're an educational website serving kids 12 and under, parents and teachers -- is really something that we call project-based, which means that it's about kids making, designing and building things over time. So, it's not about a one-time visit, and it's therefore about tools

and activities that help kids learn how to make their own media and through that process to learn how to learn.

In fact, as a child signs onto MaMaMedia, the reason they do that is so they can save the work on the server, come back another time, come back to their project exactly the way it was left. They can also -- and to the direct question of how are we currently getting verifiable parental consent, it's primarily through e-mail or in the case of when kids are submitting artwork to us for possibly posting anonymously in our galleries, then a parent permission is required, because, of course, that's intellectual property, but for kids to save their projects, they need to sign in.

What we automatically do when a child signs in -- and this is one of the surprises, I would say, for me personally, and it echos something we have heard already -- is we get a lot of thank yous from parents who are simply thrilled and voluntary e-mails from parents saying, "Thank you so much. My daughter is 4, and she's so excited. She's smart and loves to play games. In this case, I appreciate your advising parents; however, she's sitting on my lap, and I'm pressing the buttons with her."

Now, we all know that's an ideal situation in which the parent is sitting right with the child in that moment during a learning experience, but one of the things that we thought could be helpful in this workshop -- and we can talk about it later as it's more relevant to solutions -- is to think about a learning unit that's not only a parent and a child together at the same time.

Specifically, one of the things we want to make sure we don't overlook is that dynamic of a teacher in a classroom and the learning unit of a teacher in a classroom or a camp counselor and campers and the idea that we think is so important that simply because the parent isn't there at that moment, that we should make sure that a teacher is empowered to help empower a parent or a child. So, that's the area that we think is important not to overlook, and I guess it would fall under the area of exploring an exception, that we should make sure we've carefully thought through.

MR. PEELER: So, Rebecca, your basic model for getting parental consent right now is an e-mail.

MS. RANDALL: Correct.

MR. PEELER: So, you e-mail back to the parent and ask the parent to consent?

MS. RANDALL: The first thing that we do is we

e-mail them back automatically when a child signs in -- and, of course, they ask for a parent e-mail, that's required -- so we e-mail that parent address and say, "Guess what?" We notify them that their child has registered to MaMaMedia, and we tell them a little bit about ourselves, our privacy policy. We basically bring them into the loop, which, of course, dovetails with our mission anyway to involve parents and help them drive the activity with their kids.

MR. PEELER: Now, for artwork you follow a different approach or you use e-mail to get permission for artwork?

MS. RANDALL: We actually have them send snail mail, also, permission.

MS. MONTGOMERY: Lee, am I allowed to ask a question? May I?

MR. PEELER: Yes.

MS. MONTGOMERY: When you use e-mail to notify the parent, is it an opt-out system essentially?

MS. RANDALL: Yes.

MS. MONTGOMERY: Actually I know it is, because I just registered.

So, you don't wait to hear back from the parent --

MS. RANDALL: Did you get your parent e-mail?

MS. MONTGOMERY: I did get it, but you don't wait for the parent to reply, and that is the authorization, you simply notify the parent?

MS. RANDALL: Currently, correct.

MS. MONTGOMERY: Okay.

MR. PEELER: Okay.

Next let's turn to Kris Bagwell of MTV Network online.

MR. BAGWELL: Thank you, Lee, we appreciate being here today. I am Kris Bagwell with MTV Network, which is the parent of Nickelodeon, and as you know, we're owned by Viacom. We, again, appreciate the opportunity. We think the FTC has taken a very forward-looking approach to this and really appreciate the opportunity for input.

As you know, I mean, Nickelodeon is -- we have a number of sites in the kids arena. Our mothership site is nick.com, which appeals to kids 6 to 14, primarily entertainment based but beginning to branch out into a number of other areas, as well.

We also offer a nickjr.com, including a parents area on Nick Jr., and a site called teachers.nick.com, in coordination with our teachers in the classroom efforts, as well.

We also announced in February that we will be

launching a new initiative called Project Nozzle this fall, which will involve kind of a broadening of the scope of the kids offering, including content and entertainment and across a number of other areas, as well, in conjunction with some partners.

Our -- I think our -- I think the main thing that our experience has told us today is, you know, we do a tremendous amount of research. We probably do more kid research than any company in the country, and as part of that we also do parent research. We do a tremendous amount of parent research, as well.

And as we've discussed this issue with parents about the methods of parental consent recently, some very interesting things have come out. Let me just back up and tell you, today on the site what we're doing, to answer your question, Lee, we have essentially backed up a bit as we're building out our new products and today on the sites are not doing online contest entry as we used to do. We are now doing offline contest entry kind of in the interim here while we determine what the best way to do this is going to be going forward.

We're currently not operating any chat, e-mail or messaging on our websites. We do this all in conjunction with America Online, a big partner of ours, as well. But in our research with parents, it was very

interesting and I think at the very beginning somewhat surprising to some of us, but the main thing that's come out with parents is that while they're incredibly concerned about the safety of their kids online, as you would expect, they're also interested -- they're very interested that their kids have an entertaining and fulfilling experience.

If you look at the ratings of where kids go online, the overall ratings of sites for kids online, it's almost identical to where adults go. So, one thing that's going on in general is that kids are going to general interest sites, the Yahoos and Weather Channels and CNNs and everywhere also, and while those, the ones I've mentioned, are fine, the concern I think we all face here are how do we create compelling kid content for kids to come to that's really made for their needs and specialized for them?

And I think the biggest danger we face is if we don't -- if we scare them away from our sites, obviously we will be sending them out to kind of a world where most things are fine but some things are not.

In our research with parents it was interesting, because the fathers and the mothers differed quite markedly. The fathers were much more comfortable with a credit card being a method for their kids to use, but

the -- and the mothers were much more concerned about that, but the concern was that if we were using credit card as one of the methods for obtaining consent, we weren't charging anything for anything, it just -- it made them very uncomfortable, because at that point, I mean, we have a brand that they trust, but even with us, they were concerned, "Why are you asking for my credit card number if you are not going to use it? Does that mean you are going to use it down the road? Does that mean my daughter is going to be able to use it without my consent, you know, two months from now when she wants to buy something on a site that's connected to yours?"

And so there's something kind of unnatural to parents about that. So, I think that while -- while, you know, there's some benefits to that, there's some real concerns with credit cards in general on the parents' part. So, you know, it's our position that we need to have a number of methods of obtaining consent, and I think in particular it appeals to this notion of a sliding scale, as we've discussed in our filing, about it really depends on what you're doing on the site on the level of consent that you really need to have.

If you're doing things that are very non-realtime that can be monitored in advance, in essence like bulletin boards and things like that, you

know, something like an e-mail consent we think is appropriate, because you're able to get a level of parental consent that you're able to have a certain amount of trust is a parent, and then you're also monitoring what's going on there, as well.

When you get into some of the more realtime applications, we think that the hurdle -- we think that that should be a little bit higher and that there should be, you know, kind of a higher bar there for those kinds of things, as well.

I think that one of the other experiences that we have had, as well, is that when we did -- Rebecca mentioned this, as well -- but when we did an opt-out, we started it in the spring of this year -- fall of last year, actually, around our Rug Rats movie contest, when the movie came out in November, several months in advance, we were flooded with hundreds of e-mails from parents saying, We appreciate you just letting me know what my kids are doing online and that they're entering a contest or whatever.

So, I think there's a lot of good will out there around letting parents know, and in particular I think that one of the things that we also heard in our research that really got our intention was that when folks are in this medium, when they're sitting at a --

with their kids at a computer, the sense of immediacy and the sense of if I can like give the consent now and we can continue this experience, if we can kind of engage in this together, we have got -- you know, we have only got so many of these moments with our kids at the PC, that was important to them, to be able to give that consent.

They felt like their e-mail was generally pretty secure, that their kids didn't have passwords to their e-mail, and that they wanted to do that right then. If you lose that moment, what we're concerned about is that you're kind of just halting a process that, you know, normally is a pretty fluid process for them, as well.

MR. PEELER: So, Kris, in terms of what you're doing right now, are you using e-mail?

MR. BAGWELL: We are not today -- on the sites today -- now, you know we've announced a lot of things that we're imminently about to launch, but today we are not collecting and identifying information from kids today for either online contest entry or for online applications, like chat and e-mail, instant messaging.

We have kind of pulled back on that today, and in our new offerings you will see us do a number of things, you know, employing various methods of consent. We haven't -- unfortunately, we haven't announced all of

those things that we will be doing, but today we're in a pretty conservative position.

MR. PEELER: Okay, and you have been using offline notifications for contests and publications?

MR. BAGWELL: Yeah, we have -- you know, kids can submit -- for instance, kids can submit -- we have a section called Comments Come to Life where kids can submit drawings and we animate them for them and put them up on the site, but it's an offline -- the consent we receive is offline, and we had -- you know, we were doing online contests before with online entry. That's when we started the opt-out, late last year, but now we've pulled back and we're just doing offline entry on contests today.

MR. PEELER: Okay.

Another model is represented by AOL, and Caroline Curtin from AOL can tell us about that.

MS. CURTIN: Thanks. Thanks, Lee. I want to reiterate what each of the other panelists have said thus far, which is to really commend the Commission for all of their efforts in the area of children's online privacy and safety and to say how delighted I am to be back at the FTC.

MR. PEELER: We're glad to have you back.

MS. CURTIN: Thank you.

I think that the most helpful thing for me to describe is really how we go about obtaining verifiable parental consent through our subscription-based model, and basically what we do is when a parent signs up with the service or creates a screen name for his or her child, we get up-front consent.

Basically from the time a member signs up with the service, we are enforcing parental controls, strongly encouraging parents to use parental controls, especially for children 12 and under. And in order to set up any kind of a screen name on the service, you really are stepped through the parental controls process. So, it's virtually impossible not to be exposed to parental controls.

When a parent goes to set up a subaccount screen name for a child, they're provided with an important note to parents, and in this note to parents we explain and reiterate that a screen name is an e-mail address, that it's online identifying information, and we explain how it can be used, that it can be used to communicate with others online, that it can be seen in chat and message boards, it can be used for instant messaging, and we explain what each of those features are so that parents can really have a working understanding, especially if they're new to the medium, of what they're

consenting to.

And really the easiest and the most efficient way for us as a subscription-based service to obtain verifiable parental consent is to do so through the information that parents provide when they sign up with the service, specifically providing a credit card, and at the same time we are obtaining consent for our partners who are obligated to follow very stringent kids' policies when they sign up with us.

And one thing that we would like to seek clarification on from the Commission and hopefully confirmation of is that when we do provide notice and obtain consent for our partners up front, that, you know, that if there were a bad actor, heaven forbid, that AOL would not be held liable for that, that the FTC would really go after the bad actor, because we think that we're providing a service for our partners and think it's -- it cuts down on our partners' costs, it's better for consumers, it's a fast, easy -- easily digestible way to provide consent, and we want to be able to continue to do that but at the same time not expose ourselves if there is a bad actor.

MR. PEELER: Thank you, Caroline.

Paula Bruening is here from TRUSTe. Paula, how do these mechanisms that we've discussed so far fit into

the TRUSTe model?

MS. BRUENING: Thank you very much for having us today.

TRUSTe comes at the issue of children's privacy through its general trust privacy seal program in which it attempts to provide trust on the Internet by helping companies craft their privacy policies and statements, making sure companies do what they say that they're doing through monitoring and through a dispute resolution mechanism.

It came to the children's privacy seal program as a sort of separate and distinct seal from the general seal that it provides to industry, and it helps companies comply with the developing policy in children's privacy, and it helps companies that are directed towards children to address the issues that are specific to children.

Verifiable parental consent is an important piece of the online children's privacy seal, and TRUSTe considers four methods of parental consent to be acceptable for seal holders. One of them is to download a permission form and submit it back to the company via fax or e-mail. The second is use of a credit card. The third is use of a 1-800 number where a parent would dial into a 1-800 number, get a password or a code, and then

allow the parent to go online to provide the consent online with that password. And finally, you know, what we're looking toward is e-mail with some kind of digital signature mechanism.

We don't believe that strictly e-mail response from a parent is enough, and we really don't think that's going to be a really spoof-proof way of doing this until there is some kind of digital signature mechanism that can be used along with it.

Now, among these different methods, we do realize that they all have limitations, that none of them are foolproof, and we realize that companies are really in a position where all they can do is use the best method in keeping with the kind of information they're collecting, what their business is and what they think can best serve the needs of their users and the needs of their companies.

Thank you.

MR. PEELER: Thank you, Paula.

Cassidy Sehgal-Kolbet is here representing both CARU and bbb.online.

MS. SEHGAL-KOLBET: That's right.

MR. PEELER: What are the bbb.online standards for verifiable parental consent?

MS. SEHGAL-KOLBET: I actually would feel more

comfortable sticking -- talking about CARU, because I'm actually on staff at CARU. I'm more than happy afterwards to discuss fully the bbb.online since they have adopted CARU's standards, but I think it would be more helpful to talk about CARU since at this time we have about 150 sites that we work with to keep them in compliance with our guidelines, and I think that that experience may be really helpful.

In 1997 -- before I talk about the methods of verifiable parental consent that we have worked with sites to develop, I think it might be helpful to talk about some of the experiences of the bulk of our sites which fall into the third exception that you've discussed there, and I think it's a really important exception, and for example, it encompasses some of the leaders in the kids industry, including MaMaMedia -- the MaMaMedia site and some of the other really hot sites today, like the Children's Television Workshop to Mattel's Barbie to Mattel's Hot Wheels to a number of the other top 100 sites online.

What's happening -- what our experience has been is in dealing with the group of about 150 sites, I would say the majority, close to 75 percent or more of those sites, are -- have adopted the e-mail consent mechanism, which is only applicable where a site is -- where a site

is providing a service such as an e-mail newsletter or a contest.

It's not applicable where we're talking about chat or bulletin boards or highly interactive web community features where a child can post personally identifiable information about himself or be contacted by a third party directly. So, in the case of the bulk of the sites that we've worked with, what's really exciting is that we've seen that the sites have made a commitment to immediately sending parents notice when a child subscribes for a newsletter or a contest.

And instead of -- you know, in the case of contests, what we're seeing is that instead of directly contacting the child to get offline information or to gather information from children, what they're now doing is they're immediately contacting the parent and asking the parent whether it's okay that the child participate and then contacting the parent in the event that the child wins or in the event that they need to get offline contact information.

So, I think that that's a tremendous -- I think that that's a really significant change that we have noticed over the course of the last two years since implementing our guidelines, and I think it's been really exciting, because we've seen sort of a snowball

effect, where people are really instituting privacy policies that are clear and easy for kids to understand. They're posting them in places where -- wherever they're asking kids for either e-mail or online contact information.

With regard to -- with regard to verifiable parental consent, that's a much smaller group of sites that we've worked with, particularly because I don't think there are a lot of actors out there right now who are -- who have created child-directed sites that provide realtime chat, bulletin boards and pen pal features, and the sites -- and some of the sites that we've worked with have already been mentioned here.

I know that Parry talked about some of them, and they include Headbone, Freezone, CyberKids and Kids.com, and in the case of those sites, we have had -- each of the sites has implemented a downloadable parental consent form which can be mailed in. Some of the sites, including, I think, Freezone and Cyberkids offer a fax-in capability, and I believe that -- actually, none of the sites that I'm going to talk about have instituted verifiable -- have instituted verifiable parental consent using credit cards.

Generally the sites -- generally we've discouraged -- both bbb.online and CARU have discouraged

the use of credit card where the site is not a subscription-based service, where there are added risks, and I know that parents have a lot of concern about inputting credit card information where they are not making a transaction, and also there are many parents out there who don't have credit cards.

So, what our sites -- what -- in my conversations with folks from Cyberkids and Freezone, what I was hearing is that initially they had a hard time setting up the downloadable forms and there was a lot of confusion about what needed to be in the downloadable forms but that it's actually become a very streamlined process.

In fact, Cyberkids told me that now, the process of inputting verifiable parental consent has become a weekly task that they do and that it's -- that they have found it really beneficial, because they actually have a human being that screens the registrations. So, unlike, you know, an e-mail consent, it's easier for them to tell if it's a kid that's filled out the form or if it's actually a parent.

And my experience in talking to the folks at Freezone sort of reiterates the fact that they feel that they have had better experience in terms of getting nonfalsified parental consent simply because kids under

12 are -- I mean, they feel that they can spot the forms more easily and that the kids are more likely to go to a parent when -- when they do have the downloadable form.

I guess -- I guess one thing that I did want to raise is that, you know, that these actors have really stayed the course in the face of some pretty high costs, you know, in terms of adding staff, and it is truly commendable, but that we also think -- you know, we at CARU, in working with these sites and some other sites, some bigger sites, feel that it's really important where you're giving children the opportunity to post information about themselves that the costs of verifiable parental consent be considered as a cost of doing business with kids under 12, and that's why we will remain steadfast to the idea that verifiable parental consent cannot be at this time obtained via online mechanisms.

On the other hand, we also want to make sure that we commend the sites that are doing the appropriate direct parental notification via e-mail where children are not given the opportunity to post about themselves and instead are participating in an e-mail, newsletter or contest.

MR. PEELER: Thank you, Cassidy.

Now, we have a list right now of print and send,

fax, e-mail to the parent's address without a confirmation, that would be an opt-out, a subscription-based master account, toll-free numbers to call, a credit card authorization, an e-mail with a digital signature, and an e-mail -- that's a long one.

MS. BERNSTEIN: Go ahead, Toby.

MS. LEVIN: E-mail where consent to online newsletter subscription or a contest, also used to contact parent for offline address.

MR. PEELER: Is that a complete list of what is currently out there?

Jeff, do you have anything that you would add to that list?

MR. RICHARDS: Jeff Richards, Internet Alliance.

I think this list that is being built represents a good cross-section of what's going on. We had little time to survey our members and are still gathering information. Let me just say that this is the stuff of serious research. I guess I would say that not only because the mechanisms are important but what really counts -- what we're talking about here is sustained behavior change, the behavior change that motivates parents to be involved with their children's web experience, that motivates children to have the right

incentives.

We talked about some outcomes that we wouldn't like to see happen, for instance, driving kids from kids sites to general sites because we inadvertently raise barriers too high. So, for us at the Internet Alliance, and we join in the Federal Trade Commission and many others in this, for us our mission has long been building consumer confidence and trust so that -- of course, it's a market-based equation, too -- the Internet becomes the leading mass market global medium of the next century.

So, some of the principles are pretty serious and pretty simple, I think, continues to look at -- continue to look at incentives, and as rules are adopted, to continue to look at their effect in the marketplace and for all of us to seek out continuing behavior change and to test that.

We also, by the way, I think need to -- let me stray for a second and ask that we also contact and are in touch with the law enforcement community, because I'll note tangentially that many of these same issues and mechanisms are stuff of daily discussion at DOJ, at Treasury and elsewhere, and we could be building only to tear down again shortly, and we don't want to do that.

The FTC absolutely should go after bad actors,

and it sends the unambiguous signal, and if it separates those at the table from bad actors, so be it, but as that happens -- I think we'll hear about a lot of innovations today. Those need to be -- have the time -- and I'm not advocating any kind of delay. I'm simply saying that they need to be tested in the marketplace, and this is very important, because we talk about technology sometimes in the abstract, and I'm always thinking of people actually using them.

The standard in the marketplace, you know, in a sense is Apples and Microsofts, you know, Plug & Play Microsoft calls it, and that's the concept, and if the technologies are -- don't exceed even that barrier of -- that standard of usability, then I think we are -- we are actually prescribing solutions that are going to have a rebound effect.

So, we're talking about ready to use, affordable, highly reliable as determinants, because we think parents will, in fact, flock to effective, usable, economic solutions, and what we need are lots of choices and ways to test those out. After all, we're talking about parents and children making behavior change as much as anybody.

So, we need to develop those reliable, efficient solutions. We need to seek prosecution of the dangerous

bad actors in the realm of children's marketing. We want to make sure that the rules and regulations don't pick winners and losers at this particular point in time; that would be inappropriate. And ultimately, we need to focus then on how we're going to measure our success here.

At the Internet Alliance, we're going to, among other things, figure out the right kind of survey, continue the questions that we've already asked, and we think that dialogue with law enforcement is very important, and we will use that channel, as well, in our developing education programs with law enforcement around parental consent issues.

MR. PEELER: Great.

Well, I think that's a good transition to the second part of the discussion we want to have on this panel, which is to look at these different types of mechanisms and talk about what we've learned in their implementation, about how they work, what their costs are and what their benefits are.

So, I think I'd like to go back to Parry and ask her if she could start that discussion. I think you addressed some of that in the paper that you submitted, but again, the idea, having gotten the list of what we're doing, is to focus on what the limitations and

what the benefits are here.

MS. AFTAB: Thank you.

I also just wanted to comment, Lee, on the international situation. You had asked me what's happening internationally. As you know, I've been selected to run UNESCO's Program on Children on the Internet in the United States. Children in the United States are online more than they are anyplace else. About 17 million children today in the United States are using the Internet, and very few of them are using them internationally because of the high cost of using the Internet. We have to pay for local access telephone calls. So, there is no yet parental consent on a European basis for collection of data from children, even though data collection, period, is different.

Now, when we had talked -- and I know Cassidy had mentioned a little bit about some of my clients and some of the things we're doing, and I want to be specific about some of the benefits. I think that Headbone is a very good example for us to track, because Headbone uses four different kinds of offline parental consent. They collect credit cards, get credit card consent. You can do snail mail. You can do fax, and you can do 800 numbers.

Out of every 350 800 telephone calls they

receive from parents giving consent, they receive between 50 and a hundred fax responses and 25 to 50 snail mail responses and 10 credit card responses. So, it's quite clear if parents are given the choice, they would like the 800 number. They have been doing this, using 800 numbers to get verifiable parental consent, for about the last nine or ten months, and their experience has ranged from, "Oh, my God, Parry, why did you get me into this?" to, "Hey, this is working." And I'm not quite sure where it is any week.

And as I mentioned before, some of the times the phone calls that come in are, you know, "Hi, this is my father, and it's okay to do it whatever you want to do with me," and sometimes people just call and sing. So, it has been very trying when you're dealing with children 12 and under, you know that they do whatever they can to push the envelope.

And parents will call and try to give the relevant information, and they forget what they're supposed to do or they will guess at what the child's log-in name should be without realizing that somebody has to find out if somebody else has already used it. So, they get on saying, "Okay, yeah, my kid's log-in name will be purple," and somebody has to contact them and say, "Well, purple's already taken." So, it's been

very time-consuming.

They have learned that by creating a special section on the site that's a parental control center that teaches parents about what they're doing and why they're doing it, that it has cut down substantially on mistakes, and the -- and they were receiving sort of 15 percent error on the toll-free number before, and now they're down to about 5, because they put this in, and the first thing they say is grab a pen and pencil when they start talking to them on the phone, and it's an answering machine basically.

MR. PEELER: Parry, it's a -- the toll-free number is an automated toll-free number. It's not a person on the other end.

MS. AFTAB: No person on the phone. They actually use answering technology, and those numbers -- that information is swept every day or every two days by a real live person who you couldn't pay me enough money to do this job, and she is just really terrific and has a wonderful sense of humor and sometimes actually records the songs that the children send to her, and she's learned a lot, and their learning curve is very important, I think, to the rest of the industry if they are going to implement the 800 numbers, and Headbone is kind enough to agree to work with the other sites that

want to do that.

MR. MEDINE: Could you just briefly explain how the person who does the sweeping or evaluating distinguishes whether it's a parent or a child?

MS. AFTAB: Well, it's hard. I mean, there are four different ways that the phone calls come in. Number one, "Hi, I'm my father," which is an obvious give-away. The other is, "Hi, I'm the father of," and although sometimes you may have a father who actually talks that way or a mother who actually talks that way -- that's another comment -- you can kind of tell. And when the answers are too perfect and too staged and too practiced, that's a key to them that it's a kid, because the parents just aren't that good.

So, when there's some minor errors or there's some stammering and it sounds like an adult voice that hasn't been lowered several octaves, they assume it's a parent, but they have gotten pretty good at it, but it's the experience, and this is all she does.

MR. MEDINE: And what happens if they determine from their expertise that it is a child and not a parent, what steps do you follow?

MS. AFTAB: Well, in Headbone, your registration doesn't become apparent until the parental consent is received, so that the kid wants to sign up, and parents

have to do either offline consent, snail mail, fax or credit card, or this phone thing. So, you're not a member until this happens. So that if there's a failure, you can reach out to the kid and say, "Nice try," or the consent just doesn't come in and the kids come back saying, "What happened?"

And kids -- once you're dealing with 13 and 14-year-olds, you're really in trouble. So, I'm very happy that we're going to cut it off at 12. At least at 12 they are not quite as good at breaking the rules as they are when they're 13 and 14 with the, you know, "I live for the fact that I have to break this rule." So, when they're 12, they are kind of in that realm, but 10 and 11-year-olds kind of sometimes, once in a while, follow the rules.

They found that snail mail letters sometimes are written in childish handwriting, and Jorian I think will be able to add that sometimes that's because the parents write in a childish way or you're dealing with a parent who doesn't write in English or is not terribly well written. And calling to confirm that this looks like a child wrote it can be very insulting to a parent who doesn't have the same education level as some of the people that you're dealing with, so you have to be cautious there.

But they found that the kids are getting pretty -- kids understand that they're not going to be able to get by this terribly long, and I think that that can be very helpful. And one of the things that some of the sites are doing is in collecting the parents' e-mail, as well. Even though you're getting this offline consent, if the kid got through the first time, often -- repeated notices go out, sometimes the parents are actually going to get that notice.

I remember when my son was in high school and they called me in because they said that there was a note that appeared to be forged, and I walked in and I said, "No, I wrote that, but it doesn't match all these others," and I pulled these letters out of a drawer that I had never seen. So, I think -- I think that what we need to do is recognize if we're parents or teachers or if we work with anybody who is that kids are going to get past any verifiable means of adult consent that exists, whether it's a digital signature that somebody's going to share with somebody else, I mean, what we need to do is be reasonable and be sure that the sites can create something that makes sure that the parents get notice without their closing off entry, but they -- these sites --

MR. PEELER: And Parry, you said that these are

relatively expensive for your clients?

MS. AFTAB: They are very expensive. I mean, when you're talking about $50,000 or $60,000 to Headbone or to Bonus or to Freezone -- even though it's owned by Thompson, it's self-funded -- that's a lot of money, and that's money that they could have spent on hiring one and a half producers or editors on new content. That's money they could be spending marketing to -- offline marketing to get more kids involved, putting into all kinds of prizes and other things.

And so it's -- when they do this, it's not -- they are not the AOLs and Disneys of the world. When they have to spend this money, it means they are not spending it someplace else.

MR. PEELER: But presumably it's working for them?

MS. AFTAB: Well, it's working -- they are doing it because they have to do it. Safety is something that's very important to these sites in particular, very, very important, and it's embedded in everything that they do. They would not be doing verifiable offline consent if you didn't say they had to, so that what they would do, they would be comfortable with an e-mail consent, they are comfortable with other things, and one thing I'd like to make -- I know that people at

this panel believe that, but I want the industry and the press, especially, to understand that there isn't a dividing line between watchdogs who want to keep the place safe and children's content providers who are these mean, horrible pirates.

Kids -- in the kids industry, most of them aren't making a lot of money, notwithstanding IPOs, and they really truly care, and a lot of them really want to make sure the kids are safe, and I hope Kathryn recognizes this, and I was just wanting to reiterate that we are all on the same side. We are all on the side of children and their parents.

But I think that they found that parents love it when you do this, and a lot of the sites, Freezone and Headbone, have some of the safest chats on the Internet. So, in their case, they have to do some type of offline consent given the fact that the kids are chatting in realtime, and that's where some of the higher risks are online.

MR. PEELER: Okay, I want to go to Kris and ask him if that model works for Nickelodeon and then go to Kathryn.

MR. BAGWELL: Yeah, I think that in our -- again, in our research with parents, I mean, it -- it makes sense to us that there is a real divide -- you

know, I think it would be a mistake to draw a curtain across kind of everything that a kid site does and say that you have to have this kind of consent for everything that a kid site does.

You know, in our case, we have got our entire brand in a gigantic business riding on kind of doing this right and getting it right, and so sometimes I think that's led to us being a little more conservative, perhaps, than we could have been to this point.

I think that it -- when you're dealing with applications with kids that are not realtime, kind of in the ability of a kid to kind of reveal unintentionally often identifying information about himself and you're monitoring these things in advance, you know, be it bulletin boards or contests or whatever, then I think it makes sense to make that a very fluid experience for the parents to be able to give consent kind of with e-mail, you know, on the spot, because if you look at -- and again, I think a lot of this is about what a site's business practices are and what it does on a daily basis to make sure that kids are in a safe environment.

I mean, often what's going on behind the scenes in terms of how things are done and how often they look at it and how they're screened is going to really be the nut of the issue as opposed to, you know, kind of the

curtain drawn up front, you know, so that makes a lot of sense to us.

I think that -- I mean, I think again, just to go back on our comment on the question about parents and credit cards, overall I think that for a site like ours, we approach 3 million unique visitors a month. Any kind of paper method of receiving faxes and snail mail and everything else gets to be more than a bit overwhelming, and, you know, even though we are -- again, even though we are a large company, I mean, we are running an online operation as an -- again, as an operation that really needs to pay for itself.

MR. PEELER: And Kris, what about the toll-free number?

MR. BAGWELL: The toll-free number, I think that, you know, our concern is -- and again, I think it has its place as one of the methods that we would like to be able to use. I think that, you know, it is expensive. It also depends on what you're going to do. I mean if -- you know, this fall we'll be launching a number of real expansions dramatically of what we do. If that registration process, you know, if you want to ask a parent, you know, Okay, for your 9-year-old, can he have access to e-mail, chat, IM, and you are doing a lengthy registration process over the phone, that gets

to be a lengthy process, as well.

It depends on what you're going to do. Contest entry at a dollar an entry is one thing, but a lengthy registration by 800 number is kind of difficult.

MS. LEVIN: If I may follow up on that, Kris, in your experience with the contest entry, Nickelodeon has run contests on television for years and on your website you also have contests where you have kids send -- hopefully kids with their parents send in postcards, if you have any indication of what those costs are.

MR. BAGWELL: Our costs of, you know, in terms of the mail, in dealing with the mail, I mean, it's a bit of an apples and oranges thing, again, and I would caution -- you know, in our filing I think we mentioned that kind of just the straightforward costs of receiving and sorting the mail was in the order of, like, I think -- you know, 8 to 15 cents, but again, I mean, we look at that in the online world and we say, Okay, now, how long is that form? If that's a form that now has to be entered and has, say, 15 or 20 fields of data that then have to go in, and if you've got data consistency issues and you've got, you know, legibility issues and things like that, I mean, you have got -- this is much more about what's the length of that process and what level of person does it take to kind of complete that.

So, I think while you can start with a comparison on the entry on the online -- on the TV contest side, it's really kind of the very, very bottom of that -- of that chain. So, we think it's significantly more expensive than that.

MS. AFTAB: Lee, I just wanted to clarify one thing on the telephone consent. Rather than taking a lot of the information, one of the things that we've learned, not that I'm advocating this has to be done, is that the parents can say, Hi, this is my kid, this is their -- this is the log-in name that they want to use, and this is my e-mail address you can use to contact me from now on, forever, and then it's a way of confirming that the e-mail address is verifiable, and that's -- that's the real benefit on using the 800 number, because once you get into the fields, it's impossible to deal with.

MR. BAGWELL: Right.

MS. AFTAB: And the sites that we were dealing with have between 500,000 and 600,000 unique visitors a month, so they are smaller than you are but they are pretty substantial sites.

MR. BAGWELL: Yeah, I think that -- just to go back to the credit card issue one last time, I mean I think that the perverse thing that was going on when we

talked to parents was that they would rather have -- they felt more comfortable paying a couple dollars and having the charge there to verify the parental consent than to do it for free, and it kind of struck us as just an odd consequence of trying to do it this way.

You know, in the end I'm not so sure that that's not going to evolve that way anyway, and people would get used to that kind of model, but --

MR. PEELER: Get used to what kind of model?

MR. BAGWELL: Get used to a model where if the -- you know, down the road, if credit card has become a way for parents to give consent and if they understand that by paying, you know, several dollars they're simply covering the cost of that method of a programmer using that to get that, you know, consent, I think, again, it's empirical and we have to kind of test these things.

MR. PEELER: Okay, I want to go to Kathryn and then Jorian and then John.

MS. MONTGOMERY: Sure, yeah, I just want to underscore what I said earlier, maybe I didn't say it earlier, that you want to ensure that it's a system that is truly verifiable and that doesn't undermine the intent of the law, and I think what's important here is that while the online medium is a very fluid medium,

it's also a very impulsive medium and one where I think we need to institute some caution and create ways where parents can truly be involved.

And I liken it particularly with the one-time registration to sites for this age group, I liken it to enrolling my kid in a class or a camp or a club activity where I want to know something about what they're doing there, and I always advise parents to sit with their kids, and especially this young age group, and talk to them about where they want to go online and really get acquainted with that world and be able to be involved in that decision-making process.

And generally if it is a -- if you really do become familiar with where the kid is going and have a sense of trust in the site and want to register that child for the site and do so, you know, at the outset, then you have -- you know who you're dealing with. You know that kid is in a very entertaining, educational and safe playground.

But I'd also like to say something about -- and I think that it is a cost of doing business for the companies that are -- that are making money off of these kids, because I'd also like to talk a little bit about the potential income here.

We know that children in this age group are a

very lucrative target market, spending and influencing almost $500 billion a year, and Parry and I and a number of you were at the Digital Kids Conference last month, where there were all kinds of projections about how much money potentially online content creators can make from this market. So, I think that we have to put the costs in that -- in perspective in that way.

And at this point it may seem like a huge amount at the beginning of this business enterprise, but as we move forward we're looking at the potential for an enormous amount of money, and also -- and I think streamlining some of the ways these things are done so that they are not costing as much in the long run.

MR. PEELER: Thank you, Kathryn.

Before -- Jorian, before you go, I just wanted to acknowledge Commissioner Anthony has joined us.

Commissioner Anthony, did you want to say anything or should we just keep moving ahead?

COMMISSIONER ANTHONY: I'm hear to listen, thank you.

MR. PEELER: Thank you.

Jorian?

MS. CLARKE: Thanks Lee, Jorian Clarke, and Rebecca, I am going to ask you to join in we me on this one, too.

First of all, I need to correct the fact, as far as I know, no one is making money off of kids online right now. I think most of us here are in this because of the fact that we realize the importance of this medium and the power that can have for affecting kids' lives.

But I think we also have to be aware of the fact that barriers have to be thought through, because if they are too unreasonable, a lot of the companies as we know them right now won't be that same way later, and I think one of the challenges of being a small business in the kids category is that if we speak up too much, we sound like we're whining and saying, "Poor us, poor us, poor us."

But the reality is -- and Rebecca, this is where I'd ask you to back us up on this -- is it does have a significant cost, not only in terms of dollars but also in terms of effect on the kids and the parents themselves. Some of our specific examples Parry alluded to, we take snail mail permission forms for our key pal area, and a lot of times the outside of the envelope is obviously children's handwriting because they have drawn pictures and they, you know, create these wonderful letters that we post, because they're so involving.

Sometimes the inside signature of the parent

looks pretty much like the outside writing on the envelope, and so when we find those, we have contacted the parents to try and make sure that it truly is verifiable. That has an impact on parents, and that has an impact on them wanting their kids to be on the site, because there is a certain trust that they have come to have with us in the way that we protect their kids, and they want us to be involved in helping them learn how their kids are online but then also to trust them that they are involved with their kids, and that's why we found this long-term dialogue with parents is what helps build that trust.

I don't think that there will ever be 100 percent verifiable parental consent unless you have parents come in to a location with their identification and their child's birth certificate.

MR. PEELER: We're not proposing that.

MS. CLARKE: No, no, and I just wanted to caution Kathryn on that expectation because of the fact that similar to what we find with our schools, is they run into the same issues we do when you get signatures or when you have conversations as to whether or not the parent is fully then behind it.

I think that it's also important to understand that we have seen that kids -- it's important to

understand what kids want in content and then to work together as a team to provide that carefully. We know that kids want user-posted content. So, we have gone to a fully monitored system so that any kid's content is screened by a human before it goes live. That does have a cost to it.

People have to understand that -- that yes, that is the cost of doing business, but part of what we as a small business offer is content that large companies might not touch. For example, we had the -- Littleton, Colorado, we had a discussion board and experts available to kids to talk about violence in schools. That wasn't a topic, no offense, that was on Nickelodeon or Disney or some of the other big players that would find it difficult to do that.

There are other things that Rebecca is doing on MaMaMedia that's very engaging to kids and helps them learn about the world that they're in. That kind of educational content often times is -- is offered by those of us in this middle tier, and if the barriers are too high, first kids aren't going to come to us anymore, and second of all, we won't be around in business, but third of all, what we don't understand in this room is the fluidity of kids.

One of the biggest challenges we have is

shutting down fake Kids.com sites, where kids have copied our graffiti wall because they didn't like the fact that we wouldn't allow them to post their e-mail addresses to each other, so they basically exactly copy our wall, put it up, and then send out notification to other kids that they can come to the new Kids.com wall and post anything they want on it and no monitor will shut them down, and we have to track these down, shut them down, et cetera.

Now, if -- if -- I want -- it's important to understand that kids have this skill so that we realize that we have got to give them safe places to play or they will create their own places to play.

MR. PEELER: And Jorian, you have been following this business model for several years now?

MS. CLARKE: Yes.

MR. PEELER: It's been successful?

MS. CLARKE: Ah, yes and no. We have had a high turnover of staff in the position who's responsible for doing this because of the fact that they get tired of parents yelling at them when they called them up to ask them if they were really the ones who were sending in this permission form, and I don't want to make too much of it, but it is, as Parry said, not a job I would ever take.

We get continually letters, e-mails from parents saying we thought we would take the time to let you know how much we appreciate your site because of the fact that now, in the school, at home, we know our child can play here, and we know that you're responsibly playing with them.

MR. PEELER: Thank you.

John and then Rebecca and then Jeff.

MR. KAMP: Actually, what I was -- Jorian said much of what I wanted to say, but I wanted to make a couple of points. In effect, I wanted to give you some notes from the field, because over the past couple of weeks I've been calling members of the American Association -- oh, John Kamp from the American Association of Advertising Agencies -- members of my association who do kids' websites and ask them about in a general way, and I haven't done anything that I would even pretend is science here, but there are some interesting notes.

Virtually everybody is paying attention. The statute and what the Commission is doing here today and has been doing to help sort of all of us, and most importantly I think parents, to pay attention to what's going on here and learn how to use this medium in ways that works for them and for their children.

It's also working in the -- in sort of the field, in the places where people are doing this, because everybody's trying, in effect, to comply, to the extent that they're -- that they're collecting data, they're trying to make sure that their collection practices work, not only work to make sure they stay out of trouble with the Federal Trade Commission and others, but they work with parents.

And my second note from the field, from them, is that it's very hard. It's not easy. They tell me, for example, that what parents seem to really care about is notice and opportunity and the kinds of details. Most of the details we're talking about here for the parents in their day-to-day activity as they develop these sites that work for them and also work for the kids is that much of these details are details for them, and they are not details that parents really want to get into.

They just want to know what's going on and they care about what's going on, but all of it costs a lot of money. It costs a lot of money to do it right, and often times the -- for whatever reason they can't get consent back, so they lose customers.

So, I -- I raise this as a way to talk about what I think others have talked about here, is that this careful thing that we need to -- we need to pay

attention to this medium and how we regulate it and how we deal in it, because all of us are trying to determine as adults and parents and as parents of our children how to deal with this new medium to do what we as parents always do, and that is to teach our children how to become adults.

And for the most part, one of the ways -- one of the analogies that works for me is the difference between a safe street and an unsafe street. First of all, we just keep our kids off the street and then later we try to teach them how to deal with their own lives there and learn to be careful there.

What we seem to be doing in some of this is to not be creating sort of places where we can recognize where a safe street and an unsafe street is but in effect to be building Disney Land kind of parks where we want to build an enclosed environment that's so perfect that everybody who goes there always has a perfect experience there, and it really picks up on Jorian's comment about we have to be very, very careful, because kids will create their own parks if we don't -- if we don't make it possible for them to find them and find those that work for them.

We are in an environment on the net that we all know frankly is full of very unsafe streets. There are

unsafe streets even for us as adults, and when we happen to put whitehouse.whatever in there and we find that we're in the middle of a site that we really don't want to be there, we know that that's also an unsafe place for our kids.

We need to make sure that in the development of these systems we allow the development of parks by smaller companies as well as larger companies and spaces for people where they can find the kinds of places where kids can learn to play and to become adults, and it's not that easy.

I also wanted to commend the CME and Junkbusters for the piece of research that they've put on the table yesterday, but I have to tell you that I'm skeptical of it. In all of the discussions that I've had with professionals who are working in these areas every day, these numbers don't look right.

In fact, it's -- sometimes it reminds me a bit of Proctor & Gamble's senior executive came into a National Advertising Division and Better Business Bureau discussion of research a couple of years ago and said, You know, it's real easy to find what we're looking for. It's not easy to find out what's really going on out there.

And what's really going on out there from the

perspective of all the people that I've been working with and others, and looking at the Georgetown Study for Adults, these numbers don't look right. So, I am going to ask the CME to put all of their research data, particularly their questions and how the questions were arrived at and what the questions were, sort of on the record so that we can all look at them very seriously, because I think that the data, the raw data in and of themselves, at least, raises some very serious questions for all of us.

MR. PEELER: Okay, Kathryn, one minute on that or --

MS. MONTGOMERY: No, may I just on that or may I just make my comments?

MR. PEELER: Okay, go ahead.

MS. MONTGOMERY: I will be happy to respond and we will be happy to submit them.

Again, I think you have to realize that we're looking at the -- looking at a -- at an unorganized web out there. You're dealing with a lot of companies you have everyday interaction with, and there simply is a lot that still needs to happen here just for compliance with this law and to seek privacy protection.

The other point I want to make is that we are really looking at the creation of a new media culture

for children. It's really a digital culture. It's also one that will be connected with television, as everybody knows here, and when we see convergence, we will be looking at ushering in a whole new I think powerful culture for children, and I want to make certain that in doing that we create one that has built into it safeguards.

The reason all this came about is that we identified early on that there were practices emerging out there that were potentially harmful, where had there not been FTC action and had there not been a law passed, invasion of privacy would have been rampant, and it would be the norm, and what we want to do is to ensure that there are some ground rules here that everybody can follow and that they're consistent.

I would -- I'll save my question -- I do want to ask a question actually of some of the participants, but if you want I'll save that.

MR. PEELER: Okay.

MS. MONTGOMERY: How do you want to handle that?

MR. PEELER: Why don't you put out the question right now, but I want to finish with Jeff and Rebecca.

MS. MONTGOMERY: I actually have a question for Rebecca.

MR. PEELER: Okay.

MS. MONTGOMERY: I just wanted to ask you, Rebecca, because you talked about using e-mail to notify in an opt-in -- opt-out method for parents signing their kids up for the service, right?

How many kids are registered on the MaMaMedia site and what percentage of responses have you gotten back from parents? You talked about a number of them sending responses and saying, you know, how happy they were that you had notified them.

MS. RANDALL: Several hundred thousand registrations exist, and what's actually interesting, this is the "be careful what you wish for" category, is in one notification that we did send to parents, we found, without having an exact number, the vast majority of those e-mails to parents were responded to.

It's only in our interests to have the parent involved, so it -- it's interesting, though, to note, I was going to add that, so I'm glad you asked, that in this case it -- we did not find that we sent out an e-mail and nothing happened. We sent out an e-mail, and we got a lot of responses. So, I think that speaks to, again, thinking about -- it's only -- it's only our goal to be talking to the parent in the first place.

MR. PEELER: And Rebecca, does -- I think in

your comment you said 96 percent of the parents responded to that e-mail or some high number like that. Is that a pattern that you see?

MS. RANDALL: I'm giving you one example because I don't -- it's -- at this stage of our company, that's about the, you know, the concrete data that I can share, but --

MS. LEVIN: And Rebecca --

MS. RANDALL: -- it's interesting.

MS. LEVIN: -- only the parent's e-mail address or the parent's and child's e-mail address?

MS. RANDALL: We ask for -- we collect very little information, and, in fact, it's free to go to MaMaMedia and play, and so there are activities that -- and this goes to another point that Kris has mentioned, is that it probably makes a lot of sense to design levels of involvement that are tiered with levels of permissions, for example, because a child can go to MaMaMedia and play to their heart's content and --

MS. LEVIN: But with regard to the e-mail address that you collect, is it a parent's e-mail address or a child's e-mail address or both?

MS. RANDALL: Both, and we ask the kid literally on the sign-in sheet, which I have with me, for screen name, parent's e-mail address, child's address -- e-mail

address, optional, and another thing that's another reality is that kids don't always know what -- there are multiple users of one computer, there are multiple e-mail accounts, but what we ask for is the parent's e-mail address and the child's e-mail address.

MS. LEVIN: Can you tell us in what percentage of instances they are the same or in what percentage they are different?

MS. RANDALL: I don't have a number.

MS. LEVIN: Could you go back and perhaps review that data and get back to us for purposes of the workshop record? That would be great.

MR. PEELER: Jeff has been waiting patiently, and after Jeff, we have a number of flags up, but I would also like people to address the question of or give comments on the question that both Rebecca and Kris have raised about their -- about having a sliding scale for what type of parental consent based on what type of notice, because that's an issue that comes up in a number of comments that were filed in the rulemaking.

Jeff?

MR. RICHARDS: I'll be brief, a couple of points.

One is, you know, we have talked about the cost of doing business. I think we should be really

careful. It's very early on. The incentive is not to build in extra costs as a going-forward notion and, you know, begin to have problems with three segments that we talked about. Mom and pop, midsize and corporate giants is the way that Parry phrased it.

So, the key is this. We're early on. Everyone needs incentives to continue to experiment. What we need are choices, and we need to be -- have different and competitive business models as we set ground rules. We need to have innovations. I like to see dollars applied to market testing, some of the innovations we will probably hear about later, make sure that there is investment in new solutions, and for those who are cash-strapped -- and that's a lot of folks -- they are going to have to make very careful choices.

So, let's be aware that we are talking about the cost of doing business and therefore abilities to be nimble and innovative and to be really focused on what's working for kids and parents.

My second point is that, you know, in 15 years or so today's cyber kids will be parents and, you know, in an odd sense some of this may be short-term in that generational sense, and so what we absolutely want to do is teach today's kids that whatever rules we make are flexible, work in the web environment and are the kinds

of principles that they themselves will adopt as parents.

If we make this frustrating or illogical or stifle the immediacy or substitute it for paper and fax, then what we have done is teach today's kids that as parents they are going to do it otherwise and not through this set of ground rules that weren't as effective as we had hoped.

MR. PEELER: Thank you.

Char? Char Pagar, Promotional Marketing Association.

MS. PAGAR: Hi, just a couple of quick comments.

First of all, the PMA would support the suggestion that was made by MTV Networks that this should be a sliding scale between the type of information that's collected and what's done with that information and the type of consent that's required from parents.

Second, just as a quick note, the PMA is aware of at least one situation that's sort of a variation on the print and send mechanism that we talked about, and it was essentially a print and bring in to a retail location type of promotion, and what actually happened in that situation is the response rate was so low that

they decided not to do the promotion anymore. So, to some extent offline consent mechanisms may just be so slow that they, you know, prevent promotions from being conducted.

And the third quick point is even when you do something like an offline consent and have it brought into a store, have it mailed in, it really is very difficult to verify signatures from parents and to verify information from parents. So, we would urge the Commission to be cautious in assuming that online consent mechanisms are less verifiable than offline consent mechanisms, because, in fact, there may be some difficulties with all of the various methods.

Thank you.

MR. PEELER: Thank you, Char.

Cassidy?

MS. SEHGAL-KOLBET: I guess I just -- I just wanted to reiterate that where sites are engaging in activities that permit children to participate in contests or electronic newsletters or other online games where they're not posting information about themselves, we would certainly be open to the idea and we encourage, we actively encourage the bulk of our sites to provide direct parental notification via e-mail and provide opt-out.

And we are certainly cognizant, also, of the costs involved, you know, in terms of the sites that we have forced to implement offline verifiable parental consent, and in addition to the financial costs, there are certainly -- one thing that we didn't talk about was there are -- there is a high -- there is a high drop-off rate right now.

One site that I worked with just last week called me and said since instituting verifiable parental consent, we have noticed a 50 percent drop-off, and we have had parents call us and say why can't we just fill out this form online. And I think that what this signals to us, also, is that right now this is not -- this system -- the system of verifiable parental consent that we have been working on is not perfect yet and that there is going to have to be some flexibility going forward and in trying to work out what mechanisms are going to be the most effective.

And I guess the final thing that I wanted to say was also relating to the study that -- that has come out, and while I don't have formal numbers in front of me by any means, I do want to say that in our experience and in preparing for the comments here today and in working with many of the sites that we did, we found that the bulk of the top 100 sites for kids that are

directed for kids were posting and were compliant with CARU's guidelines.

So, we're also very interested in working with the CME and trying to get a sense of the picture that they've presented, and we also want to make clear that while our experience has been terrific in terms of the sort of changes that we've seen in the kids industry, there are a lot of mom and pop sites out there that don't know about COPPA, that think it's great to have pen pal clubs, you know, people sitting at home and, you know, they're -- you know, they have key pal clubs for kids that are completely outside the scope of the law, and so I certainly hope that when you look at these figures you'll also take that into account or that CME will make that clear to us, whether that's the case.

Thanks.

MR. PEELER: Thank you.

Caroline?

MS. CURTIN: Yes. I just wanted to add that I spoke a little bit about how AOL obtains upfront consent for the collection and the use of a child's screen name or e-mail address, but I wanted to add that if we need to collect further information, say to mail out a prize for a contest or one of our partners needs to do this, we do require prior written parental permission at this

time.

And AOL really went out on a limb and was requiring that before the statute was enacted, despite the costs, because we felt that really that gave us the greatest assurance that we were obtaining permission from the parent, at the same time recognizing that the great part about this medium is that it is so fast paced. It is seamless hopefully in many instances.

We would be very open to exploring the possibility of expanding our policies to use a 1-800 number that parents could call in order to give parents more choices and sites a little more flexibility and in addition be very open minded to e-mail-based consent mechanisms if we could be assured that that was coming from the parent, as well.

MS. LEVIN: Caroline, in terms, again, of getting some data on the number of children that have e-mail addresses, would it be possible for AOL to provide us with information about what percentage of family households do have children that are given screen names and e-mail -- therefore e-mail addresses?

MS. CURTIN: I think it would be hard -- it would be challenging to come up with a hard and fast number for that, because, you know, we have parents that elect a certain screen name for their child that would

be, say, a kids-only screen name, which we strongly recommend for a child who's 12 and under; however, you may have parents who decide for whatever reason that they want to -- because the child may be more mature, may be 12 years old, but they want to give that child a young teen screen name. So, it would be challenging for us to decipher, you know, the exact ages of the children.

What I can say is that we're really, really excited, because in studies we've done, we've learned that of AOL households with children between the ages of 6 and 17, almost 80 percent of the parents are activating and using parental controls.

MR. PEELER: Hmm. We have both Kris and Rebecca with cards up, and I'm wondering, Kris and Rebecca, if when you talk you could discuss this issue that Caroline's presentation raises about the tension between your practices with respect to obtaining parental permission for use of intellectual property, artwork and stories, where you do have a form that's printed out and mailed back in, and the suggestion that to collect other information from children it should be done electronically.

So, why don't we start with Kris, and you can address that, and then your other point.

MR. BAGWELL: So, you -- this is Kris Bagwell. You're asking that we're saying that we collect it by print for certain things but then why would it be difficult for us to collect it for --

MR. PEELER: Right, and is there a tension there.

MR. BAGWELL: Right, well, I think there is. I mean, I think that we know that, you know, with certain activities that we put up, we have an idea -- we can understand the traffic pattern and know how many of those, you know, we're going to get, and any piece of content of a given site is only getting a, you know, some small percentage of the traffic on a site. So, when we do this and their comments come to submission to Nickelodeon, we have kind of an understanding on what it costs us to do based on historical patterns there, as well.

When you kind of shift from that to, you know, registering perhaps up to 3 million kids on a monthly basis coming to the site, you're really into a whole different order of magnitude of cost, and I think what it -- what's it's also about is that when we're getting permission for kids sending in artwork and whatever, there is not a matching up. There is not this kind of one-to-one match that has to go on.

You know, if you are taking part of the information online and then receiving the parental consent in the mail, you know, we have looked at everything from bar code scans to everything else to figure out what the best way to do that is, but you get into a much -- I think it's just an order of magnitude difference in terms of the cost to us, as well.

I think it's interesting, we -- just to go off on somebody's comment earlier about e-mail addresses and kids, I just want to say two things. We have kind of asked ourselves -- I mean, one of the questions when we were down to visit you guys at the FTC one time, the question is why do we need to collect certain information from kids, are we collecting anything more than we have to, and it's our position and our philosophy that we don't want to collect anything more than we absolutely have to to provide the kind of environment and, you know, and experience that we think is appropriate for a kid of that age.

One of the problems, though, is when we were doing online contests, if you were going to notify the parent, if you asked for a parent e-mail to notify that a kid has won a contest, a lot of parents aren't reading their e-mail or they are not going to read it for a week or two or it's an old e-mail account or something like

that, and so you get this kind of disconnection between the activity level of a kid who is interested in knowing, you know, Saturday if they won the contest and the parent who's not going to go look at AOL -- even if it's not AOL, but they are not going to go look at their Microsoft Network e-mail because they are busy reading their AOL mail. So, you know, there's that kind of issue, as well.

The other -- you know, the other thing I would say about e-mail, there's a bit of a -- we totally agree that the -- you know, what we're interested in doing is matching the consent and the way we get it with what we're doing on the site. I think that we're just trying to kind of strike a balance between what we do on the site and what we kind of have to go through to be able to drive the model forward, and while it is early in the business, Kathryn, there is a big potential in this business.

I think one thing that the smaller sites and the larger sites probably don't differ on is that the appetite for investment in this business to really drive the level of kind of good kid content really rides with what management and the owners of these companies see as kind of the baked-in cost of doing business in this arena. So, I think that we're -- you know, we agree

with you that it is a cost of doing business, but, you know, it's a judgment call on kind of what that is overall.

You know, one of the other comments that I just wanted to mention that I remember that we got in our focus groups with parents is we had held out e-mail -- we had asked them all the different methods before we got their response on e-mail and before we even asked about e-mail, we asked about credit card and phone number and everything else.

E-mail came up and it was one of the fathers who said, who said, Gees, I can buy a car, I can buy a house, I can practically arrange for like an organ transplant online now, why wouldn't I be able to give consent for my child with e-mail? So, there is a sense --

MR. PEELER: Kris is setting up the next panel here.

MR. BAGWELL: So, there is a sense that they expect an online medium to have an online solution for this, so that's what we have to come up with.

MR. PEELER: Rebecca?

MS. RANDALL: I actually, if it's all right, wanted to talk about what I raised earlier to make sure that we don't rule out the teacher in the classroom, and

I had an idea, we could talk about it another time, but as opposed to talking about the issues that have been pretty well covered about the various methods, et cetera, but the idea would be that to -- I think it strikes me as I hear people talking here, I know that our expertise is about creating powerful learning experiences, and it's not creating foolproof validation experiences.

So, I think that's why we're all here, to try to learn what things are working, what makes sense, what's reasonable, and the one thing that we want to make sure of is that since there's currently no provision for dealing with the supervised learning that can come from other third-party qualified adults, the rule doesn't address the school-based interaction or organized group activities.

So, one of the scenarios that we want to make sure doesn't take place is let's say a child -- let's say a teacher wants to provide to their classroom over a year, over the school year -- you know, their lives are dependent on a school year that starts at a certain point and ends at a certain point. Couldn't we make it easy for teachers to have time-based accounts, group accounts, for which the teacher is the point person for that learning experience, and they can notify parents

but not hold up an entire classroom or a year of project-oriented activity because we have now put them in the position of getting a verifiable parental consent --

MR. PEELER: Right, and you did raise that in your comment, and so that will be one of the issues that we'll be looking at in connection with the rule review.

We are almost exactly on schedule, and to conclude, I'd like to just ask each of the panelists to give me a one sentence on what you think the most important point that was raised today at the panel for our consideration should be, and I'm going to put Caroline on the spot by starting at her end of the table and just moving down the table.

Caroline?

MS. CURTIN: Let's see, the most important point? Can I choose one that I made?

MR. PEELER: You could do that.

MS. BERNSTEIN: We would very much expect you to do that.

MS. CURTIN: Thanks, Jodie. You know me well.

MR. PEELER: Could you speak into the microphone, Caroline?

MS. CURTIN: Sure.

The most important point that I'd like to make

for AOL is really that we feel that we are offering consumers and our partners a real service by obtaining up-front consent early in the process when a parent signs up with AOL. We want to be able to continue to do that, but again, we don't want to be -- we don't want to be held liable if for whatever reason one of our partners acts out.

MR. PEELER: Okay.

John Kamp, AAAA?

MR. KAMP: An important point, perhaps the -- the very fact of this meeting, which I think importantly the press is here and other people are here to help the American public learn where the safe places are for this new medium, and the more of these kinds of things that the agency and others can do to raise the awareness among the American people, the better off we all are.

MR. PEELER: Cassidy?

MS. SEHGAL-KOLBET: I guess flexibility in going forward where sites are doing the right thing and are protecting children's safety and privacy and continued adherence to verifiable parental consent where children are able to post and exchange information with third parties.

MR. PEELER: Kathryn?

MS. MONTGOMERY: I do think the fact of this

meeting is very important, and I'm very glad it's taking place, I'm glad to be part of it. My I guess principal point is a warning that in our efforts to be flexible -- and I'm certainly willing to be flexible -- we do not end up creating -- lowering our standards, I guess I would say, for implementing this law and creating what could, in effect, be loopholes that would enable some companies to get around the intent of the statute.

MR. PEELER: Thank you, Kathryn.

Rebecca?

MS. RANDALL: I think I hear violent agreement around this table, which is really about trying to establish standards that serves kids' interests, empowers parents and importantly other qualified adults, elevates the standards for kids, which I think is everyone's mission here, and also doesn't inadvertently disenfranchise some kids versus others because of the way that they're accessing online.

MR. PEELER: Great. I am going to skip Toby and David.

Kris?

MR. BAGWELL: Kris Bagwell.

I would just encourage the Commission -- I do think today has been an important event. I would encourage the Commission to allow all of us on the panel

to continue to try to create the best places for kids online by having, you know, by letting us be responsible and having us, you know, match what we -- what we do to kind of make sure we have parental consent with what we're actually doing on the site, and I think that will create really the best experiences for kids online and keep them in a world that's really designed for them.

MR. PEELER: Paula?

MS. BRUENING: Yes, Paula Bruening with TRUSTe.

I think one of the most important points that were made today was actually made by Kris to my left. I think that it is important to recognize this is an electronic media, and we -- and that we at TRUSTe feel that the kind of parental consent that should be available should be one that is available electronically and that e-mail probably is the most viable way of doing this.

But we take our commitment to assuring that these mechanisms are really working, we do the monitoring on an ongoing basis, and so we recognize also that e-mail response has got to be coupled with something else that makes it a more robust approach than we have right now.

MR. RICHARDS: Jeff Richards, Internet Alliance.

I learned that answering that 800 number must be a heck of a job, which gets me to I think a point I have heard here, too, is that's exactly an issue we need to be careful about, is mandating early solutions for things that we already know have problems, where there's a requirement of experience of actually developing expertise that we can freely share, too, around the table. So, I'm hearing strong agreement here, as well.

I'd love to see incentives for investment of human intelligence, creativity and capital into solutions that will achieve the goals that we've all talked about today. I really fear inadvertently picking winners and losers. That's my concern.

MS. CLARKE: Jorian Clarke with KidsCom and ParentsTalk. I like very much that information and collection needs are not the same. I like the sliding scale based on what information, how to use. I really urge the Commission not to forget that kids and families are not the same. Don't forget about the nonprivileged kids who need to still be able to use this medium.

And then last of all, small businesses need to stay in this kids communication medium, and we need to consider those differences, as well.

MS. AFTAB: I agree.

MR. PEELER: Parry, you have to identify

yourself, Parry.

MS. AFTAB: Parry Aftab.

I like what everyone said. One thing, though, based on what CME has told us today, if the statistics are true and if a lot of sites that we're not aware of aren't complying, I think what we need to do is educate the sites that aren't here today on how to do that. So, even though I'm supposed to be just writing my book, you know, A Parent's Guide, Protecting Children in cyberspace, I am going to have to wait two days, and when I get back to New Jersey, I will recode the CyberAngels site, which is actually the most active of all my things -- I'm actually the web master there -- and provide as much information as I can and information about the sites that are doing this so they can get credit for what they're doing.

And a couple of free e-mail policies that as a cyberspace lawyer I think might make sense is band-aids for the sites who don't know how to hire a cyberspace lawyer or couldn't afford us anyway, I do remember we bill sometimes, and so that we will try to provide a place at the Cyberangels.org site as a resource until the FTC stuff gets up, because I think they have got the best resource in this area.

MR. PEELER: Char?

MS. PAGAR: Char Pagar, PMA.

Two final points, I guess. One, we very much support the idea of the sliding scale, and two, encourage the Commission to not -- to explore very carefully the ideas of online consent mechanisms and allow the technology to develop, create flexible regulatory standards that will allow the technology to develop in ways that will benefit us all.

MR. PEELER: Thank you, a good summation and a good segue into our next panel, which will explore electronic authorization.

In the -- but first we have a brief period for which we can take comments from the audience, and if I will -- you will have to step up to the microphone and identify yourself and your organization. If we could just get a line, I think that would be great. We will start with Ron Goldbrenner, a frequent participant.

MR. GOLDBRENNER: Hi, I'm the general counsel of the Promotional Marketing Association, and I thank the Commission for the opportunity and for the appearance.

I'd like to translate something I heard into what I think is really the most important issue that we have to face in this. I think the Commission has to develop an equation of reality with respect to at what level of regulation do you drive entrepreneurs and

companies away from doing children's sites and at what level of regulation do you drive the children away from visiting the sites?

And I think that's more important than establishing a level of security, because if there are no sites and there are no kids visiting them, you can have the safest procedures in the world, and it doesn't do you any good. We may have to give up some level of security in order to achieve the reality of dealing with the greatest number of people and keeping them at the safest level we can and still attracting them to this medium, still allowing this medium to develop.

But I think from a regulatory point of view, the essential issue has to be how do we keep the most people coming in and not block them out with a level of regulation but still provide some level of security.

Thank you.

MR. PEELER: Thank you, Ron.

MS. CATLETT: Hi, I'm Jason Catlett from Junkbusters.

I'd like to ask Parry Aftab about this wonderful experience we had with the woman who checks the 800 number and switches the phones and makes the calls on yes, that was an 11-year-old trying to sound like a parent and then it wasn't. It's a very difficult job

obviously. Some people would do it better than others, some people would do it more diligently, and we could expect that at some companies experience would be stronger than others and that there would be a level of variety of quality in the job being done here.

Now, I think the key question for the Commission is what quality is proper to be expected of such a person? And Parry has said that you cannot expect absolute perfection in this case. So, how do we rate that and what mechanism is the Commission going to have for determining what an acceptable level is here in some -- in a technical sense, you can look at this as a cost of a false positive versus a false negative.

How many children do we let through as an adult versus how many real parents do we not because we thought they were children because they had a high-pitched voice? So, how do we make those decisions and how does the Commission ensure that they're verified?

MS. AFTAB: Jason, you know I'm a fan of Junkbusters, the new book. I think this is part of what the children's industry is concerned about, because if there's a good faith test, we need a safe harbor of some type, so that if we hire somebody and give them as much training as we can, we are still dealing with people who

will allow things to slip through even if they're being diligent, and I think it's Caroline's concern, too.

I mean, I think all of our concerns is that we are not strictly liable, that if something -- if a child gets through that we thought in good faith was an adult that we are going to face liability on that end, and I think that's something that we're all hoping the Commission will deal with, but --

MS. CATLETT: Parry, would you support a requirement that sites keep records of all of the instances of consent that they have that would be available to the Commission on a random basis to audit so that it could be established that a certain level of --

MS. AFTAB: Absolutely, and when I represent clients, because we do a lot of safety and privacy consulting as well as the law, we advise them to keep records and keep copies of the tapes and do all of these other things. There's a cost to that, but I think, as far as protecting everybody's liability, I think that's the safest way to do it. So, I advise them to do that. I don't have any objection with that, and I would support that type of thing.

MS. CATLETT: Thank you, Parry, and could I invite the other corporate representatives here to

express their willingness to keep such records and to make them available for audit with the FTC?

MR. KAMP: No, I would not. I disagree with Parry on that. I don't think the agency is in a very good position to be the decider of who has good judgment and who has not good judgment. I remember in my own case the one time I tried to sign a bad report card, the nun handing it back to me with a smile and saying, "No, I think you better take this home."

I don't think that is the kind of thing a federal government agency can do a very good job on, and I think the development of a set of rules that would require, as a matter of law, in order to get into this business that kind of a record keeping requirement would take us some places I don't think we should go.

MS. CATLETT: John, could I point out --

MR. PEELER: Jason, I think we need to keep moving along. Thank you.

MS. AFTAB: And John, we'll talk.

MR. BRYAN: Good morning, my name is Steve Bryan. I'm with Zeeks.com. I have a million questions. I guess I am going to limit it to one in the interest of time.

I'm just interested in the panel's opinion, anybody really. We have been in this business just a

short time. We launched a children's website about four months ago, and one of the things that really has been exciting and has impressed us is the ability and the willingness of lots of the I guess what you'd call the mom and pop sites and the midtier sites to work together to provide different strengths at different sites.

We've worked with Headbone and we've worked with Freezone, and we've found very receptive management teams at these companies to help all of us build this industry. My great fear is there is going to be a dramatic chilling effect on that with this parental notification and that, in fact, what we will move to is who does the best job of parental verification, not who does the best job of providing kids content.

And I think I can stand here and give the answer, at least from my perspective, is a few years or so down the road, the winners of this will be the people with the very high-recognition, trusted brand names and that MTV, Disney and Warner Brothers will be the dominant players, and there will be no room and no ability for the small companies to participate not because of content or not because of good intentions but because of the very high hurdle to getting parents to go in and give verification, not just for one site, but for my site and your site and your site and your site and

your site over and over again.

I think that I'd be interested in any comments that anybody has. Thank you.

MR. PEELER: Thank you.

Caroline, do you want to --

MS. CURTIN: Ah, well, let's see. I hope that that doesn't end up being the case. I mean, AOL's -- we're in a very fortunate position, because I think we do have a very strong brand recognition, and it is attached to kid safety and privacy, and we've really put a lot of effort and thought into that, and I think our partners hopefully benefit from that when they sign on with us, and we can go about the business of getting -- of providing notice and getting consent up front for them.

I think it just -- it goes back to really asking the Commission and others to look proactively and think about making the process for obtaining parental consent as guaranteed as it possibly can be but also as innovative and using the online medium really to -- to assure that we can get the kind of consent necessary to be comfortable.

MR. PEELER: And I'd also put a pitch, make sure you stay for the third panel today that's going to talk about that issue, that exact issue, actually, in more

detail.

Next?

MS. MONTGOMERY: Can I respond to that?

MR. PEELER: Oh, yes.

MS. MONTGOMERY: Really quickly. I guess my concern is that in this new culture that we're creating for children, and I do hope that there is a range of diversity and choices for kids and I'm excited about that possibility, that we not create a situation where we have sites that protect children's privacy and sites that don't protect children's privacy, where there's a level, there's a standard that everybody adheres to, so that this culture is one that really will nurture kids and be able to provide for them all of the wonderful benefits of this new digital media that we are excited about.

MR. PEELER: Thank you, Kathryn.

MR. MENGE: Good morning. My name is Eric Menge, I'm with the United States Small Business Administration. I handle all of the Telecommunications International emerging Technologies Advocacy at the SBA. I'm very grateful to be able to come today.

MR. PEELER: Welcome. We are glad to have you here.

MR. MENGE: According to our latest studies,

there are about 24 million small businesses in this country. Of those, 41 percent have a presence on the web, and according to our latest study that should be coming out in the next couple of months, about 21 percent of those have actually engaged in electronic commerce. So, as you can imagine, with that many small businesses involved in this emerging medium, we are extremely interested in any regulation that could possibly create barriers to entry to small businesses trying to get involved in this.

However, we are also cognizant of the fact that there is some public policy concerns that need to be addressed, and we are, of course, looking at balancing the public policy concerns with the cost of regulation.

My question today was on the sliding scale, as was recommended by Mr. Bagwell. My question, I guess, would be addressed over to the small business representatives who we have on this side, and I was kind of curious at which point the sliding scale was a viable option for small businesses or would the complexity of such a regulation actually inhibit small businesses from being able to get -- to comply with such a regulation?

And also, would a sliding scale only rely upon what information is collected, or would it also depend upon the size and capability of the collecting entity?

MS. CLARKE: Actually, I was a Small Business Person Winner of the Year for the State of Wisconsin, but I didn't think I'd mention it, because most people here wouldn't know where Wisconsin is. Rebecca does, she's from Milwaukee.

I think that there is -- you raised very good questions, and I think that that may be another forum or to be picked in a forum that needs to be considered because of the fact that getting into the nitty-gritty, the equipment, the people.

I know, for example, there are some regulatory differences between companies that are 50 people and less and the kinds of regulations they have to follow, and there may be some level there balancing off the need to protect children with the -- with the resources and how to -- and how to match that. So, I do think it needs to be looked into further.

MS. AFTAB: I wouldn't cut it off based upon the size of the company, but I would -- I really support the sliding scale, and so what you're collecting and how you're using it I think should be the judge as opposed to the size of the company, because a lot of the small ones aren't going to be using it and aren't going to be collecting a lot of the stuff anyway, but we need to educate them, and I think that's your job. We'll help.

MR. MENGE: Thank you.

MR. PEELER: A man who needs no introduction.

MR. JAFFE: Well, nonetheless, I'm Dan Jaffe with the Association of National Advertisers. I'd like to associate myself with everybody on this panel who has complimented the FTC and agree that you have been extremely open and the staff has been very helpful to all of us when we have had questions.

I just wanted to ask Kathryn, first I want to thank you for agreeing to provide the backup for your study, because obviously your study has interesting data, but you have one statistic I'd like to at least get some understanding of right away, which is if you say that only 3 percent -- well, let me just read it.

It's, "Less than 3 percent use methods for obtaining verifiable prior parental consent that are consistent with the Children's Online Privacy Protection Act."

What we're doing right today is deciding what is consistent with the Privacy Protection Act, and I wondered whether you did not find those systems who use e-mail, looking at your comments to the Commission, whether those were found not to be meeting the COPPA requirements or how you decided what was consistent and what was not.

MS. MONTGOMERY: Yeah, actually, Katharina can answer that question, too, Katharina Kopp, who's standing right behind you.

MR. JAFFE: Whoever can answer the question.

MS. MONTGOMERY: I am going to let her answer it.

MR. JAFFE: I will step back.

MS. KOPP: We made a distinction. We decided that verifiable parental consent are methods like print and send, 800 numbers and fax, and so we put those in the category of verifiable parental consent, and then we also noted in the study that we had up earlier that the sites that use e-mail also -- were covered there, but there was a separate category. So, that is covered in the --

MR. JAFFE: So, they are not part of the 3 percent?

MS. KOPP: No.

MR. JAFFE: So, if you used e-mail, you would be part of the 3 percent that were complying?

MS. KOPP: No, we had 3 percent -- less than 3 percent that used print, send -- print, fax and e-mail and another less than 3 percent for the random sample that used e-mail.

MR. JAFFE: Okay.

MR. BAGWELL: Can I ask one more question on the data? Is this percent of data collecting sites who were collecting identifying information from children or percent of --

MS. KOPP: Personally identified as defined in COPPA, which includes e-mail.

MR. PEELER: Thank you Katharina, and you have a comment?

MS. KOPP: Yes, I'm Katharina Kopp for the Center for Media Education, and we have also taken the position that it is not necessary to collect personally identifiable information from children under 13 in order to have good interactive websites, and so I was happy to hear from Mr. Bagwell that currently Nickelodeon is not collecting personally identifiable information from children under 13, so I was wondering whether you had noted any drop in the traffic to your website since you stopped collecting personally identifiable information.

MR. BAGWELL: Well, I mean, I should say we -- remember, we were -- you know, today we run -- at nick.com and at Nick Jr., we run basically entertainment-based sites, and so most of our interaction -- I mean, not yet -- we do a lot of our chat and everything on AOL, so that's kind of where the communication piece of our business happens.

Going forward, that's going to change, so this will be a little bit different going forward, but when we did pull back contest entry online, we did see a significant drop in contest entries. I don't have the exact numbers with me, but it was a dramatic drop from the people who would have entered online versus the folks who were going to print out a form online and mail that in.

I mean, it's just a -- I think in the order of magnitude that I think Time Warner had said something in their filing about an 80 percent drop. I don't know that that's our exact number, but it's that kind of magnitude drop. So, I think that we're not interested in collecting anything more than we need to provide the right experience and a safe environment, but again, if you just think about this issue of what do you do in a contest when a parent doesn't read e-mail, if you just try to notify the parent, I mean, there are some very complex little problems here about how you communicate with a household when the kid is a little more electronic than the parent. So, that's kind of what we're trying to balance.

MR. PEELER: Kris, could we -- could I ask, why wouldn't the statutory exemption on contests meet your needs for e-mail on contests?

MR. BAGWELL: I guess I'm not -- I guess I'm not saying that it doesn't. I guess what I'm saying is that we --

MR. PEELER: Okay.

MR. BAGWELL: -- we've considered, just from a business standpoint, we have just asked ourself kind of through this whole process why do we need to be collecting each piece of information that we are? So, whether we meant it or not, I mean, I think we kind of -- for a while we kind of took a de minimus approach to this, let's just back up, let's just back up and say what do we need to do here.

MS. LEVIN: Kris, I think Katharina Kopp's question was whether there was a drop in traffic on the site, not whether there was a drop in contest registrations. Do you have any data on whether there was a drop in traffic?

MR. BAGWELL: I don't have any data on that in front of me. I would -- it -- I don't know. I would need to get back to you about that.

MS. LEVIN: Okay, thanks.

MR. PEELER: Last question or comment?

MS. ELLIS: It's a comment. I'm Allison Ellis from Freezone. We have been mentioned a couple of times before. I just wanted to elaborate on a couple things

we're doing.

We do verifiable parental consent currently through snail mail and fax, and I just wanted to reiterate, it is expensive. It's been kind of a pain to set it up, but we feel really strongly about safety, and we've always taken safety really seriously since the beginning and really take it as kind of a cost of doing business, and in doing that we kind of look at, you know, we're looking at our advertisers, we make them adhere to the same rules that we do.

So, an advertiser says, Hey, can you do this mini site for us? Can you do a contest? We say, Great, you know, build in the cost to do the registration, do the contest in a safe way. I can't say we're making a ton of money, but we're definitely covered -- trying to cover our costs with it. We just really believe that in building our site we have to take safety and the parental consent extremely seriously. Otherwise, we have no business doing everything else that we do. So, that's our position.

Thanks.

MR. PEELER: Thank you.

Well, that concludes the first panel this morning. I'd like to thank all of the panelists for their excellent participation. You brought a lot of

energy and enthusiasm here today.

(Applause.)

MR. PEELER: Now, everyone is allowed a 15 -- 20-minute break courtesy of the panel.

(A brief recess was taken.)

\- - - - -

SESSION II

- - - - -

MS. LEVIN: If everyone on the panel could please be seated and we can begin, since everyone's ready.

Okay, if we could close the doors, please, to the anteroom. Thank you.

I'd like to welcome the panelists to Section II. My name is Toby Levin. I'm a staff attorney here at the Federal Trade Commission and now the team leader for the Internet Advertising Program that's part of our Division of Advertising Practices, and I have been working on the important issues of children's privacy now for several years. And this is the day many of us have been waiting for, which is an opportunity to explore existing and potential mechanisms for verifiable parental consent.

As you can see from the first panel, there is a great deal of interest in electronic mechanisms, and

that's the focus of both Session II and Session III. In some ways there is a great deal of overlap, but in this particular session, we really want to look at what we may commonly refer to as e-mail-based mechanisms, mechanisms that websites can themselves use to obtain parental consent, and in the third session, we'll get more of the intermediary services that can apply across a number of websites, but you'll see some representatives actually in both sessions to address both.

I would like to first just indicate with regard to procedurally, the court reporter would appreciate any handouts, overheads that you use, if you've made copies of them, to be sure to give them to her, you know, as you're using them so that way -- or immediately after so that way they can be added into the transcript of the meeting.

If you were interested in a copy of the transcript, she has some forms that you can complete. It will become available on our website as soon as we can get it up there, as well.

I'd like to start by having each of you identify yourselves and your affiliation just briefly and note that in terms of the schedule, we are -- we will actually have a break in the middle in order to

accommodate lunch, and then we will resume at 1:45, and there will be an open comment period at the end. So, some of you who are just filled with questions or comments, there will be an opportunity for you to raise them.

So, let's start, if I can, to my right, if you identify yourself and your affiliation, please.

MR. PLESSER: Ron Plesser, I'm at Piper & Marbury, LLP. I would really prefer to say cyberspace lawyer, but somebody else --

MS. AFTAB: Already taken.

MR. PLESSER: -- has taken it, and I'm representing the Direct Marketing Association.

MS. HARRIS: Leslie Harris, Leslie Harris & Associates, cyber lawyer, and I represent the American Library Association.

MR. WENGER: Eric Wenger, and I'm from the Internet Bureau of the New York State Attorney General's Office. We filed comments on behalf of a group of about 17 states, and we also chair a group from the National Association of Attorneys General on Internet privacy, but anything I say is my own opinion and should not be used against any of these groups, so...

MS. MILLAR: I'm Sheila Millar with Keller and Heckman, LLP, another cyber lawyer, and I represent Mars

Incorporated.

MR. JAFFE: Good morning, I'm Dan Jaffe, with the Association of National Advertisers.

MS. KOPP: Good morning, I'm Katharina Kopp with the Center for Media Education. I am not a lawyer, and we filed comments with about eight or so other organizations representing children and families.

MS. LANDSMANN: I'm Leanna Landsmann. I'm president of TIME for Kids, which is a entrepreneurial subsidiary -- not a subsidiary, a division of Time Warner, and representing Time Warner here. I'm not a lawyer. I'm not a technology expert. I'm a teacher at heart and wearing that hat while I am here, because I think some of the issues that are addressed here have relationship to schools.

MS. RICH: Jessica Rich, Federal Trade Commission.

MR. TEICHER: Jim Teicher with CyberSmart!.

MR. ALEDORT: Eric Aledort with the Buena Vista Internet Group, the Walt Disney Company's online division.

MR. BRANDT: I'm Jim Brandt. I'm with the VeriSign Company.

MS. FISE: I'm Mary Ellen Fise. I'm general counsel of the Consumer Federation of America.

MR. HERMAN: Hi, I'm Paul Herman. I'm the founder and CEO of iCanBuy.com, which provides safe, secure, private electronic commerce and electronic finance for teens, kids and parents.

MS. CATLETT: I'm Jason Catlett from Junkbusters. I'm not a lawyer, but my degrees are in computer science.

MS. LEVIN: Can you hear me? Is this working? Okay?

THE AUDIENCE: Yep.

MS. LEVIN: I love doing this. I'm a former high school teacher for seven years, and this is a throw-back to those wonderful days of working with kids.

(Laughter.)

MS. LEVIN: I was just going to say, but with you, you're a much less difficult audience, because you have to do songs and dance with kids, you don't have to with adults, because you'll listen.

I thought I'd like to start first of all by getting a list of what are the electronic mechanisms that you either are using now or in your dreams would like to be using so that we have sort of a working list, and then we will go through them in more detail again. So, I just want to be sure we have the world of

electronic mechanisms.

And I always prefer volunteers, but you know in school rooms, that hardly ever works either. You will get a few eager hands and the rest you will just have to call on people.

So, let's start just in sequence here, Ron, if you could start with electronic mechanisms that you think are, you know, viable options for online consent.

MR. PLESSER: Well, that's a different question, but electronic mail I believe is viable in circumstances as Cassidy had laid out, but I think that one of the current features is electronic mail certainly with the presence of a credit card, I think is more what you're generally looking for.

MS. LEVIN: I'm not looking for anything in particular.

MR. PLESSER: Electronic mail with a credit -- with and without a credit card, two categories.

MS. LEVIN: Okay, next.

MS. HARRIS: Well, the libraries use nothing, because they collect nothing, but it's our view plainly that e-mail is an appropriate method of collection, and moreover, that it is no less verifiable than any of the other methods that have been discussed.

MR. PEELER: Toby, can I just interrupt?

For the audience downstairs, you have to speak into the microphone.

MS. HARRIS: So, we have to move it -- oh, it's right next to my name so I can remember it. We have it on both sides for those of you -- does that mean you want my to say that again, Lee?

MR. PEELER: I think that would be a good idea.

MS. HARRIS: Okay, I won't say all of it again. I'm Leslie Harris representing the American Library Association, and yes, we firmly believe that e-mail is an appropriate method -- I mean, that's putting aside whether or not we think parental verification is a good idea in the first place -- and that it is no less verifiable than any other of the methods that are presented here.

MS. LEVIN: And to be sure that we're clear, we understand what you're meaning by e-mail, it's e-mail alone or click-back e-mail --

MS. HARRIS: E-mail alone. I mean, our view would be a credit card is very nice, but most people who use the libraries, families don't have access to credit cards, which is another subject.

MS. LEVIN: Okay, and also keep in mind, that as Lee pointed out earlier today, that the notion of Federal Trade Commission requiring a single method is --

is, you know, already I think pretty clear in terms of our proposed rule, that we are looking at a variety of methods that would be available. So, if -- so websites can have that kind of flexibility.

MS. HARRIS: Right, no, I understand.

MS. LEVIN: All right. Eric, and it need not necessarily be a mechanism that you or your organization supports, but --

MR. WENGER: Well, we are not really collecting any personal information on our website except for -- actually, we have a very prominently posted privacy policy on our website, and we have a complaint form that people can fill out, and it explains exactly on there how that information might be used, but it's not -- it's not really targeted in any way towards children, and we don't get complaints from children, to my recollection.

So, having said that, though, I think that the states are very supportive of the approach that the FTC took, which is to lay out a flexible standard to allow technology to develop and for industry to develop mechanisms that are verifiable and do actually give notice to parents and resulting consent.

Having said that, the exception should not be construed in a way that allows anybody to say it was too difficult to obtain consent. So, any mechanism that

results in something that appears -- that really seems to be the consent of the parent is probably okay as far as we're concerned, and it seems that that's the conclusion the FTC reached, as well.

Having said that, the FTC seems to reach the conclusion that e-mail alone, without some sort of digital signature or some other mechanism of verifying who sent the message, is problematic, and we support that conclusion, as well.

And so I would -- I guess my contribution here would be an e-mail message that combines some sort of digital signature mechanism, and exactly what that is we would leave for the market to determine.

MS. LEVIN: Okay, thank you.

Sheila?

MS. MILLAR: Sheila Millar, Keller and Heckman, for Mars Incorporated.

I think Cassidy outlined this morning the position of Children's Advertising Review Unit or Lee outlined or reviewed again the exemptions to the statute. As a long-standing member of the CARU Advisory Council, Mars supports the CARU Council and guidelines.

Its own information collection practices do not include offering chat rooms or bulletin boards for children, and they certainly don't sell or share data to

third parties. So, the separate parental e-mail technique has worked well for the company and for the types of information it is collecting, and, in fact, as other panelists mentioned this morning, is very popular and well liked by consumers.

MS. LEVIN: And we'll come back for any details on that, but could you just describe, is the e-mail -- what the e-mail technique is?

MS. MILLAR: The e-mail technique requires, for example, when a child wants to sign up for an e-mail newsletter, the child receives a confirmation back from the company, and in the process of signing up, the child is required to provide a separate parent's e-mail address. The parent also receives an individual e-mail notice, which is much lengthier, and I can provide a printed out version for the record if you like.

The parent's notification would include some description of what the content is on the site. The types of information that would be contained in the notice, both notices, both to the parent and to the child, contain instructions on how you can unsubscribe and then subsequent notices, of course, to the child with the newsletter updates would also have the unsubscribe information.

So, it's a fairly straightforward process but I

think perhaps a little bit more descriptive in terms of the content of the site and as coupled with an invitation to the parent to visit the site. And so like many of the other commenters this morning, the company has received a significant number of e-mail from parents complimenting them on the site, on the notification process and expressing appreciation for getting these e-mail notices. They like the simplicity of it.

MS. LEVIN: Thank you very much.

Dan?

MR. JAFFE: Dan Jaffe, Association of National Advertisers.

We also want to compliment the Commission on their focus on flexibility in the rule, and we believe that a part of this flexibility that e-mail systems should certainly be given very careful consideration as a means of verification. As was noted, the e-mail system may be as verifiable as some other systems that are offline.

It's been mentioned that the e-mail systems should -- have so far been coupled with either a credit card or a digital signature, which I think is fine, but I think the FTC should be very cautious in not limiting the -- this approach to any one mechanism.

In our submission to the Commission earlier, we

talk about passwords or PIN numbers, but we're not saying that that's the right way either. We should leave as much flexibility in this area to meet the requirements as long as it meets what the FTC and the law requires, which is that it creates a reasonable likelihood that you are reaching the parent with your notification.

So, I don't think there should be any one magic answer, that the credit card may not be the magic answer, the digital signature may not be the magic answer, though they may work for particular groups, PIN numbers we mentioned, but we don't necessarily think that's the magic answer, but any system that gives you a reasonable expectation that you're reaching the parent should be good enough.

MS. LEVIN: Thank you.

Katharina?

MS. KOPP: Katharina Kopp, Center for Media Education.

We're looking at obviously what the regulation requires, and it clearly states that it has to be verifiable that you are actually dealing with the parents so that you can ensure parental involvement, and so we don't believe that -- currently that there is a mechanism that's electronically based that would fulfill

that requirement, and so we support what the FTC has already said on record in the June '98 report where it specified what it -- what's meant by parental consent and what mechanisms would work, which is for consent, fax, credit card, and in the future, digital signatures.

So, we are, you know, we welcome digitally based consent mechanisms, but we don't see right now any mechanism that would satisfy the statute.

MS. LEVIN: Okay.

Leanna?

MS. LANDSMANN: I'm glad you said the final one, "in your dreams," because we don't think that the perfect one is out there, but we very -- speaking for the Time Warner sites that reach kids, these are free, content-rich sites, most of which do not have a revenue model. I was interested this morning on the first panel about big companies making a lot of money off kids' websites. It's not true.

We very strongly support e-mail accompanied by a digital signature and would like to see an e-mail parental verification system in place now with a short sunset period in which we would all work to identify what's -- what we hear is around the corner that will be ubiquitous, easy to use, cheap, easy to access no matter

what your income level and where you are geographically, and home and school friendly.

And we've come to this position based on interviewing -- talking to kids, teacher board, parent board and student board, and in viewing folks who use other websites that we have. And the "in our dreams," it would be something that's, you know, ubiquitous, easy to use, cheap. It would have some sort of a mechanism that would allow teachers to use what is increasingly common in schools, which is parental permission.

I don't know if you're familiar with it, but most schools now have some sort of internet use policy, and these -- these vary by district, they vary by school, but almost every single school is creating these things, and our teachers, since about two-thirds of the activity on the TIME for Kids site, for example, is during school hours, we want to make sure that there is some mechanism built into the digital signature that doesn't make it cumbersome yet again for teachers to use this site for the kinds of interactivity that we envision.

One of the kids said, Well, as long as you're creating this thing, make sure that there's a child notification provision in it, too, and we all laughed, but that's -- it's -- the child notification provision

is that we have a lot of parents and kids who get on the TIME for Kids website together, and we have -- we hope to institute an online version of this, Family Reading with TFK, where kids put their -- give their responses to an article that they've read and the parents give their responses to the article they read and they bounce them -- right now it's all being done on paper -- they bounce them back to us, and we have this sort of very awkward paper community of people who are responding to the things that they read in TIME for Kids.

But down the line, we would be able to -- we would like to use the potential of the Internet to promote this kind of activity. So, the "in our dreams" would be ubiquitous, easy to use, cheap. I have to be able to -- if it's downloadable, I have to be able to download it. I can't call Marcella from across the hall. And it has to allow for schools to be able to use it and probably use the parental consent that schools are being given.

I did have one other thing that one teacher suggested and one parent suggested that it would be useful to have a registration time period -- and I know some of them already have a registration time period -- but we don't want this thing to be every transaction, but there ought to be certain kinds of things that you

can go on and if it's responding or sending your letters to the editor, the -- there are -- that parents ought to be able to say, "My kid can do this for this school year, my kid can do this for this time period," so that parents feel very strongly that this should not be an every-single-transaction mechanism if the kinds of activities are going to be supervised.

MS. LEVIN: Okay, thanks very much.

Jim?

MR. TEICHER: First, I want to preface this by saying that CyberSmart! is actually in the business of developing an authentication online solution for parents, children and schools, and I want to add digital certificates along with e-mail, but also I have to say that, you know, I think that it's not as much a matter of the technology, you know, as the processes.

I think that just putting a list of technologies is -- is great, but I think that the process has to be easy, it has to be inexpensive, you know, it has to be ubiquitous, has to have value to kids, and kids have to want it in order to for it to work, also.

And I think that we have to keep all these in mind, and this is what we clearly have in mind as we're building these processes.

MS. LEVIN: And we'll come back to hear more

about the service that you're developing.

Eric?

MR. ALEDORT: Thank you, Toby.

I would like to just urge the Commission to remember that one of the key goals is to drive kids to sites that do protect their information and treat kids appropriately, and we're very concerned that asking for credit cards, requiring a fax back, requiring a mail-in, will actually leave kids out of the sites where they should be spending time into places that either aren't designed for kids or don't comply with the methods that you want them to.

We believe very strongly in kind of a safe harbor environment where if a company is collecting minimal information and not distributing it to any third party and not marketing to children in any way, that an e-mail verification opt-in by a parent is sufficient, and that's what we do, while the idea -- if you would like to sell your list or you would like to send a newsletter to your child or somehow market to the kid, different levels of verification would be appropriate, whether that be digital signature, even a credit card, which again we're fairly strongly opposed to because of the disenfranchisement issue, but we look at a sliding scale.

MS. LEVIN: Okay.

And Jim?

MR. BRANDT: Thanks, Toby.

Well, as a PKI technology provider, VeriSign sees a digital certificate or public key technology really as a mechanism to provide Internet privacy and Internet trust, and that mechanism of digital certificate can be applied to a number of different Internet communications protocols, and I just think one of those is up there now, which is secure mail.

Certainly there are a number of free tools out there that exist today that can be used in conjunction with the certificate to provide digitally signed e-mail, but in addition, there's other technology.

Certainly using a digital certificate to sign web forms or a -- or an HTML page, for example, is another mechanism which certainly is Internet-based, gets into the context of a web-based scenario, but is just a different technology, which I haven't heard addressed. So, I would add to that list digitally signed form as another appropriate technology mechanism to provide electronic authenticated communications.

MS. LEVIN: Okay.

Mary Ellen?

MS. FISE: Well, I think this all goes back to

that key word in the legislation, which is "verifiable," and, of course, we take the position that e-mail alone is not verifiable.

With respect to some of the things -- or one of the other suggestions, I just want to comment that we have concerns about e-mail plus credit card alone as being a singular option because of access by a range of consumers, and also I'm -- consumers -- we have concerns about proliferation of credit cards and credit card use, and we don't want to see this as the main password to using the Internet, to have folks get into a credit system when they might not already be wanting to obtain more credit cards for use, et cetera.

MS. LEVIN: Okay, Paul?

MR. HERMAN: Great. Thanks, Toby.

Also, we would like to thank the Commission for being extremely accessible, both by e-mail and phone, though there is no 800 number yet, for being collaborative and --

MS. LEVIN: There actually is an 800 number that we have rolled out just recently. It's FTC --

MS. BERNSTEIN: 877-FTC-HELP.

MS. LEVIN: FTC-HELP, I know it by the words and not by the numbers.

MS. BERNSTEIN: And I want you all to report

that.

MR. HERMAN: So, I will save everyone tax dollars and still call on my dime.

For being extremely collaborative and team oriented outside of the Commission as well as inside the Commission and being conscientious of industry as well as consumers. I think we are fans of a sliding scale, mainly for one of the points that hasn't come up yet, is there are different uses for information, and so there should be different rules or guidelines for those different uses of information.

There is no law against having a free content site which anyone can access, and you don't need to provide personal information to go to a free site. If you'd like some degree of personalization and customization, there can be a fee and there can be a charge in terms of personal information, and if you'd like to share financial information, there's a cost and a benefit to doing that, as well.

So, I think we're fans of the sliding scale, and we have some suggested technologies to add to the list and some suggested processes, but I think the Commission is fully conscientious of focusing on the results and the results with auditable accountability. So, I think we'd all like to be kept to the same outcomes and

results and goals but not micro-manage the process or the technologies necessarily.

That being said, here are some potential technologies to keep in mind. Of course, e-mail has already been listed, and e-mail with some previously verified account, potentially an ISP, like an AOL or an Earthlink. The key domains that we found in parents signing up their kids for commerce services have been AOL number one, which is where many parents and kids and teens hang out; Yahoo, number two, which is a free service but can be personalized and customized; and Hotmail, which is a free service and has more than 50 million accounts. So, in terms of e-mail itself, there is not always a -- you are not always preverified, especially with a Hotmail account, where you can have several per person.

Of course, since our site verifies parents through a credit card or debit card or other trusted financial account, we believe that since most financial accounts are for adults who are over 18 and they are enforceable contracts with adults over 18 or through trusted accounts with minors under 18, that that is a method, again depending on the type of service that you'd like to provide and the type of personalized or customized information that you'd like to provide.

Other technologies to keep in mind aren't just sitting at the computer or potentially at your web TV or your soon-to-be set-top box but also portable devices. So, those would include cell phones, two-way pagers, your personal -- your PDA, your Palm Pilot, and so there are additional ways to have access both personally as well as in the field.

There are companies who have stand alone -- like your bank branch at your grocery store who will have stand alone verification. Today that's a PIN. In the future it could be fingerprint, could be retinal scan, could be body heat scan, but will most likely be voice recognition next, and those are nearly ready for prime time.

And then, of course, any current account with a user ID and password, and something I haven't heard discussed yet is if there's a previous database, which as part of the government or a nonprofit entity or some other trusted entity as to whether that universal user ID and password is an appropriate mechanism so that you do parental verification once.

Parents are not interested in our focus groups and in our customer relationships with signing up for 15 or 20 different registration mechanisms. They like the choice and the control over that; they do not like the

hassle of it.

And then finally, digital IDs and authorization, again, most likely being tied to something that is a -- not a hassle for the consumer, like a voice recognition is probably the most likely technology.

MS. LEVIN: Could I ask a clarification or the -- you said the previous databases. Could you give me an example of what you're thinking of?

MR. HERMAN: There -- there -- I don't see any in use today yet, but businesses collaborate. For example, when Charles Schwab and the Excite At-Home Network recently did a joint -- combined their businesses together, you can sign into the portal at Excite with your Charles Schwab password. So, they have combined their customer databases together, and it's essentially seamless.

It was a surprise to the customers that you could do this and a service and value to the customers, but both are trusted accounts, both the portal account and your financial account, were trusted accounts as they merged together. So, there's not something like that on a broader industrywide basis, but there's the potential for that, and so the question would be, is that something of value? Are there or can we add -- can the privacy risks be addressed so that if that central

database were hacked, that privacy information would not be easily available, how would it be encrypted, various methods like that.

But again, Toby, just wanted to outline various technologies to keep in mind, as technology moves quickly, and process suggestions, but keeping us accountable to results would make sense from an industry point of view.

MS. LEVIN: Thanks very much.

Jason?

MS. CATLETT: Thanks, Toby, Jason Catlett from Junkbusters.

I'm a little concerned about the privacy implications Paul raised of, say, requiring the parents to submit to a retinal scan or a DNA test in order for the parents -- for their kids to enter a sweepstakes, so I think we have to bear in mind that privacy protection is the goal that we have here.

However, I'm delighted that Paul is enthused about being -- companies being auditable for the outcomes rather than the simple particular mechanisms, and it's great that we have this list of options here of -- that companies are exploring.

I'd like to draw people's attention to the options that they decided not to provide because their

direct commercial interests are in conflict with privacy.

Now, a bit of common sense and experience will tell you that a very effective way of avoiding junk e-mail, for example, is to make sure that spammers don't know your e-mail address, and generally a good way to avoid an invasion of privacy and misuse of your information is to make sure that that information is not associated with you personally.

So, think of anonymity as the solar power of privacy. It's infinitely renewable and it doesn't pollute, but is it too expensive or unsuitable for the job?

Well, in most of the tasks that we've heard described today, anonymity or pseudonymity is perfectly suitable for the tasks. For example, Rebecca told us about how children can save their artwork on MaMaMedia's server and come back to it later, and Kris Bagwell gave us the example of wanting to be able to tell a child if they've won a contest.

Now, there are many applications where there are good reasons to maintain consistent information about a visitor in order to personalize the experience, but is it necessary to collect an e-mail address or any other personally identified information in order to do this?

No. And many, many, technical means are available to do this.

For example, a website can ask a user to book mark a page as a unique, pseudonymous identifier, and then when the person returns to that website, you automatically identify that person pseudonymously. It can also be done with cookies, which generate their own privacy problems, but that requires no action by the child to identify themselves. The pseudonymous identity is available immediately when they return.

It's also possible for a site to generate a log-in name and a password that are unique but are not associated with any personal information. In fact, this gets over the problem of two users both asking for the user name "purple."

So, why do companies want to collect e-mail addresses? Well, the answer is so obvious to any Internet marketer that the question would never even occur to them. Marketers want to increase the stickiness of their sites, as they call it, to keep the visitors coming back to their site instead of going to one of their many competitors who are only a click away. And as Jorian said, most of these companies are not making much money now, but they're hoping to make a pile of money in the future by building an asset that's

valuable.

The currency of those assets in today's IPO-crazed web world are page views, because they can sell advertising proportional to the number of page views, and registered users, because this indicates a relationship with a company that lasts longer than a few seconds.

So, all of the economic incentives for companies are to ask at every opportunity for an e-mail address or other personalized information, even if they don't need that identification for providing the service that they've proposed to the user.

Another reason they want an e-mail address is so that they can sell information associated with that e-mail address, possibly after the child exceeds the --

MS. LEVIN: Jason, I'm wondering if we can save that discussion about the costs and benefits when we go through -- and we will make sure that we get to that one.

MS. CATLETT: Okay. So, I'll just summarize in one sentence, then.

MS. LEVIN: Please, thank you.

MR. CATLETT: That it's in the economic interests of companies to gather as much data as they can using whatever pretext consumers might find

plausible and to provide abundant opportunities to provide services in anonymous and pseudonymous form.

MS. LEVIN: And we definitely would like to get information about that in the next phase.

Okay, yes, Jim?

MR. TEICHER: I just want to say, you know, there really is a balance that must be struck between anonymity and accountability, particularly when you're talking about children and parents online. The fact is it's been communications functions, a la chat and e-mail, that have historically driven the Internet and its predecessor from day one.

This is what -- what kids like to do. This is what they want to do. This is what people want to do, communicate online, and unless there's a degree of accountability that's established, particularly with children, there -- there won't be a responsible level of behavior that -- that is critical, that -- that parents need, that commercial websites need in order to have trust and confidence to grow, and that's really what we need to achieve here, and we can't discount the value of accountability.

MS. CATLETT: Sure, there is certainly an important place for accountability, but let's not grab identity in the name of accountability and then use it

for marketing purposes.

MS. LEVIN: Okay, let's go ahead now and I think we've got a list -- a working list, and it looks quite extensive, and we will try and, as they say in the online world, get more and more granular about all these mechanisms one at a time, but we have a couple of people who have asked to speak, and we will try and -- if you keep your comments short so we can go ahead and talk about the individual mechanisms.

Ron, you're first.

MR. PLESSER: Thank you, Leslie.

MS. HARRIS: Sure, Ron.

MS. LEVIN: Please identify yourselves.

MR. PLESSER: Ron Plesser representing Direct Marketing.

There should be a concept of e-mail plus where you can have e-mail but where questions can be asked and only the adult is likely to know, like who your ISP is, zip code and town affiliation. I think there's other questions that could be asked that could help verify it.

Again, this has to be seen in the context of the statute. Since the statute was mentioned twice today, I think it's very -- by Katharina and Mary Ellen, I think it's critical to read the statute and also to make

reference, Toby, to the exceptions that you have up on the wall.

The statute says, "The term 'verifiable parental consent' means any reasonable effort, taking into consideration available technology," so before we even get into talking about verifiable consent, it's any -- it's not just reasonable effort, it's any reasonable effort, and so I think industry has a responsibility and the FTC has a responsibility to look at reasonable efforts that can ensure notice and consent.

I'll also point out that in the exceptions themselves, I guess the second exception is an exception to verifiable consent to collect the e-mail address of the parent and the child. I wonder why that would be in the statute if not so that the parent and child could be contacted on e-mail.

I think any rational concept of legislative construction would -- would require the idea that e-mail would be seen, and I think the available technology sentence that -- quote that I gave just a moment ago indicates that this may change over time, and it may be that what works today won't work in five years or that there's a better solution in five years, and so that we should perhaps take what approach we need and put a sunset in.

And the final question on the sliding scale which was mentioned, I've had a lot of experience in individual cases as well as working with the Commission, and I think I could not agree any more with what Cassidy said this morning. The concern, I think the safety concern here, is the empowerment for kids to get free e-mail address or posting.

I think that's significantly different than a legitimate exchange of information with a site, and if we can separate those issues, if we can look at verifiable consent perhaps at a higher standard, the way Cassidy suggested, where there's posting or where there's an ability to communicate to third parties, and then look at a more flexible approach when we are dealing with collection and interchange and more of the one-on-one communication, I think that's the way we get out of this. And I just commend CARU and Cassidy for what I thought was a really brilliantly stated approach.

MS. LEVIN: Okay, Leslie and then Eric.

MS. HARRIS: Leslie Harris representing American Library Association.

Well, I want to associate myself with almost all of Ron Plesser's remarks. We always find ourselves sitting next to each other but not always in agreement,

but I wanted -- you know, we're talking a lot about what industry does versus parents, and I want to, you know, put on the table that language about reasonable efforts, et cetera.

Much of what was going on in the negotiations around this bill, and that's when we did identify that there was another interest at stake, and it's an interest of great importance to the American Library Association, and that's children's access to information in the context of the medium that we are functioning in, and that medium is fast and it's interactive.

So, what I would urge, you know, I mean the ALA's goal in that bill, which we achieved in part but certainly not in whole, was to try to keep that balance intact. I don't think we want to be in a situation of destroying the village in order to save it here.

And when I look at some of those approaches, you know, beyond e-mail in terms of online, we're moving again into, number one, situations that could be as violative of privacy as any possible collection of children's information, and also extremely burdensome in terms of time and parental response, and three, not one of them is going to deal with the parent who doesn't speak English, the parent without access to technology except through their children, in schools and libraries

and community centers.

And I think in the context of this conversation about verifiable consent, we have to go back to whether any of this is going to become a plus at the end of the day for those children, you know, whose parents are absolutely without their resources to respond to this or have the interest and inclination to do so.

MS. LEVIN: Eric?

MR. WENGER: I think we all would agree with what Leslie was saying about trying to balance competing concerns, on the one hand making this -- whatever mechanisms that are developed fast and easy for parents to use so that they are not overly burdensome and so that they don't hamper the development of electronic technology or the electronic marketplace, but at the same time we don't want to compromise what we think is an important goal, which is obtaining parental consent before children are interacted with -- online with marketers.

MS. HARRIS: Eric, can I just clarify something?

My concern is not with the development of the interactive marketplace. My concern is with children's access to information, and to me the -- you know, as I said, there is one balance, which is the marketers'

balance, you know, are developing the market. The balance I'm concerned about is children getting on this technology and finding that it is valuable and that their eyes are driven to kids sites, because those sites are accessible to them, not an increased burden.

MS. LEVIN: I think it's important just to mention that the focus of the discussion is on collection of information from children and not children's accessing a website, but --

MS. HARRIS: I understand that.

MS. LEVIN: Okay, Eric, continue, please.

MR. WENGER: But I think the reason that Leslie and Ron agreed with each other is because there's a common perspective there, which is increasing access to children to reach the -- these kinds of information without undue burdens is -- it shares the same goal as the business community has of developing the marketplace and not imposing undue hurdles on their ability to develop their businesses.

And I hope I didn't mischaracterize what Leslie was saying there, I didn't mean to do that, but I would like to come back to comments that were made by VeriSign and by CyberSmart!, and I think that they raise a very important point, which is that a lot of this technology is out there. It's just that there -- for some reason

there is a difficulty in developing momentum behind a particular technology.

And I think that that's one of the really important things about this Act and about these rules, is that hopefully they can set a baseline of governmental regulation that will set the goals, set the bar, and then, you know, a flexible method to allow industry and the marketplace to figure out how to meet those goals under the supervision of the Federal Trade Commission and the states who also will have a role in enforcing this Act, as well.

And I think that one of the things that we're all having trouble grappling with is in the absence of these mechanisms for verifying your identity online, we use substitute mechanisms, proxies, like credit card numbers or Social Security numbers, and the problem with using it is that information is the same. It's -- it's very much like a private key encryption system.

If I give you my credit card number or my Social Security number in order to verify who I am, now you have that information, and it can be used for other purposes beyond what it was originally intended for, and that's why it's so important for us to develop some mechanisms for authenticating who you are that doesn't give away your identity, at the same time prove who you

are.

And that's what's interesting about public key methods of encryption, where I have a password that verifies who I am, but I don't actually give that password to you. I type that password in and it creates a signature or a certificate or something that proves to you who I am and that I have authority to say what I say, and it doesn't compromise my ability to use that same password again with somebody else.

When we use credit card numbers or Social Security numbers to authenticate who we are, then that information ends up in databases, and who knows what happens to it? And that's what's kind of scary about it, about the use of credit cards.

MS. LEVIN: Okay, what I'd like to suggest is to try and keep the discussion focused on particular mechanisms and develop some context for each one sequentially, and I know several of you have asked to speak.

MR. WENGER: I'll just finish with saying that I'm not going to lay out what I think are -- or the states are not going to say what they think are the optimum technologies for doing this, but we hope that the result of this discussion will be that the marketplace will help develop some of these solutions

under the supervision of Federal Trade Commission and that this will help solve some of these problems.

MS. LEVIN: Well, let's explore the mechanisms one by one, and we'll start with the simple -- the first one we started off with, the click-back e-mail mechanism. If some of the sites here have experiences with that mechanism, we would be interested to hear how that has worked and any -- any comments on what the -- what the cost or benefits would be, simply a click-back e-mail. And if there is no proponent or comment on that, we will move on to the next one.

Yes, Eric or Paul?

MR. HERMAN: Yes, we have had some experience with that --

MS. LEVIN: Identify yourself, please.

MR. HERMAN: Sorry, Paul Herman from iCanBuy.

Essentially when a sign-up takes place at the iCanBuy site, you need to identify yourself as a parent or a kid. You need to self-select. And when that happens, of course, a little screen pops up and says, "Are you a parent, are you a kid?" And we are not trying to collect birth dates to verify that.

What happens is you -- as you go through the sign-up process is a fair amount of our sign-ups are abandoned once you get to the -- once you get to the

shopping cart.

Subsequently, a -- an e-mail goes out to say, Did you have a problem with the sign-up process, is there something wrong? It's a one-time e-mail that goes out, and you can click back from that e-mail back into the subscription procedure, and if you're a parent and you had a problem and you truly had a problem, you can get back there.

What we've also found is that a fair amount, you know, I don't have the exact number, but it's more like 10 percent have parents and kids share e-mails. So, if a kid starts to sign themselves up, goes back, gets an e-mail back, the kid can actually pick that up, so that the risk is -- for click-back e-mails is the uniqueness of that e-mail address to a particular kid, teen or parent.

MS. FISE: How do you know if it -- when you ask, are you a kid or a parent?

MS. LEVIN: Please identify yourself if you're asking questions.

MS. FISE: I'm sorry, Mary Ellen, just asking for a clarification.

You said that there's an initial question, are you a kid, are you a parent.

MR. HERMAN: Right, it says, "Click Here." It

says, "Teens or Kids, if you have a parent around, proceed to the sign-up. If you don't, fill in your parent's e-mail so we can ask them for their permission." So, it's a -- it's a self-selecting procedure.

MS. FISE: What if they select parent?

MR. HERMAN: And if you select parent, you go there -- you go through the sign-up process, and then to complete the sign-up process, you need a credit card, and since --

MS. FISE: So, it's really not click-back e-mail. It's e-mail plus credit card really to verify it. Is that --

MR. HERMAN: It's a process to get you back into a verifiable system.

MS. LEVIN: Okay, I think we would like to start off with simply a click-back e-mail consent. The consent is conveyed simply by clicking back with an e-mail.

Is there a comment on that specific point?

Eric? You've been waiting.

MR. ALEDORT: Yes, I would just like to describe very briefly the Disney practices, which were really developed --

MS. LEVIN: But let me just hold you off,

because that's not really a click-back e-mail, unless you are going to describe your previous -- it's what we call a confirmation e-mail. I'm trying to draw a line. A click-back e-mail is where there's a button that says "Submit your consent," that's it.

MR. ALEDORT: Well, the parent -- that's what the parent gets. The parent is asked to verify the account with -- by responding to the e-mail.

MS. LEVIN: But you have some additional features in addition to that. It's -- as I understand it, it's a confirmation back. Is that correct?

MR. ALEDORT: Well, the parent -- the parents must respond to the e-mail in order to activate the account. So, it is an opt-in, not an opt-out, but you don't -- the account is not a verified account until the parent has responded.

MS. LEVIN: Okay.

MR. ALEDORT: For me, they are very similar, and I just wanted to talk a little bit about our experience so far --

MS. LEVIN: Okay, sure, go ahead.

MR. ALEDORT: -- and why we think that's been very successful.

First of all, one of the important points is that on the Disney family of sites, the community

activities would consist of bulletin boards, which are monitored within an hour of posting; chat, which are auditorian chat, so everything is reviewed before it goes up; and contests, where if you were a winner, you would actually need to go -- to have another step to verify that you've won a car or a trip.

MS. LEVIN: What is that additional step?

MR. ALEDORT: That additional -- if you're a contest winner, we get a written affidavit, and we would support that -- the sliding scale where if you're doing something differently or you have to get the child's actual offline address, you would need to take extra steps to get that, and that's why we only ask for the bare minimum amount of information to establish an account and some kind of identity to Jim's theory that you do need some accountability.

What we found with our -- so, a child comes to our site, registers to be allowed to post a message on the Zoo bulletin board, and we ask for the parents' e-mail address. The child -- it is a self-selection process. The child must identify himself as a child, and in this world there is some level of trust that you have to begin with, and we've found that if a child is going to take the step of identifying themselves as a child, there is very little likelihood that they will

then try and circumvent that selection by responding to their parents' e-mail.

And the -- just to throw out some numbers for the group, we get about a 33 percent yes response rate from parents where they have responded within 14 days of receiving an e-mail that they want their child to have a validated account; a 33 -- a 30 percent, no, I do not want my child to have a validated account; and 37 percent who never respond.

So, we're very pleased with those numbers and we think that actually represents a true sampling of what's going on. Obviously at 37 percent no response, it's still very high, and, you know, we have concerns that even this method is leaving a lot of people with unvalidated accounts who never come back, because we have to remember, the kids are probably five steps ahead of their parents, and the idea of having a parent go through extra hoops to sign up for a public key or something like that I think will still prove very difficult in this day and age.

MR. MEDINE: David Medine from the Federal Trade Commission. Could I just follow up with a question?

You had said that 33 percent click back yes. I take it that you're inferring that because it's not a much higher number that the kids are not clicking back

themselves.

Do you have any evidence beyond that suspicion, any empirical evidence through subsequent kinds of acts with children or parents that would confirm that the vast majority of the 33 percent yeses are, in fact, parents clicking and not kids clicking back?

MR. ALEDORT: We have -- we have never had a parent come and send us an e-mail later saying, My child's account was incorrectly validated, please take them off. It's never happened in three years. So, that's why -- we don't have hard, empirical evidence that those yeses are parents versus kids, and I know, Toby, you were interested in the number of accounts that have both a parent e-mail address and a child's e-mail address that's the same, and we found that to be about 40 percent.

I think a lot of people don't like to set up multiple e-mail accounts for a household, and parents like to have control over all the e-mail coming into the house.

MR. HERMAN: And if I could just build on that --

MS. LEVIN: Please identify yourself.

MR. HERMAN: Oh, sorry, Paul Herman.

It's not as high as 40 percent of same e-mails,

but it's in the 10 to 20 percent range, and essentially in terms of the a third, a third, a third, we find that the permissions' point of view that about a third of the parental permission settings in terms of using your money are very tight, approve anything. A third are looser, use it however you'd like. A third are variably set in terms of -- in terms of permissions on the site.

MS. LEVIN: So, Paul, let me just go back. You said that you found that 10 to 20 percent of participants at your site, children and parents had the same address?

MR. HERMAN: That's correct.

MS. LEVIN: Now, I know there are some other people.

Yes, please, Leanna.

MS. LANDSMANN: Well, Leanna Landsmann, TIME for Kids.

In our filing we described a Nickelodeon experience where to participate in a contest a child would enter his or her first name and a parent's e-mail address. Nickelodeon would then send them -- an e-mail response to the parents indicating the child's desire to participate. The e-mail gave the parents a choice, et cetera.

Even the system was designed for opt-outs, 96

percent of the parents whose children wanted to participate decided to communicate with them and opted into the program, and, you know, we all took that as a really good sign, that parents appreciate the efficiency of e-mail and are actively doing things with their kids online. That's one example.

The Cartoon Network has had a recent experience where they offered both online e-mail-based opt-out and consent and offline, and I don't -- in my big pile of show and tell papers here, I don't have the data -- those percentages, but I can -- I can dig them out. One percentage is really easy. There were no offline submissions, and there were only online submissions, and that's very telling.

MS. LEVIN: If you could obtain that specific information and add it to the record, that would be helpful.

MS. LANDSMANN: Well, mark us down for zero percent on the offline. Also, I know you want to keep to this point. I would like to come back to Jason's point about anonymity, about which I feel very strongly, at some point before we close.

MS. LEVIN: Katharina, you had something.

MS. KOPP: Yes, Katharina Kopp, Center for Media Education. I just wanted to go back to the numbers we

presented this morning. We found that those sites had used e-mail consent with a few exceptions with regard to Disney, used it as an opt-out mechanism, that they basically collect information first and then send the information to -- an e-mail to the parent saying, you know, we just collected all this information, and if the parent doesn't approve of that, you know, they have to take another step to -- in order to stop this.

And so this is not in compliance with the legislation that clearly says it has to be a prior parental notification and consent. I just want to make that point, that the way it's used right now would not work under the statute.

MS. LEVIN: Okay, and continuing on the topic, Ron?

MR. PLESSER: Just a point of order. That certainly could fall within the exception in terms of the notice if the information is being collected as part of a multiple contact. So, I don't -- I don't know, Katharina, how you can say that that necessarily is illegal. It's very consistent with the exception.

MS. KOPP: If the notice would state, for example, that it was a subscription, but if it doesn't identify how that information will be used in the future, I don't think it would apply.

MR. PLESSER: I don't think you'd have to identify specifically subscription, but we can talk about that, and I don't --

MS. KOPP: That would be one of the exceptions.

MS. LEVIN: One at a time, please, because the --

MS. KOPP: Sorry, that would be one of the exceptions, the subscription, that you could subscribe and then notify the parents, say, By the way, your child has subscribed to the service.

MR. PLESSER: I don't think it's limited to subscriptions but multiple contacts.

MS. LEVIN: It's multiple contacts, and the two examples that we've referred to over and over are the contest and an online subscription, those two examples.

MR. PLESSER: That's an example.

MS. KOPP: It would have to be specified in the notice to the parent what the information is used for, and if that's not the case, then I don't think it would be in compliance.

MS. LEVIN: So, you're suggesting that if the notice doesn't describe the uses, then you can't tell whether it's in compliance.

Leanna, you came across some data and wanted to add --

MS. LANDSMANN: Yes. On this particular Cartoon Network contest, we got 71,552 consented entries online and none offline.

MS. LEVIN: Okay.

I'd like to see, then, if we can move to some of the mechanisms which are e-mail plus some accompanying screening information that was suggested as another mechanism. Is there anyone who has had experience with that, collecting any screening information in conjunction with the e-mail address?

Katharina? All right, we will start with Katharina and then Leanna.

MS. KOPP: Actually I just wanted to make the point, I think Ron was mentioning it earlier, the option of collecting also the zip code of the participant as a way to verify that it's a parent. We at the Center for Media Education have a problem with that. That's another way of collecting additional information of, you know, that is not necessary in the first place to get, you know, to increase sort of the data that companies can have.

MS. LEVIN: Okay.

Leanna, you wanted to go next?

MS. LANDSMANN: I -- will you permit me if I don't have an example of the screen information?

MS. LEVIN: Can you hold off then on your comment? I'll get back to you on the next round.

MS. LANDSMANN: Okay, promise?

MS. LEVIN: Yeah.

MS. HARRIS: I wanted to respond to Katharina. With all due respect, what you're suggesting is asking in an e-mail for additional information like the zip code somehow violates privacy, but to have to collect all of the parents' personal information in order to mail them a verifiable form does not, and I think it points out here that, you know, the question is, you know, are we going to, you know, in the search for the perfect ignore the good?

And the statute very clearly adopts a reasonable standard, and the -- and I -- you know, there will always be a child who will have the capacity to go around any one of these mechanisms, and it seems to me, whether it is a zip code or the mother's maiden name or, you know, anything that might be -- that you -- it's far less intrusive on the parent's privacy, you know, to do e-mail plus a question, it is far less burdensome on the kid's access to information, and from what we have heard from those who actually do this, the actual response rate is so substantially higher, it seems to be that, you know, that online sort of meets, you know, for sort

of balancing, you know, the interests of the kids, the interests of the parents, parents' privacy and marketers, that somehow to, you know, assume every online verification somehow is more intrusive is, you know, I must say is hard for me to understand.

MS. LEVIN: Let me suggest, too, that in terms of the screening information, there are several alternatives. One would be that the screening information is maintained in your database. Another is that you strip the information of whatever screening information you collect so it's not necessarily the fact that you would keep it.

Ron?

MR. PLESSER: And also I think the point is that we didn't suggest address, we said town and state and zip code, so that if it was in a small town, you would identify the zip code. It's unlikely that a 10-year-old or 9-year-old would know zip code, but if you did it in a metropolitan area like Washington, you would have a choice that you could verify.

The presence of the ISP, also most e-mail systems you can -- you can -- you can unload the track of how the e-mail came to you, kind of what the root map was. I don't think many 11-year-olds know who their ISP was. It may be the exception with AOL, but AOL is a

consent, as we heard before this morning, is more of a consent-based system, but there's a -- there does an 11-year-old know that PSInet or somebody like that is the ISP or Sprint? I think unlikely.

None of these questions are going to be foolproof, but they are -- they are reasonable efforts to ensure that they're getting parental consent.

The other thing that is just confusing to me is that the statute -- and I think the FTC has accepted it -- believes a child when the child says what age they are. So, if a child says that they are 14 or 13, the statute directs that that child is to be believed. So, if that's the case, I'm unsure why we think that 10 and 11-year-olds are going to be -- to ruse these sites and kind of not only lie about their age, which they may, but also to create essentially frauds against their parents, and I -- I just don't think that that's likely.

It's not consistent with Eric's experience at Disney. We have had no evidence of that whatsoever, and it seems that we're walking into this with the assumption that that's going to be the rule rather than the exception, and I think we have to challenge it. I think if -- if my 12-year-old was asked for the e-mail address of her father, I think she would give it, and it

would be -- it would be real and honest.

MS. LEVIN: Okay, thank you very much.

Dan?

MR. JAFFE: I just think that both Eric and Katharina have been trying to add something to the law. I mean, at least as far as I can see, there's nothing in the law that says anything about choosing methods on the basis of how much privacy information is contained within it. It says, "Any reasonable efforts to obtain verifiable consent," and then you have to look at whether, you know, it's reasonably calculated to actually reach a parent.

I think there's a danger on the other side of some of the company groups that say this is the best method. Again, if that was what the Congress was looking for, then they would have said that only the best method that had the highest probability would work. It says, "any reasonable effort." So, I think you have to -- and I think you -- that's important, because if you don't take that approach, you're going to force out all sorts of smaller companies and you're also going to have an effect on people who are not rich and who do not have access to faxes and to computers.

So, I think the Congress in this legislation, working with the FTC, working with all of the interested

groups, wanted to get a system that would provide a range of solutions that gave a reasonable likelihood of reaching a parent and that it was not trying to come up with one solution or picking one magic bullet, as I said earlier, and I do think, however, that a sliding scale may be -- go to the question of reasonability in that you may want to have more assurance in some circumstances than you may in others, and therefore an e-mail system alone may work where there is no outside sale or chat room situation where people have closer contact.

MS. LEVIN: It was helpful when Ron gave us some other examples of screening information. If others on the panel have specific ideas to add to that list, it would be very helpful.

Eric, you're next.

MR. ALEDORT: Yeah, we looked very seriously at adding to -- adding a question that would be verifiable, and we thought about, you know, the date of your first diptheria shot, things like that, which many parents wouldn't know, but the problem I think with e-mail plus is none of that information is verifiable. So, if I ask for the mother's maiden name and someone writes Smith, I have no way to find out if that's true or not. The same with a zip code or anything else.

So, I don't think you actually get more confidence from asking an extra question that you can't then find out if that is the correct answer.

MR. PLESSER: You can match zip code and a city. You can see if a zip code is in the range of --

MR. ALEDORT: But you don't want to ask --

MS. LEVIN: Excuse me, I think it's great if we have dialogue, but we have to make it a little more formal in terms of identifying yourself and we can have a dialogue.

Ron, did you want to respond to that?

MR. PLESSER: Ron Plesser.

I was just going to say I think the point on that is you would ask the city and the zip code with the concept that children would probably give you the wrong zip code, they would make it up or -- so, again, it's not a perfect thing, but it just is another indicator that if you said, you know, Washington, D.C., 20008, that you knew that that was at least within the range. If you said 10008, you knew somebody was making something up, and that could be easily verifiable.

MS. LEVIN: Excuse me, I am going to defer to Lee Peeler.

MR. PEELER: Actually, a very similar question for Eric. What if it was a phone number that came along

with the e-mail and -- and, you know, Disney checked, you know, every hundredth one to see if that came from a parent?

MR. ALEDORT: I mean, a phone number is a possibility. It kind of goes against the principle of, A, collecting the minimal amount of information you actually need, and B, a phone number is what we would define as offline contact information. So, it would make me nervous as a parent, why do I need to give you my phone number to let my kid enter a contest?

We really are open and are really trying to come up with something that is easily -- easy to verify, like a city and state, which you can run an algorithm to check on that and see if that's correct or hook up with the Post Office, or a phone number, but I'm just nervous about asking for more than you need.

MS. LEVIN: I think it would be important that whatever mechanisms you use you explain them clearly to parents and why you're using them, so in that context they may be more receptive.

Okay, trying to follow up, Eric Wenger?

MR. WENGER: This is a little confusing to me, I'm not used to having other Erics, and every time somebody says that Eric had a point or something, I'm not sure if they are talking about me, but in any case,

I wanted to come back to what Eric said, which was when he was asked about using screening questions, he said that you don't necessarily get more certainty and you sometimes do create privacy concerns, and that's really the point I was trying to make.

And for some reason I think you said that I was calling for a magic bullet or a particular type of technology, and I think if we look back at the transcript about what I said, each time I mentioned that it was important, that the approach that the Commission took, which was to encourage flexibility and to set only a baseline of standards and then allow the marketplace to develop the particular solutions.

And I talked about digital signatures as being one approach that might do that in a way that would alleviate some of the privacy concerns that I could see coming up when we start to use personal information, like Social Security numbers and credit card numbers, to identify somebody and to prove that they have the authority to give permission on behalf of a child.

But in no way did I mean to suggest that -- that some -- one of those mechanisms is -- is the only way to go or that there's -- that there's a very limited universe of solutions that may be available to us to approach some of these problems. My only point is if we

are going to develop these mechanisms and if the Commission is going to encourage them through these rules, which is I think what this proposed rule does, that we should be keeping in mind other concerns like privacy at the same time.

MS. LEVIN: Okay.

Sheila?

MS. MILLAR: Sheila Millar for Mars Incorporated.

I just wanted to follow up on a couple of points and maybe reach back in the FTC's own history for a little bit of an analogy. We're talking about any reasonable efforts here, and I think a number of years ago when the FTC did its hearings on standards and certification bodies, you came out with a lengthy report that talked about the desirability of performance standards in general terms as opposed to very specific hard and fast rules.

And I actually think that there's a great commonality of interest between the Commission staff, representatives of the business community and the privacy advocates around this table for that principle.

The statute already provides the performance standard, and so perhaps one of the tasks here is to question whether some of these methods are inherently

unreasonable or whether some mechanisms are somewhat more reasonable than others, taking into consideration I think another point that we all agree on that is also driven by the statute, that you have certain areas of information collection which are not deemed to be particularly problematic and others which are.

And I think perhaps if we focus our discussion on the continuum and whether or not there are any of these aspects that are inherently unreasonable, we might spend it a little more profitably.

MS. LEVIN: Okay.

Mary Ellen Fise?

MS. FISE: I just wanted to respond to a couple of things. First off, this Eric said, you know, we haven't received any complaints about this, and just the fact that parents haven't complained about it, I don't think that we can take as a significant piece of evidence right now in terms of where we are. People may not know or understand this whole privacy issue. They may not know how to complain or they don't have time to complain.

And I think that's true across a broad spectrum of consumer issues, and so I hate to kind of rely on the fact that some existing practices have been okay just because we haven't been hearing about some complaints.

Also, I think we have to remember that this rule goes to commercial purposes, websites for commercial purposes, and companies do an excellent job at marketing to children and enticing them, and 2-year-olds know what Happy Meals are, and where we are right now in time is very different from where we're going to be five years and ten years down the road.

And, you know, while I don't want to put forward any notion of impugning the veracity of children, the marketing that is done to children in broadcast media and what is happening online and probably will expand and grow online is very, very enticing, and so I think we need to keep that in mind in terms of are we going to be doing things that is going to lead to what I would call impulsive false consent by a child because of the vast appeal.

These are commercial marketers, and the reason they're appealing to kids is for reasons of making money, and I think we need to keep that in mind as we look at these kinds of solutions and what is going to be verifiable and what isn't. I don't think that we have seen the worst that can come yet.

MS. LEVIN: Okay.

David Medine?

MR. MEDINE: Thanks, I want to follow up on that

Sheila's comment over there about setting performance standards, for that's the approach that the Commission has taken not only in the proceeding you mentioned but also in many of our orders, not dictating how companies comply with the orders but telling them where they have to be at the end of the day.

My question is to the panel, I guess, does anyone have any views on what those performance standards ought to be? Is there any way to elaborate beyond what the statute says in terms of how to assess whether a particular mechanism meets a performance standard?

MS. LEVIN: And I might throw in, the question I think the way it was framed is perhaps what wouldn't fit the performance standards as opposed to what might fit?

Okay, Jason.

MS. CATLETT: Jason Catlett from Junkbusters.

I'd like to propose a specific performance standard or at least a framework for a performance standard. If you look at the process of determining whether parental consent was obtained as a test, like a test for having Lyme disease, there's a mathematical framework for that that's well known. You look at false positives and false negatives. Does it say you have got Lyme disease when you don't? Does it say you don't have

Lyme disease when you really do?

Now, what does that mean in this case? What is a false positive and what is a false negative here? Well, I think it means a false positive is when the kid gets away with pretending they're a parent, or the company says, Yeah, we got consent, but no consent was really there. A false negative then was it really was a kid, and the parent would have consented to the use but was prevented by some circumstance for doing it.

For example, if a fax was required, the parent didn't have a fax machine, or if a credit card was required, then a parent didn't have a credit card. So, if we formulate our view of what is a false positive here and what is a false negative, how do we balance these two failures? And then we have to decide on a simple ratio, which is to say how many false positives we will allow or false negative?

And, you know, in the judicial system, we are used to saying, Well, we are willing to let nine criminals off free for -- for the price of convicting one man unjustly. So, I propose that we decide what is a false positive, what is a false negative and what is the acceptable ratio between those two.

MS. LEVIN: Okay.

Leslie?

MS. HARRIS: Well, I certainly listen to that worry about what we would have to collect in order to determine that, but let me just suggest looking at it another way, and that is over time you're going to be able to tell sites, you know, let's just assume for the sake of discussion we have e-mail and we have a flexible approach with a range of possibilities.

I think one thing you have to look at over time is whether the verification method is driving kids' eyes away from the site, assuming the site is -- has information that kids want to see, that their parents think they should see, et cetera, et cetera. I mean, that -- it's just as important and reasonable -- I mean, I am going to keep factoring in that reasonableness has also to do with kids' interests, not just with parents and companies, that if over time a particular method produces a significant drop-off in kids going to that site, then we have somehow -- then we are out of balance. We have created something that is a burden and a hurdle to the kids as well as to the parents. So, I would urge that the Commission over a period of time be looking at those factors, as well.

MS. LEVIN: Okay.

Leanna?

MS. LANDSMANN: Thank you, Toby.

This is not about screening. This is about two comments that I've heard. One is, Jason, your comment about anonymity was better than a double espresso at Starbucks for my system, and Mary Ellen, yours about the assumption that all for-profit companies that are interested in this issue are going to collect data and sell it for purposes that you disagree with, I think we have to --

MS. FISE: I didn't say that, just so the record is clear, thank you.

MS. LANDSMANN: Well, what did you say? State it again, because that's what I -- that was my summary of what you wrote. I mean, you said that this is for -- that for-profit companies are going to -- they may not be making money now, but the purpose is to create commerce so that they can sell to kids, you know --

MR. WENGER: She said make a pile of money.

MS. LANDSMANN: Pardon?

MS. LEVIN: I think it probably would be best if we just continued.

MS. CATLETT: Yes, the record will be solidified with all of those comments.

MS. LANDSMANN: I think that there's a bigger picture here, and there's -- parents have concerns about privacy about the Internet, but they also have other

concerns about the Internet, and anonymity is one of them. It is not good for us to consider a system that is, as eloquent as Jason's ode to anonymity is, it is not good to consider a system where we're encouraging kids to be somebody else.

And I think, you know, teachers mentioned this when we talked to them last week, parents mentioned this when we talked to them last week, and I think it's ironic that, you know, TIME for Kids on its Letters to the Editor page in print, you can see "Toby Levin, Washington, D.C." We don't do that online. It says, "Toby, Washington, D.C." It's not good for kids not to own -- not to own their ideas.

I think if you look at this from a pedagogical standpoint, we have to make an assumption that -- we're in the midst of a school reform movement in this country, and there are some central tenets in that school reform movement, and whatever we do probably ought to take these things into consideration and somewhat align with them.

One tenet is it's really important not to make a monster out of the Internet and to have kids learn to use it with power and purpose. I mean, if you look at the data from the Department of Ed, I think three years ago 36 percent of classrooms were hooked into the

Internet, now that's 96 percent and we're looking at a hundred percent in mid-2000. We're spending a lot of time, effort, curriculum reform to ensure that teachers and parents can help kids use this incredibly potent medium for something more than surfing or entering contests. That's number one.

Number two, the whole literacy instruction in this country is founded on two principles. One is that kids read and write for authentic purposes, and when they -- when they do that, they are more motivated to read and write than if they make something up. So, one of the things that we as educators and educational publishers -- and I'm putting TIME for Kids in this group -- and textbook publishers aren't represented here, they are commercial folks who want to encourage a high degree of interactivity in this community of learners going forward, they're kind of unaware of this -- of COPPA and what it means for them in the next 18 months.

We want to do something that will not constrain the very things that we are trying to do in classrooms, which is to get kids to read, respond, share, you know, all of the research says that kids read more powerfully if you ask them, What did you think about that when you read it? Would you like to tell somebody else about

that?

I mean, I'm paraphrasing the research obviously, but teachers know that, and one of the very important things that we see that the Internet provides us are ways to share this, and we don't want kids to be anonymous when they're sharing their ideas.

MS. LEVIN: Leanna, let's be sure, you're saying that in terms of the way the site has worked in the past, you would have "Toby, Washington, D.C.," and that conveys that sense of participation to the child?

MS. LANDSMANN: Yeah, but you know, I'm in publishing now because I got a Letter to the Editor published in my local newspaper when I was in the fourth grade, and it had my first and last name and my grade number and my town, and that was a very big deal for me, and I worry as an educator about -- you know, I guess Linda Roberts calls it making the Internet a monster.

I also -- you know, we have to find ways -- Kathryn this morning referred to -- and there was an eloquent phrase called "the new media culture," and that's true. We have to find ways to equip kids with armor to -- to function within this new media culture, and I -- you know, I brought something down that I'm sure you all will be interested to find out.

There's a phonics book now called The Internet,

A Kids' Handbook, it's a phonics reader, and it's all about the Internet, and it has rules in it. Well, this -- I brought this because it's an example of how everyone is coming around to support the positive -- kids' positive growth and development in this culture, and, you know, as I said, I'm not a lawyer, I'm not a technology specialist, I am an educator, and I think that we need to keep these things in mind.

So, when I hear support for anonymity, you know, I just -- that's -- we're going in completely the wrong direction.

MS. LEVIN: I think it might be helpful if there was some data as to whether the children care that it's their whole name or whether it's sufficient that they have their first name. Do you have some evidence of that that you could supply for the record that would help?

MS. LANDSMANN: It's anecdotal, we didn't go out and survey them, but they like to own their ideas.

MS. LEVIN: And that means their whole name has to be displayed publicly, you think, as opposed to their first name?

MS. LANDSMANN: We -- we have this discussion with kids, we have it over the phone so that we get verifiable parental consent. We know that they -- that

they would rather see their full name on it, and they understand why, they understand why we're cautious.

MS. LEVIN: And how do you go about getting the consent to use the full name now? Could you just --

MS. LANDSMANN: We call them. We -- for the -- when --

MS. LEVIN: You call who?

MS. LANDSMANN: We call -- well, when we get a -- an e-mail or a paper letter, we make a decision, is this something that's going to go in the Letters to the Editor, either in the print version or online, and when we make that selection, we call the kid and the parent to get their permission to print this, because that's just basic -- I mean, it's not just a privacy issue. It's a basic fact-checking issue.

MS. LEVIN: And how do you get the telephone number from the family?

MS. LANDSMANN: Well, if it's on -- if it's on a piece of paper, you can track them down. If it's on an e-mail, we e-mail them back and say, Please send us your phone number so we can verify this comes from your child and we can publish this letter.

MS. LEVIN: Great. I appreciate that information.

Eric?

MR. ALEDORT: I just wanted to respond -- Eric Aledort.

I just wanted to respond to Mary's concern, and I think it's a very real concern, that people really view commercial websites as out there to collect information solely to market to their children, and I think that's why we strongly support a higher threshold if you are going to be an AOL where you're giving your partners the data or if you're going to market directly to the children yourself or if you're going to sell your list.

We think that it is absolutely essential that you get more verifiable parental consent, and I would also just like to say that we do believe that because we haven't gotten complaints, people like to complain to Disney, it's very easy for them to track us down, I get complaints about all kinds of things, that it actually is, although somewhat anecdotal, a fairly telling sign that in three years we haven't had a complaint about this.

MS. LEVIN: Okay, Paul, and then I am going to try to wrap up so we can break for lunch.

MR. HERMAN: Great, I just wanted to answer the question about metrics or possible performance measures, some frameworks that might be helpful before getting

into specific ones. The Baldridge Award in terms of business evaluating quality, the -- the government was able to set out both criteria and suggested processes or check boxes in order to compete, and so a similar privacy and consent score card that businesses can use for themselves in order to meet those criteria and meet those processes would be a way to help evaluate that, and someone like a Gomez Advisers that does that for financial sites and now for commerce sites through their Gomez.com or Gomezadvisers.com helps you figure out who ranks better on what criteria. So, that would be a process and a framework.

Metrics, just off the top of my head, would be a percentage of customers verified, which sounds like it would be close to 100 percent if not 100 percent; some sort of sampling of existing customers, as either a suggested or required process, with the requisite statistical analysis behind that so that you talked to at least 30 people, depending on your sample size.

And there would be other privacy and consent measures that would be both quantifiable as well as qualitative that could be -- that could be held to, and I think what you're hearing is some feedback to say everyone's willing to be held accountable to results. We would prefer some flexibility in terms of methods,

because we each have unique businesses, and technologies will change over time.

So, there are some processes that we'll probably have to go through, but being able to adapt those over time, especially given the speed of the Internet and the time availability of both parents and kids and teens, parents are very time-constrained, many have dual-income households or single households working, so the power of the Internet is we might be able to access them at work through a browser or their Palm Pilot, but again, there's a time constraint. And so the -- balancing the impulse against the benefit of the Internet would be extremely helpful.

MS. LEVIN: Okay, one last comment, Jim, and then I'll wrap up.

MR. TEICHER: Sure. I mean, look, the issue being how do you know a kid's a kid in cyberspace? How do you know a parent's a parent? Key to this is the kids have to buy into all of these processes, given children's level of technical sophistication, and you know, we all wanted to join clubs and be part of clubs and didn't want the parents to participate when we were kids.

Kids like to be identified as kids grouped with other kids, and I think methods of authentication that

can totally respect privacy, where kids can get to buy in, where kids can get more out of the Internet and all that it offers, by virtue of buying into these processes is really what it's about, and I think that we need to involve kids in the process and make it appealing to them, as well.

MS. LEVIN: Okay. This is a good breaking point. We are going to resume with this panel at 1:45 promptly, and at that point I hope we'll turn to some of the other mechanisms that we have not yet addressed, but before you break, on behalf of the privacy team, I did want to thank my colleagues and the staff, because I know some of you won't be here later in the day at the tail end.

I did want to thank the hard work of Jill Samuels and Abbe Goldstein, who worked diligently to help the workshop proceed as smoothly as it has, and also my colleagues Jessica Rich, Loren Thompson and Martha Landesburg, who have been working on the privacy -- the COPPA rulemaking with me, and we very much appreciate the group effort involved. And we'll look forward then to seeing you at 1:45.

(Applause.)

(Whereupon, at 12:30 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(1:45 p.m.)

- - - - -

SESSION II (cont.)

- - - - -

MS. LEVIN: If everyone will please take their seats, we'll get started.

If everyone could please take their seats.

If everyone could please be seated. You're more unruly than my classes used to be. We need to get going, folks.

First, a request regarding written handouts. If you have any written material that you wanted to be included, panelists, in the record of the -- for the workshop today, please make sure that the court reporter receives it, and all of that material we will try to make publicly available through our website.

MR. PLESSER: Can I ask a question about that? Will the record remain open for a period of time?

MS. LEVIN: Yes, the record on the workshop will be open until July the 30th.

MR. PLESSER: Because I know once we get the CME, there will be some interesting responses if we can see the questions and comments.

MS. LEVIN: Okay, I'm not 100 percent confident

that we will be able to get this on the web in time for the -- the transcript back and on the web before July 30th, so we'll work with -- try to figure out a way to make sure you get the material.

I'd like to start off this portion of the session just to be sure that we haven't omitted any important examples. Before we move on to digital signatures, without anyone repeating themselves, please, is there any other e-mail plus option that we did not put on the table?

For example, use of a delayed e-mail was one that some of the commenters had made, but I just want to be sure if there's anyone else on the panel who had an implement -- an example of how e-mail plus could be done that we put it on the table before we move on to digital signatures.

MR. PLESSER: Well, use of delayed e-mail I hope would be included in there.

MS. LEVIN: Okay, Ron Plesser.

Is there any other example of how the e-mail could be augmented that we did not mention?

MS. LANDSMANN: I don't have an example of --

MS. LEVIN: Again, please identify yourself.

MS. LANDSMANN: I'm sorry, Leanna Landsmann, TIME for Kids, other than the ones I mentioned this

morning, but I would be interested in if there is any evidence or examples of how click-back e-mail has not worked. We had some examples this morning of how they have worked; if we could have some examples of how they have not worked.

MS. LEVIN: Okay, that goes back to whether there's any data on falsification or any other indication about click-back alone without anything else on the site. Is there any other information to put on the record at this point?

(No response.)

MS. LEVIN: All right, let's go ahead and move on then to looking at digital signatures, and I -- as well another service that has come on the market, iCanBuy. Paul, if you could tell us a bit about your product and how that's working.

MR. HERMAN: Great, thanks, Toby, and I guess we've got the special slot here of not only before lunch but after lunch, so we will keep it lively.

ICanBuy is essentially a service that has existed and basically pioneered a new industry of kids -- kid-enabled commerce back in March that's a safe, secure and private system that enables kids and teens with their parents' permission to do electronic commerce and do electronic finance.

What does that mean? Is that parents can authorize specific places and amounts to spend at destinations where you can shop, you can bank, you can donate to charity, and ultimately you can invest, as well.

The concept around this that we developed in reading the FTC materials was essentially to build in parental permissions, not only to collect information, like bill-to and ship-to and financial payment methods, but essentially to build in parental choice, and parents get to choose how -- what permissions they would like to set on the kids and teens.

So, the -- the criteria that we've used is we only collect personal information from parents which meets the -- which meets the guidelines. We have also been validated with the TRUSTe kids seal, which is a higher -- a higher criteria to meet in terms of privacy and disclosure and in process with the bbb.online seal, and there are restrictions on the private information which we collect.

In other words, our partners cannot use the privacy information to use outbound spamming or e-mail for marketing purposes. They can use it for fulfillment purposes, to fulfill physical or digital goods. They can use it for customer service related to that order.

They cannot use it for outbound marketing. And we believe -- again, we're taking a stand and have had some stand-offs with some merchants who wanted to break that policy, and we were prepared to walk, and they backed down.

So, the process and the mechanics behind that are when the parents come to a site to sign up for iCanBuy, it's a three-step process. The first step is some basic demographic information, name, address, phone number, e-mail and a unique alphanumeric password. Because we are dealing with financial funds, it's an alphanumeric password similar to what you would find on your online bank or trading house.

The second step is to set all the permissions for each individual child, and they can be set individually whether you're a youngster, a kid, a preteen on the verge or a teen, and those permissions relate to how much money you can receive, where you can use it and what the permissions are in terms of a tight leash or a loose leash and what the parents are enabling them to do.

What we've found in the permissions is about a third had very tight permissions; parents require a transaction be approved on every -- on every interaction. A third have been loose; they enable the

kids to use all the money in their debit account, it is a cash account. And the third has been variable. And what we found is for the teens, the variable is set at about $50 as to what teens can do with their money, and for kids it's $10 to $20.

So, again, this permissions-based wallet or permissions-based passport is a method, as they go to different destinations, to restrict how they conduct business online. So, that's the second piece.

And then the third piece, how we validate all of this and where we find that there's drop-offs in the sign-up procedure is a credit card or debit card or trusted financial account, and that's what we're using to say credit cards and debit cards typically don't issue to anyone under 18, and in the 9 percent of teens and kids who do, they are related to a parent account who is responsible for those finances.

So, that is our means of validating that we have some 16 and 17-year-olds who have signed their selves up, but again, they have their own credit cards with their parents' permission. If there are cases of kids signing themselves up, they usually drop out at the place. So, that's the automatic procedure that's built in.

We built that logic into it based on the FTC's

work last summer, and as the proposed rule has been going forward, we are building in the proposed rule into our business today. So, we are prepared, and that's why our comment was that the current proposed rule is implementable, because these are all easy technological changes to design into your business from a technology point of view. In addition -- so, that covers 80 to 90 percent of the work that we do.

From a human point of view, we have human-related monitoring and checks. So, first of all, if your credit card doesn't pass, you put in a wrong number or you put in a high amount, it doesn't pass automatically. Then if someone does put in, say, $400 into their account, we actually pick up the phone, call the parent, call the kid, and verify and validate -- the kid usually picks up the phone and we ask to talk with the parent, and we verify with the parent on a voice-to-voice basis.

That is both a cost of doing business, but it's also an opportunity to establish a personal relationship with the customer and deliver some customer satisfaction. And so as we talk about offline methods of talking with customers, we believe that's an opportunity for business, not only a cost for business.

In addition, we -- and we do random checks, as

well. So, every 10 or 20, we pick up the phone and we call to validate and make sure that our methods are straight. So, we haven't had any cases where they've -- people have spoofed the system yet, but I'm sure once we get to the size of an AOL, we will have cases like that and we will have to work around that.

That's a broad overview of the system. There are parental e-mails that get sent to the parents to validate and verify. ICanBuy does customer newsletters. So, on a weekly basis, we communicate with our customers, but again, since the parent has authorized the entire account, we view that as fitting within the guidelines that we're pursuing here.

MS. LEVIN: Okay, thank you very much.

Jim Teicher with CyberSmart!.

MR. TEICHER: Sure. CyberSmart! is a tool that will authenticate children, parents and schools in the online world. CyberSmart! is not a filter, it is not a safe area or an online space that children are confined in, but rather it is a communications enabler.

Again, what children want to do and will want to do more of is communicate between themselves and with others, between websites and themselves, chat, message. We think that enabling communication and assuring privacy while enabling websites to offer and children to

receive information that is -- that they care about while assuring privacy is critical. So, our product addresses that.

We do really two -- sorry, three things. We identify through a process utilizing digital signature technology. Weber e-mail is also part of the process. We have a registration process for parents that involves a feedback loop to assure that when a child is issued the certificate, they are truly a child. What this will enable is safer chat areas. It will also enable when a child visits a website to receive content that they carry about without revealing their identity.

Now, so far as the state of the technology and what we're using and where we think it's at, because I think this is really important vis-a-vis digital certificates and e-mail, you know, we looked at this very carefully, and I think that the biggest -- the biggest need in order for digital certificates to be able to work so far as our concern is the -- the availability of really good front ends that -- to that technology, which are easy to use and which parents and kids can relate to in a way that they find interesting and valuable.

I think the technology is here today and almost over the next few months really full of the kind of

functionality necessary to facilitate the use of digital certificates. I don't mean that it's ready for the marketplace today. I mean that it's going to still be some time, because our product really won't be making its commercial debut until into next year.

It's going to be some time until I think it -- it's totally ready for prime time, but I don't see that time frame as so far out, and I think it's really a -- really very viable.

MS. LEVIN: Okay. Could you just tell us a little bit more about how your service would work with, let's say, your partner -- Disney next door here or Time Warner over here or Jorian Clarke in her small KidsCom site?

MR. TEICHER: Well, without going into the sign-up process, you can make the leap of faith that there really is a digital certificate on a computer and that the user is a child. What would happen is, for example, let's say the child went to a site because he or she wanted to chat, and in essence the child would be carded, like someone, you know, going into any kind of environment where they would have proof of their age.

The site would be able to, with no development on their part really, identify, read the certificate and say, Yes, you know, this is an authenticated child, they

can get into this chat area with other authenticated children; or no, they don't -- or no, they are not, they can't get in; or it might be a case where the child goes to a site that doesn't want children, and they don't have to say, Well, go through the -- you know, if you're under 18, click here, but rather, they're just bumped.

So, you know, I think the application really varies. It -- since the certificate doesn't identify the child at all in terms of who they are, this also gives the site an opportunity, you know, to be able to interact in terms of registering -- possibly automatically registering the child or supplying content to the child.

MS. LEVIN: And you would envision, then, that it's -- your service, then, is to provide the place where the parent would come to establish the certificate for their child.

MR. TEICHER: It's the registration of the child, it's the authentication of the child, and also, on the part of the website, it's the reading of the certificate and using it.

MS. LEVIN: Okay, David?

MR. MEDINE: Okay, yeah, just to follow up, something we have gotten out from prior workshops about the strength of digital signatures and how secure -- I

guess what they say is what they say. I guess the question is, what is this digital signature saying in this context, or put another way, who's the certifying authority who's going to say, This certificate was issued to a child?

In other words, once that happens, and clearly the digital signature may be a good way of passing along that authority from the parent, this is a child, and you can collect that child's information, how does the digital certificate issuer know that, in fact, they're dealing with a child?

MR. TEICHER: Well, there are two ways, and again, it has to do with the level of security we need, just as we're talking about the various permission levels here, as well.

We are involving a feedback loop with schools in the process. We believe that we've created a mechanism that will take care of that. I'm not going -- revealing all the details of the feedback process right now today, but I can assure you that the feedback process involving -- between parents and schools and children will create, you know, the kind of security that is critical here.

MR. MEDINE: I guess the next question is are there any other panelists who think that digital

signatures are one of the many ways that we can go, offer some assurance that they do, in fact, provide verifiable parental consent because, in fact, it's the parent that's been involved in the issuance of the certificate?

MR. BRANDT: Well, I guess I could add to that what Jim's describing is not --

MS. LEVIN: Please identify yourself for the record.

MR. BRANDT: I'm sorry, Jim Brandt from VeriSign.

We are a technology provider, that is, of digital certificates and PKI. What we find is that we have the capability of issuing these certificates, but often times, as Jim describes, you need to have a front-end registration process that better tunes the particular market or vertical market that will use that certificate.

Albeit, we would all like to get to this Utopia where a single certificate might be used for every single application. I think that will be a fair number of years before we reach that point.

In the context of this particular use of a certificate, though, certainly the technology is there, and as you've indicated, you've had testimony to verify

the technology is there. What we're finding is that some entrepreneurs, some smart folks with the right partners are coming together to say, How can I tune that in a working relationship to provide this technology in the context of providing mechanism for kids and parents to provide this kind of authenticated feedback?

And so there are a number of ways that that can be done, none of it rocket science. I could indicate that over the past couple years we've worked with a number of vertical industries, whether it would be the credit card industry, for example, with MasterCard and Visa, who have their own particular rules on what they want to do; whether it would be the Automotive Network Exchange, ANX, where they have a community of automobile manufacturers and particular data that they would want to authenticate themselves, so they have a front-end process for handling that information.

So, it's really how do I take this -- the people that best know that information of the intended recipient or use of that certificate and provide a front end to that in a way that tunes the process to the application? So, I would agree with Jim that there's no inhibiting capability today to move forward.

MR. TEICHER: And equally important to making sure that you have an authentication process that works

is having an authentication process that kids want and that kids like and making sure they're part of the process. I mean, I think one of the major aspects of CyberSmart! is that we think that, you know, empowering children to be safe online and getting the most out of their Internet experience is something that we can structure in a way that they like and that they want and that they don't feel locked up and that enhances their experience online.

And that's really critical, you know, because with all of the talk about parental involvement, you know, the fact is that a lot of families are lucky if they have one parent. A lot of families don't have two parents at home in the evening. A lot of kids know a lot more than their parents.

You know, we have to develop processes that the bulk of children in the United States can embrace in order for any of this to work, and that's really at the foundation of our business.

MS. LEVIN: Okay, Eric Wenger?

MR. WENGER: I just had a question for Jim about the certificates. If a parent registers and a certificate is created, it's created on a particular computer, and then does that create a setup for multiple users can have that computer and have different access,

and can the child go to another computer and be able to use their account, or does the certificate have to be loaded on that machine, as well? Just some logistical questions.

MR. TEICHER: Regarding the portability question, in general, which is really critical, because we know that children use multiple computers and can't be tied to one computer only, the answer is yes to all your questions, and that's largely because technology is evolving in such a way that will permit remote access and authentication.

You know, we all have been fixated on smart cards and that you have to hold the physical device and that these devices are expensive, and the cost in order for this to work has to be really, really low. So, that portability issue I believe is virtually solved and definitely into next year will be solved.

MS. LEVIN: Let me just follow up on the timing question. We've received comments from some who are suggesting that the Commission give website operators a five-year sunset extension on using perhaps less rigorous mechanisms to permit time for the new technologies to be developed. What is your view -- I'll start with you, Jim, and then the other Jim -- with regard to the time frame? Is five years what's needed?

MR. TEICHER: I think that if we look at the Internet five years ago and we couldn't possibly imagine what it would be today, and therefore, we can't possibly imagine what this technology will evolve to in five years. So, I think that's a bit broad given the pace of change, and we can all I think logically assume it will be faster than it was over the past five years.

However, it's important to realize that we do need a period of time to implement tasks and refine these technologies and these processes where we can't reasonably require them to be implemented globally for some time. Therefore, I suggest that we have -- that we look at -- revisit this in perhaps 18 months, because even in 18 months, that will give significant change -- give time for a significant change in advancements to have occurred.

MS. LEVIN: Okay.

And Jim Brandt?

MR. BRANDT: No, I would agree with that, that clearly the technology can be applied today. I really believe it's a matter of taking the basic technical capabilities and technology and to feel comfortable with that with all the constituents; that is, the websites that will be applying it, making decisions based on that, electronic authentication, the users, the

children, the parents, to understand -- government, to understand a comfort feel on that.

So, I really believe a gentleman's comment earlier that -- on the first panel that addressed this issue of making sure that we don't preclude the technologies but also move forward in sufficient testing phases to feel comfortable with and to touch all of the aspects of a systemic aspect of this system, and this is a system, and each -- and all aspects of this system have to be tested.

PKI and a certificate is just one piece of this very important system, and it needs to be engineered and evolve in the context of its utility. So, I would certainly say five years is much too long of a time frame to expect widespread deployment. Perhaps six months is too soon, but -- but maybe a year, 18 months, I would say that would be sufficient time to provide sufficient testing and feedback and comfort that the real use of the system will be adopted by the constituents.

MS. LEVIN: One follow-up on that. Are there any stumbling blocks that perhaps we are not aware of that may, you know, affect that timing?

MR. BRANDT: Stumbling blocks?

MS. LEVIN: In terms of, you know, incentives or

lack of incentives or if technology is not the problem, what's the stumbling block?

MR. BRANDT: Well, I guess a number of panels, a number of fora could address this kind of a question, but the question really is why isn't this technology more ubiquitous, why isn't everybody running around with a certificate today in their wallet, for example, and it's not the case that -- if you look at a system, a PKI-based system, you need an infrastructure to provide that certificate, you need applications that use that certificate, like an e-mail or a web browser. You need -- and you need a program or a rationale for using that security mechanism in the context of its -- that its intended purpose.

So, what we're finding is that the technology has been around, it has been deployed significantly within, for example, pieces of the Department of Defense for classified applications, and we're finding that because people need and want to use the Internet, for security and privacy and authentication, to do business in electronic commerce using that medium, it's now becoming a forcing function to use this technology in a more commercial orientation.

And so as that paradigm evolves, as electronic commerce evolves, as these applications evolve, as

perceived legal barriers or perceptions are reduced, that is, people feeling that maybe if I go in this kind of a technology, there will not be sufficient nets there that will save me or that will be sufficient questions or the technology isn't good enough, et cetera.

I think it's a matter of time. I think it's a matter of adoption and applications, and I think it's ensuring that the government -- personally, the government will provide sufficient credibility and support for the technology for its intended applications.

For example, the past Congress passed a GPEA guideline, the Government Paperwork Elimination Act, that in there calls for -- among the use of other technologies, is digital signature for end consumers or end citizens to deal with the government electronically and will require in the next several years each federal agency who deals with the public today to be able to give the public an option to transact with the public in an electronic means that provides for security and authentication. So, those kind of enablers, those kind of enablers are also important to the whole process.

MS. LEVIN: Okay, Ron Plesser.

MR. PLESSER: I'm glad you brought the timing issue up and, you know, I want to be very, very

supportive of the two Jims and Paul Herman and the people that I think are going to be on the next panel, the development of technology is going to be of great assistance here, but we are looking at a -- kind of a regulatory -- you know, a statutory implementation dated April 2000, if I count right, and even on the most optimistic predictions, this kind of technology is not going to be there for April 2000.

Whether or not the implementation is five years or another period, I don't think there's a magic in the number. I think, again, it forces us to look back at the statute that talks about available, realistic, reasonable, in the light of available technology. The Internet has been the scene of a lot of technology that's come on very quickly, but it's also been the scene of technology like CyberCash or DigiCash, the cash-based systems, that everybody thought was going to take off immediately, and it kind of got replaced by the traditional credit card payers. And the cash systems are out there, they have some applications, but they haven't spread like everybody thought they were six months before.

I'm not saying that I don't think this technology -- I know it can work, it does work, there's no question about it, but there is a long way between

that and the kind of ubiquitous market, and I know that people, Jim, wants to do this, wants ubiquitous market acceptance, but to tie a rule to it where the statute says "available technology" I just think is not being realistic.

And if we do a look-back in whatever it is, two years, three years, five years, or a look-back when there is sufficient -- it really shouldn't be so much time, the look-back or look-again by the Trade Commission is when there is some threshold of available technology that makes sense, and we would like to see some rule or some approach that built that flexibility in.

I don't know that there's a magic to the time. There's more a magic to the technology and the application, and that's where I think we'd like to see it going.

In saying that, I want to be encouraging, not -- from the Direct Marketing Association perspective and others too -- because this technology isn't only going to be great for consent purposes. This technology is going to be great for a whole lot of commercial applications and reliability. So, the technology is -- I'm sure Eric would agree -- this technology is great. We're all waiting for it to develop, but it's just not

realistic that it's there yet for this kind of market.

MS. LEVIN: Katharina?

MS. KOPP: Yeah, Katharina Kopp for the Center for Media Education.

I just want to clarify, the five years that has been brought up by industry in connection with allowing e-mail consent to parents during that time period, we think that's a really bad idea, to have -- to lower the bar during that time, which in Internet time is an eternity. I mean, that's a really long time where a lot of things can happen, and we think it's really important to provide incentives for companies to develop new technology that actually would allow it to make the interaction more seamless. So, if we establish e-mail as the standard, in the next five years, there will be hardly any incentive for anybody to develop new technology.

MS. LEVIN: Mary Ellen?

Oh, I'm sorry, I thought yours was up.

MS. FISE: Not me, it's Paul.

MS. LEVIN: Go ahead.

MS. LANDSMANN: I want to follow up on one of your -- are you starting down there?

MS. LEVIN: No, go ahead.

MS. LANDSMANN: I think this morning we asked

for a two-year sunset period, because we do believe this technology is around the corner. I wanted to pick up on your question a couple of questions ago, Toby, and ask the three gentleman who have described very intriguing, very intriguing and very hopeful products, what's your business model?

I'm in the process of doing our three-year plan now. What's this going to cost us and how -- how -- and I ask this for -- believe it or not, the TIME for Kids website budget in 1999 is $178,000. So, if you're going to come in with a program, you know, three years from now that we need to budget three times that for verification, we need to -- we need to know that now.

MR. TEICHER: Okay, I can --

MS. LANDSMANN: Jim?

MR. TEICHER: -- I can speak from our perspective. Well, actually, our business model does not involve charging websites.

MS. LANDSMANN: It does not?

MR. TEICHER: No.

MS. LANDSMANN: Who pays?

MR. TEICHER: It's a low-cost subscription model packing lots of value into the product. What we really want is, you know, at the end of the day, you know, for it to be extremely low cost and there to be tremendous

value on the part of children for having this by virtue of the values that they will reap from the Internet safely, and so we're -- we really want -- I mean, we're very sensitive to costs on all ends; however, this is a business, and it's important to consider that, as well, and we believe that a low-cost subscription-based business model that will bring as many websites in as players and acceptors of this standard will offer the most to children online and websites.

MS. LANDSMANN: What is low cost?

MS. LEVIN: Excuse me, just for the record, identify yourself.

MS. LANDSMANN: Leanna Landsmann, TIME for Kids.

MR. TEICHER: We can have a meeting about this offline.

MS. LEVIN: Okay, Paul?

MR. HERMAN: Paul Herman, iCanBuy.

Which question am I answering?

MS. LEVIN: I'm not sure.

MS. LANDSMANN: Business model. Are you charging the user or the operator?

MR. HERMAN: On a business model, it is -- well, our business model is free to consumers, but since we are a financial engine, we actually need to put some

money in the financial engine, but you get it all back. There is not an extra fee beyond that. So, it's essentially a free service like your -- I'd like to say like your investment house is, banks aren't free service, and so the business model we have is a share of revenue with the merchants and a revenue share back to communities like yourself that have content and aggregate audience. So, that's on that question.

On the timing question, Toby, I think the issue is to what level does the Commission want to rule on what results are expected versus what process or methods are used versus what specific technologies or mechanisms, and if you're talking about a sunset period, the more results-based it is, the more shorter it can be. The more specific it is in terms or methods or process, the longer it would have to be to accommodate for solution development, to accommodate for businesses to put priorities on it, to accommodate for an emerging standard, if there were to be a standard enforced, and to accommodate for the technology queues in all the businesses across the country.

So, the key question, I think, is what is the consumer problem, and the reason why solutions like CyberCash and DigiCash did not work is there was not a blazing consumer need, and so the consumer need that's

here is definitely recognized by everyone in the room.

The question would be what do the consumers out in the mass market believe the consumer need is? Do they need privacy? Do they need permissions? And for businesses, they need to recognize that either there's a consumer need, there's a competitive reason to do it or there's an economic opportunity to do it or there's a proposed rule reason to do it.

So, I think that those are some of the issues to address in terms of timing, but if there is a sunset and it's not clear from the implementation of the April 2000 statute, it should be no longer than 12 or 18 months.

MS. LEVIN: Okay, and one last comment, Jason, and then we are going to do a wrap-up.

MS. CATLETT: Thanks, Toby.

As a technologist, I tend to get a little skeptical when told that technology is right around the corner. In fact, I get a sense of deja vu in this room, because two years ago around this time we had a demonstration at one of the FTC's technology hearings of P3P, a technology that would protect privacy and would make legislation unnecessary.

We are here and P3P is still the technology of the future. I think it has been and always will be the technology of the future. So, let's not wait around for

wonderful technology before we live in the present world.

The proper thing for the Commission to do is to insist stringently on a performance standard to be applied. If the Commission does that, that will enable the development of appropriate technology, not hinder it.

MS. LEVIN: Thank you.

To wrap up, let me sort of do the -- what Lee Peeler did this morning, and I'll start with Ron and give you a minute to collect your thoughts, but do it a little bit differently and ask, what's the most important point that someone else made during this session? So, no tooting your own horn.

MR. PLESSER: Well, the most important point that someone else made, as I said before, was made in the earlier panel, I think, which was the CARU point, which is that there has to be it seems to me a sliding scale in terms of the nature of the consent. E-mail is appropriate, you know, for notification when the information is only going to be used by the marketer.

I think it perhaps is not sufficient, and I would agree with Katharina that it's not sufficient, in circumstances where you're enabling somebody, a child, to communicate to third parties or to the rest of the

world, and I think that that really is the most important thought.

And it wasn't original to me, so I can say that.

MS. LEVIN: Okay, Leslie Harris.

MS. HARRIS: Well, I think probably the notion of performance standards. I mean, I think it's really important for us to think about how we're going to measure this bill. I think Sheila was the one who raised that, but in that regard, I think what I -- what I want to say is that I think the performance standards have to be in the context of what it is we want this bill to achieve.

Is the goal of the bill parental consent or is the goal of the bill to change the practices online? I mean, you know, we do a performance standard that says, you know, 37 percent of the parents did X and 10 percent of children. Why if the ultimate goal of this is to measure that? If what you're trying to do is change the practices online, then the performance standards need to look at how these different models impact the -- impact the sites, how many -- how many more sites comply, how many more sites change their practices, perhaps so that they aren't even collecting the information that triggers the requirement in the first place. I mean, I

think that's what we need to focus on.

MS. LEVIN: Okay, I am going to -- sorry to cut you off, in order to make it through and keep on time.

Eric Wenger?

MR. WENGER: The most interesting thing that I heard today is that the technology is there to do a lot of these -- to make creative solutions for obtaining parental consent and that hopefully the performance goals set by the Commission will spur industry on to adopt mechanisms that will create real, verifiable parental consent.

MS. LEVIN: Sheila Millar?

MS. MILLAR: Sheila Millar for Mars Incorporated.

I guess the most interesting point to me was the point that Cassidy made this morning, which is that the vast majority of the CARU sites are sticking to information collection practices that fall within the exemptions, and so what I think we're doing today is spending a lot of time on a very important topic, which is how to get verifiable parental consent, for those parts of the Internet activities where I think we all share, as Ron mentioned, some pretty significant concerns about protecting kids in that environment.

Frankly, I think what may make sense is the

emphasis on the need for flexibility, flexibility to allow the marketplace to mature, to allow technology to achieve market acceptance and to prove itself out and that perhaps because of the statutory deadlines, moving quickly towards recognition of some safe harbors where some of these discussions can continue to evolve would perhaps make some sense in terms of protecting children.

MS. LEVIN: Thank you very much.

Dan Jaffe?

MR. JAFFE: Well, I also think that the sliding scale point was a very important one and deserves a good focus by the FTC. I also felt both in this panel and the one before that the law of unintended consequences was a worthy idea, that if you set the bar too high with a performance standard that's too difficult, you are going to have the unintended consequence of driving kids into nonkids sites, which is the opposite of what anybody here wants to do, and it's also going to create economic disincentives for new start-up companies, because it's going to just be too expensive for them to compete.

So, I think the FTC has got to be a little careful in how they affect the marketplace by these standards, as well.

MS. LEVIN: Thank you.

Katharina Kopp?

MS. KOPP: The most interesting point I think is the point that Leslie made, because it worries me most. Leslie made the point about children will be prevented from having access to information if the hurdle is too big, and I think we should remind ourselves that the access to information should not be conditioned on giving out valuable personal information, and I'm concerned that the business community has accepted the standard that -- and has made the consumers believe that it's normal to give out personal information in exchange for access to information.

Therefore, I think the standard for the Commission should be whether -- not whether kids leave certain websites because the burdens are too high but whether or not websites develop content without asking for data collection and return.

MS. LEVIN: Thank you.

Leanna Landsmann?

MS. LANDSMANN: Leanna Landsmann, TIME for Kids. I think this is a good way to go about this, Leslie, and there were several, and I think the one that resonates most with me as fundamentally important, actually, was Jason's, who said in the balancing of the

false negatives and false positives, you know, we not only need a means to identify the kid who poses as an adult, but we have to make sure that we are not preventing the kid whose parent would have given him permission or her permission to participate if we had only reached that person.

So, I think that the -- that this opens up a whole arena of areas that I think have been unexplored today, not only equity issues about socioeconomic groups but the place where kids are online in schools, and it takes -- it looks at a whole slew of educational applications that I think I would encourage you all to explore, but I thought, you know, Jason's point was very well taken, that we can't do something that's going to shut the door on a lot of kids.

MS. LEVIN: Thank you.

Jim Teicher?

MR. TEICHER: Yeah. I think what's really remarkable is the phenomenal progress that all of us together are making to understand and resolve this issue, which I think is wonderful, but to be a little bit more specific, I think the sliding scale is critical. I think giving technology time to mature and to Ron's point, as opposed to putting a date, look at technology instead and where we're at and do that on a

regular basis.

MS. LEVIN: Eric Aledort?

MR. ALEDORT: I thought the most interesting thing that's come about today was your question about what hurdles exist besides technology on implementing some of these solutions, and I just think it's important that we keep in mind that although we're past the very early adopter stage on the Internet, there are still a lot of people who still are not online, and those who are online are very nervous about giving out a credit card or providing other personally identifiable information in order to do something simple like get an e-mail account.

So, my point is one that we need to remember, that it's going to be a slow process of getting 80 or 90 percent of the households in America online, and also, too, I think the businesses can take a leadership role and try to really encourage the way Microsoft and IBM and Disney have of not accepting advertising, not doing business with people who aren't posting privacy policies, and that's a great way to really incentivise both small sites and big sites to really get behind this wave of concern on private information.

MS. LEVIN: Thank you very much.

Jim Brandt from VeriSign?

MR. BRANDT: Okay, I think the most telling comment that, of course, has been said in a number of different ways is the recommendation I think for the FTC to concentrate on the framework and the metrics under which the ruling can be embodied. We've heard this notion of a sliding scale, et cetera, but what this really means is to try to establish the criteria based on whatever the right definitions of that matrix are, to establish the appropriate criteria, which would be -- criteria would be both mechanisms and processes which together can be combined to provide verifiable parental consent, and perhaps they be tuned to the particular data which is being requested for interchange and the particular intended use of that information.

This whole notion of rated assurance, et cetera, is a fundamental theme in security systems, and we ought not lose concept or lose sight of that particular concept in applying appropriate mechanisms to this particular application of security. Thank you.

MS. LEVIN: Thank you.

Mary Ellen Fise.

MS. FISE: I'm reminded of the philosophy from the movie Field of Dreams, "If you build it, they will come." I think if the FTC requires this, it's going to happen. We have been told the technology is there, and

a sunset provision is not needed.

MS. LEVIN: Paul Herman?

MR. HERMAN: A blend of things have appealed to me today, from what Kris said in terms of distinguishing entertainment from other activities on the web, in terms of audience and the need for personalization and customization, depending on what the purpose of the content or the commerce is. I think Parry is very tuned into the pragmatic ways of approaching how to balance the needs versus the value, and then the discussion about performance standards and performance metrics is something near and dear to my heart, from David.

MS. LEVIN: More than one significant idea.

All right, and we'll close with Jason Catlett.

MS. CATLETT: Thanks, Toby.

I think the most important point was Ron Plesser's opening statement that e-mail is an adequate standard of verification. Unfortunately, I think this statement is plainly wrong. I would also question whether e-mail plus is --

MR. PLESSER: Point of personal order. Toby asked us to list the e-mails without necessarily saying those are the ones that we supported.

MS. LEVIN: That's true.

MR. PLESSER: So, I think it's very important to

have the context, Jason.

MS. CATLETT: Okay, so I think I'll just make a general statement that -- without attributing it to Ron that the -- that e-mail without -- by itself is not -- not adequate. I would even question whether with a credit card it's adequate given that no charge is made to the credit card. So, if a charge were made, then the parent would find out that there had been this kid who perhaps pilfered it from the handbag, but absent that, there may be no mechanism for detecting that.

But the positive point that I liked most was Paul's point that the FTC should define performance criteria and that companies should be audited for -- to verify their compliance with those criteria rather than trying to designate a particular technology as adequate, per se, without regard to how it's applied.

MS. LEVIN: Okay, thank you very much.

Now, I'd like to invite those of you in the room who would like to come forward and add some of your comments to the record, please line up, and keep your comments short, please.

MR. CHESTER: Thank you very much. I'm Jeffrey Chester, the Center for Media Education, and one comment I have heard today, and I'm sort of flabbergasted by this comment, that people here -- although I'm heartened

that people here are concerned about the so-called "have-nots," I did not hear that the one way to ensure that you reach those people is through mail.

As you -- the mike is not working -- as you may know, telephone penetration in this country is at 94 percent, that might be high, but there is still 6 percent, and as you know, if you look at a low income community and communities of color, that telephone penetration drops down to 85 percent, and as a group that's been involved in working with others in getting the e-rate, we are trying to get kids connected, but we've got a long way to go.

So, if you really are concerned about the have-nots, and I have heard some admirable comments today from people, I think that mail is the one way to reach those people. And I've also heard some concern that the Commission address rules that would allow some of the companies to come and, in essence, market to the schools, and I suggest to you that was sort of outside the scope of this legislation, and I'd be very weary before the Commission develops policies that allows personal information to be collected in the schools.

Thanks.

MS. LEVIN: Thank you. Because we're running short on time, I really can't allow for --

MS. LANDSMANN: I just want to make sure that he's not attributing that to me.

MS. LEVIN: There was no attribution.

MS. LANDSMANN: No, but I'm the only one who brought up schools, and --

MR. CHESTER: No, this morning, I think this was MaMaMedia, so it was Time Warner and MaMaMedia.

MS. LANDSMANN: Meet me outside later.

MS. LEVIN: Please identify yourself.

MR. BRYAN: Oh, I'm sorry, Steve Bryan, Zeeks.com.

I just want to direct a comment here to Mr. Catlett about his statement, I think you called it the solar power of the Internet --

MR. CATLETT: Anonymity.

MR. BRYAN: -- anonymity, I couldn't agree with you more, and I have a feeling you and I would agree on very little; however, we built a website based entirely on anonymity, and I just want to make it very clear to everyone here or please make it clear to me that I misunderstand that a nickname falls under this rule, and providing anonymity even with a made-up nickname requires me to get verifiable parental consent and burdens me with all of those costs of building this -- okay, I'll be corrected if that's not true.

MS. CATLETT: I'd like to ask the FTC, but I think a pseudonym is regarded as not personally identified.

MR. BRYAN: Okay, maybe I'm wrong.

One quick thing, too, on the cost of this. I have some personal experience here in the last four months in developing a system that both in some areas does not require parental consent and we also run a chat room that does, and we have set up our chat room through Freezone, who I think is here, and they do a wonderful job.

They are one of the leaders in doing kid friendly verified parental consent chat, and we currently have over 70,000 registered members at our site in only about 90 days of activity, and in the chat area, which has been running concurrently with that, we have 1400 people who have gone through the process of taking the extra step in getting the parental consent, and I can tell you that that destroys the business.

If you apply that rule broadly across all activities on the site where we use nicknames, set cookies, things like that, we're out of business.

MS. LEVIN: Now, for your information, if -- go back and take a look at the proposed definition of personal information. It calls for identifiable

information, such as a full name. Nickname has not, as far as I know, to date, been suggested as identifying information.

MR. BRYAN: Okay. Well, if I --

MS. LEVIN: So, that would not be, nor is aggregate -- nickname -- nickname alone would not be identifying information. If you collect the nickname with an e-mail address, then it becomes identifiable.

MR. BRYAN: Sure, yeah.

MS. LEVIN: But a nickname alone is not identifying under the current proposal.

MR. BRYAN: Okay, if I --

MS. LEVIN: Nor is any aggregate information.

MR. BRYAN: Then I'm going to keep down the anonymous trail, and that's how we built the business and will continue to run it.

Thank you.

MS. JALLOH: Jeneba Jalloh, Institute for Public Representation, Georgetown University Law Center. We submitted comments on behalf of Center for Media Education, Consumer Federation of America, Junkbusters and other commenters.

My comment and question concerns verifiable parental consent. I believe this morning this afternoon's panel showed clearly that there is a

distinct difference in verifiability between e-mail online versions of consent versus other types of consent, meaning offline methods of consent.

For example, Parry Aftab this morning mentioned how one of her staff members was able to determine that a child was posing as a parent. Similarly, Jorian Clarke from Circle 1 also determined through the mail that -- they were able to determine that it was a child and not the parent; however, when the representative from MaMaMedia, Disney and I believe -- there was another one -- I think it was TIME for Kids, when they said that they had facts which showed that it was e-mail, they weren't able to verify that it was a parent actually and not the child that had sent that e-mail, and that's -- I think that shows clearly that verifiability is more -- it's easily found in offline methods as opposed to e-mail methods.

And my question is, for those of you who are supporting a sliding scale, how do you -- what other variables do you suggest for the FTC to use and how do you suggest that they enforce that?

MS. LEVIN: Given the fact that we have a number of people who want to make their comment, I am going to leave that as an unanswered question just so that we allow for an opportunity for other people who haven't

had a chance to participate to at least get their comment or question on the record.

MS. CLARKE: I also need to make a correction. Circle 1 Network did not say that e-mail was verifiable. We could assume that there were some things, but we had to contact them in order to verify that. The mail was not verifiable.

MS. AFTAB: Right, and the same thing with us, although in some cases it's obvious that it's a kid, you can't always tell, and we're not sure that it's more credible on the phone than it is by e-mail.

MS. JALLOH: Okay, the point was you were able to determine --

MS. AFTAB: In one case, but that wouldn't mean that we wouldn't otherwise, but...

MS. LEVIN: Okay, next, yes.

MS. LINN: I'm Susan Linn from the Media Center of Judge Baker Children's Center, and I have a question for Leslie, actually, I have two questions.

My first one is what is the ALA's position on commercial companies eliciting personal information from children?

MS. HARRIS: They are opposed to it. You know, at the beginning of this whole process, our view was the right way to do it, which were we were told by the FTC

was not going to be doable, was to decide what was going to be an unfair trade practice and prevent it from being done in the first place. It isn't our desire to have that information collected.

What we are saying very simply is that when you -- when you seek to solve one problem, do not create solutions that create problems that are -- that could be equally troubling, and it is a mission of ALA to make information accessible to children. They do that every day with children in libraries and are able to see the barriers, particularly for poor children. So, I mean, the ALA has the strongest confidentiality policies in the country.

MS. LINN: You know, I certainly share your concern that children have access to information, but I -- my other question has to do with the issue that Katharina raised, and I want to know under what circumstances does the ALA think that children's access to information should be limited by the requirement that they provide personal information?

MS. HARRIS: I'm sorry, I don't understand the question. When should you? I mean, in the --

MS. LINN: Under what circumstances should children's access to the information --

MS. HARRIS: The ALA's view is the only time you

should be collecting information is if you need it for the transaction that's presented, you know, it's a game or you're signing up for -- I mean, something. They are perfectly happy with the notion that all other collections and third-party disseminations be illegal. That's not what we're doing here. We're -- rather than -- rather than proceeding with telling the companies what they are not allowed to do, except for some of the things that have been found unfair trade practices, instead --

MS. LEVIN: I think I am going to have to --

MS. LINN: So, this is not an access of information issue, is that what you're saying? This does not have to do with access of information?

MS. HARRIS: Of course it does, but we can talk to that later.

MS. LEVIN: The statute really is not focusing on access to information. It's verifiable parental consent, but I appreciate your comments.

MS. MULLIGAN: Deirdre Mulligan at the Center for Democracy and Technology.

I had a question for CyberSmart! and VeriSign, and it's a two-part question. One is what's the kind of information that you require parents and children to submit in order to issue something "verifying," quote

unquote, their identity, and what kind of authentication do you go through to do that?

And two, what are your obligations as far as using that information?

MR. TEICHER: Well, so far as what we collect from children, we don't -- from children themselves, we don't collect any identifying information whatsoever. From parents, we collect a lot of identifying information, including their credit card number and their address as if they were buying a product, and at their children's school, a fair amount of information.

MS. MULLIGAN: And do you collect any information about where that certificate or where your product is used?

MR. TEICHER: Where it can be used?

MS. MULLIGAN: Where it is used. For example, do you collect --

MR. TEICHER: No, none whatsoever.

MS. MULLIGAN: -- any data?

MR. TEICHER: None whatsoever.

MS. MULLIGAN: And what do you do with the data that you maintain, anything other than provide the service?

MR. TEICHER: The data that we maintain is just for the purpose of signing up parents. Remember,

parents are the customers --

MS. MULLIGAN: Right.

MR. TEICHER: -- of our service. Children are not.

MS. MULLIGAN: So, you don't disclose that information or make other uses of the information or --

MR. TEICHER: No, we don't -- we don't -- wouldn't disclose it or provide it to anyone whatsoever, no.

MR. BRANDT: Briefly, I think, in the interests of time --

MS. LEVIN: Please.

MR. BRANDT: -- to find out what information we do collect, when a consumer comes to VeriSign to request a certificate, check our website, www.verisign.com --

MS. MULLIGAN: I've been there, it's not just for me.

MR. BRANDT: Right, but that would be my answer in the interests of time.

Secondly, by our policy of privacy requirements, we do not do anything with that information that we use to obtain for authentication purposes. It is our responsibility not to divulge that information, but we have to retain that certainly for the purposes of verifying that we issued a certificate to a particular

individual, and we have a responsibility for auditing requirements in order to provide evidence that, in fact, we gave the right person the right certificate.

MS. MULLIGAN: And you don't collect transactional data, either, about where people use it?

MR. BRANDT: We do not know about anybody's transaction, correct.

MS. MULLIGAN: Thanks.

MR. TEICHER: We're not either.

MS. MULLIGAN: Thank you.

MS. LEVIN: Yes?

MR. CORLIN: Phillip Corlin, Federal Legislative Associates.

I'm representing MP3.com, and I just want to caution the Commission that one should not presume that traditional economic models are going to be the models which are prevalent in the Internet going forward. I think a lot of this discussion is predicated on assuming that a child-specific site and that information being collected by the operator of the site to market something to the child or at least the parents of the child.

And there are a lot of new models which are general purpose sites, I think my client in particular, in which one small portion of the site is dedicated to

something that is designed to appeal to children, specifically children, which is children's music, and the primary information being collected is the e-mail address, primarily not to sell something but to allow the artist, the musician, to communicate directly with the visitor for whatever their purpose, to let them know they are going to have a concert, to, say, have a website with more information.

So, there's going to be an awful lot of free content available, a lot of it for promotional purposes, high-quality content, and to the extent you make it burdensome for either general website operators with a portion devoted to children's content or people creating content who want to draw people to their site, to comply with this, you may make -- diminish the amount of low or free-cost content available to consumers and drive them towards more traditional purveyors. So, I would hope that that would be taken into account as you're finalizing this regulation.

MS. LEVIN: Thank you very much.

MR. IZRAK: My name is Mark Izrak, and I'm with bizrocket.com, and we operate a portal site that is a search engine/public forum specifically based on ethics, and it has a business ethics bureau on the site, and as a part of the portal site, we have a free e-mail system,

and one of the things that we're doing on the e-mail system, which I think will be of interest, is that we are delineating the domain name at the end of the e-mail address to verify whether or not it is an adult or a child.

So, that will tell any website right away that this website has been or this -- I'm sorry, this adult has been verified that they are an adult, and that should solve a lot of problems.

MS. LEVIN: And if I could just follow up, and they will be identified as adult because what -- what information have they given you to -- for identification purposes?

MR. IZRAK: They will be using a credit card for a very small transaction, or we will be mailing to them via normal U.S. mail if they want to go the long way to do it, which will be a free transaction, but that will enable this to happen, my guess, within 30 to 60 days.

MS. LEVIN: And is this service up and running on your site?

MR. IZRAK: The free e-mail is up and running and this is an upgrade that is in progress.

MS. LEVIN: Thank you for bringing it to our attention. We appreciate that.

MR. IZRAK: Sure.

MS. LEVIN: Thank you very much.

We are going to take a ten-minute break, because I think everyone is feeling the need to move around, and we are going to switch panels.

MR. PEELER: Before we break, if anyone -- there's been a lot of discussion in the last two panels about performance standards and criteria, but we haven't talked or haven't had the opportunity to talk with any specificity about what those performance standards and criteria might be.

There -- the record of this workshop will remain open until July 30th, so if you have ideas or thoughts on what those performance standards or criteria might be, if you could submit those thoughts for the record of the workshop, we would appreciate it.

MS. LEVIN: I'm sorry, thanks very much.

(A brief recess was taken.)

\- - - - -

SESSION III

- - - - -

MR. MEDINE: Okay, thanks very much, if everyone could just grab their seats.

If we could close the doors there so we could get started. Shaun, close the doors, please.

Well, thank you. We clearly have a group here

that's very committed to children's privacy if you're willing to stay all day here to discuss the subject. So, you're all to be commended for sticking around.

We're going to move in this last session to looking forward, see where technology is going, to see what alternatives there are to the technological solutions that we have heard about so far. And in addition to that, we're also going to look at the possibility of intermediaries or infomediaries serving as a conduit between parents and websites in order to provide efficient means of giving verifiable parental consent.

I notice we have also been joined by yet another commissioner, Commissioner Thompson, as well as Commissioner Anthony, and actually, they should feel free to involve themselves in the questions and the dialogue as we go along.

I want to first start off -- start with a series of discussions of various models for new technologies to provide solutions, and the first -- Oscar Batyrbaev from eOneID.com has something called a lune check, and I would like you to describe the technology that your company is developing and how that would work to provide verifiable parental consent.

And if people could speak into the microphones

and identify themselves.

MR. BATYRBAEV: Yes, Oscar Batyrbaev, eOneID.com, and what we have is a free web-based service for -- the service is free for companies as well as for consumers, which does use a credit card or bank card authentication or verification of the fact that it's a parent.

I actually have some slides here, as well. I'm not sure if that's appropriate, but I can talk to --

MR. MEDINE: If you want, we can use the --

MS. LEVIN: You can put it up.

MR. BATYRBAEV: Okay, great.

MS. LEVIN: Sallie, would you get the slides and put it on the --

MR. BATYRBAEV: Okay. No, no, the other one first, Exhibit A.

So, this web service meets -- in our estimate it meets all requests of privacy advocates and at the same time it meets industry concerns and also meets Visa concerns that they don't want, according to their comment, use of a credit card network as a verification vehicle. It uses both credit and bank card verification online, because some people, for instance, don't have credit cards, and preserves consumer privacy at the same time, because the card number never leaves their browser

and doesn't go over the Internet. We actually have a guarantee to them that, you know, it only will be checked inside of the browser.

And as well, it has -- like the Library Association was talking about here, it has service for parents who do not have Internet access but whose children do have Internet access in libraries and schools, and this allows parents who do not have Internet access but do have telephone service to verify themselves and give parental consent that way, and as well it's free service, as well.

So, the company, by the way, is located in San Jose, California, and the -- also, the Commission raised questions what incentives it will give to companies as well as parents, and my next slide talks more about that.

And we have a reward program which diminishes the pain of a parent having to verify themselves. It only takes actually two minutes if they do have credit or bank card handy or may be asked to verify their -- that they are parents, and -- but they still would get, if they want to, our reward currency.

And as well it has what we call kid e-allowance program that lets kids shop without credit cards online. And this program has two variations, fine grain

parental control for parents who do want to exercise control over what their children want to buy or are buying, and also more freedom for children and for 'modern age' parents, as well.

MR. MEDINE: Can you explain how it is that you're able to verify that someone is a parent based on information that's provided, as I understand it, through their browser and that's not transmitted to the website?

MR. BATYRBAEV: Yes. We use a number of algorithms. One of them is a [onecheck] (phonetic) algorithm, and the idea of using it came from the Senator's comments on the COPPA, Children's Online Privacy Protection Act, and the senators found that -- the senators that were backing COPPA this mechanism is acceptable to verify that a person is over 18 years of age.

And what we have, we have a developed system which maintains state, and we know that this is parent of this child, so it links the parent and the child together without knowing exactly who the parent or child is.

MR. MEDINE: Again, I guess I'm not sure if we're getting into your trade secret area, but if you could explain a little more how that process is

accomplished, I think it would be helpful to assess the extent of how verifiable is it is under the statute.

MR. BATYRBAEV: Okay, the system works, if some of you are familiar -- similar to Disney system. Disney system does maintain, as well, the state, when parent comes, they give them URL. That's what we do, as well, we give them unique URL or send them e-mail or do SETP transfer or interact call, and then we know exactly that this is the parent of this child.

The technology is there. It's actually not that super difficult to do. We use -- we do not use digital certificates or anything like that. We use the standard protocols and our developed algorithms to maintain the state between the parent and the child. So, when the parent comes into, let's say, a website who wants to take e-mail and full name and so forth from them, they come to a website -- I have something on that, as well, here --

MR. MEDINE: If you could just briefly describe it.

MR. BATYRBAEV: Okay, they come to the website, and we identify that child by URL. Then parent, if the parent is at home, can verify himself or herself right at that time by going to our website and going through a number of algorithms. Then we do a CD transfer

transparent to the parent back to the children's website where they came from, let's say Disney or Warner, and then they -- they have already eOneID in their possession, and then they just verify themselves that they are parents at the actual Disney site -- using that just as an example -- and then they know that it is a parent verified by our system.

MS. LEVIN: Oscar, if you could provide the -- a handout, too, at some later point of the download that you would have provided, send it to us for the record, then we can add it to the transcript.

MR. MEDINE: Okay, and is this service up and running right now?

MR. BATYRBAEV: This service is in alpha right now. The -- some components are already of production quality and some of them are in alpha state, but by the -- by the date of the -- the statute may go in effect in April, right, it will be all up and running for many months.

MR. MEDINE: Okay, thank you.

Let's hear from another model, we will go through a couple of different possible models with new technologies. Next, Steve Lucas from Privaseek, if you could describe the direction you're heading in terms of methods for providing verifiable parental consent.

MR. LUCAS: Thank you. My name is Dr. Steven Lucas, and I'm the senior vice president and CIO of PrivaSeek.

First I'd like to thank the FTC for inviting us to this very important workshop and commend the FTC for its thorough work in drafting a proposed rule that comprises the general goals and the specific mandates of COPPA. Our written comments are part of the current rulemaking record, and we focus on, again, the verifiable parental consent section of the rule.

It's our belief that personal information from children or about children should not be collected, used or released to a third party without parental consent. As a general matter, PrivaSeek is concerned about nondigital and digital signature, enabled e-mail, land-based mail, faxed-in consent forms, credit card transactions and toll-free consent calls to be authenticated.

We believe that technological solutions provide the most effective, the safest and efficient means of protecting sensitive online data without unnecessarily hindering the growth of the electronic marketplace or the ability of consumers to control their information and ultimately even get value from that information.

Our model is based on what's become known as

permission-based marketing. Permission-based marketing is where consumers either volunteer or request to be marketed to. It's based on the fundamental notion that consumers own their personal information and should be in control of it online. That also includes the ability to track the use of the information and to control under what circumstances it's provided.

I'll give you an example. Seth Goden (phonetic), former CEO of YoYoDine, in his book entitled Permission Marketing defines permission marketing as, first of all, anticipated, people look forward to hearing from you; personal, messages are directly related to the individual; and relevant, the marketing about something that is interesting to the individual.

He also, in an article that was published in Digital Commerce, describes his success with permission-based marketing. He talks about the fact that before he was acquired by Yahoo, he created and ran about 150 of these permission-based promotions, and the response rate he got using a permission-based approach was 20 -- between 15 and 20 percent. Using traditional direct marketing approaches, his response rate was less than 2 percent.

He also talked about several companies that he mentions that are spending in excess of $300 using

traditional, again, direct marketing approaches to acquire a customer, where he mentions a large brokerage house in New York that's spending less than $15. I think it demonstrates that permission marketing is effective, and also the rates of response and the numbers in terms of numbers of consumers acquired were equal to other methods.

We announced last month the first stage in our technology called Valet, and Persona Valet acts as a negotiator between the site and a consumer. When consumers visit our site, they are -- and they decide to become a member, they fill out what we call a Persona, and in that Persona they are asked to provide their name, their address, their age, their e-mail address and the preferred method for PrivaSeek to contact them.

They can also add additional information, such as hobbies and interests, and e-commerce information, like credit card information, and ship-to. That information is never released without the consumer's consent, and the way that happens is for every data element, the consumer has the ability to assign a privacy preference or usage preference for that data.

That usage preference can be changed at any time by simply going back to the site and changing that preference. At the end of the day, it's the consumer

who chooses what information is going to be released and when.

Security is obviously very important to us. What we've done is we've engaged a third party who manages our -- what we call our Persona vault. That Persona vault is maintained at a secure facility with a company that has a long history of managing sensitive information, and that company has auditable security practices from both a data as well as a physical plant perspective.

PrivaSeek partners who want to become certified have to go through a very rigorous approval process where we use a third-party privacy expert to go in and review their privacy policies and their data collection practices. If they are approved, they agree that they will abide by all of the PrivaSeek preferences that the consumer has identified. If they fail to abide by that contract, we will seek legal action against them, plus we will also assist the individual consumer in any private right of action that they may have available to them.

We don't believe that any information should be collected from children under the age of 18, and it's our belief that that information is essentially owned by the parent. We are incorporating what we call the Child

Persona into our technology, and what that does is it is similar to what we talked about just now, but it's based on the idea that the parent creates the Persona for the child and determines what information and again under what circumstances that information can be released.

We also look at the children's information as being sensitive information in that there may be information that can identify the child or cause potential harm. Because we think it's impossible to really know the implications of certain combinations of data, we think it must be possible to employ a very extremely conservative model of information delivery as a default.

The way it kind of works is that a parent is assigned a digital ID and an e-mail account. The parent can then create a Child Persona, and that's to be used by the child. The child Persona contains information supplied initially by the parent, and the parent's Persona ID is also embedded into the child's Persona. The child can use the Persona to access the web and interact with either Persona-enabled sites or not Persona-enabled sites.

The parent can specify the required privacy specifications required with each data element. The child can -- has the ability to modify those

preferences, but it does not take effect until the parent responds to an e-mail that is -- includes a digitally enabled -- digitally signed form and responds back using their digital certificate that's been issued.

If the parent responds with a yes, the Persona is updated. If they respond with a no, those changes are cancelled. If they don't respond within a certain amount of time, those changes are automatically cancelled.

We think that the technology does meet the requirements of COPPA. Again, the parent is notified of any kind of transfer that takes place. They are -- they can go back later on through use of the technology that tracks the use of the information and go back to a site and request that the site block out the child's information if they change their mind later on.

We hope that just as a grace period has been given to companies to adhere to the Fair Information Practices set forth by the FTC, that we would allow time for some of this technology to be able to be deployed, recognized and trusted and used by both consumers and in the marketplace, and we look forward to working with the FTC and other industry to make this happen.

MR. MEDINE: Thank you, Steve, just a couple of

questions.

First, what are the costs of this to the parent and the cost to the website, and second, when do you think this will be available for widespread use?

MR. LUCAS: The current model is that there be no cost to the parent, to the child, that it be sponsored by websites, sponsored by, you know, by advertising, third-party providers.

The -- we anticipate it being ready -- our aggressive schedule is by the end of this year, at the latest within the first quarter next year. We have technology now that does a lot of what we're talking about, but because of the seriousness of the kind of information we're capturing, we are going to go through a very, very extensive beta test.

MR. MEDINE: And again, it will cost the website you say?

MR. LUCAS: It will cost the website.

MR. MEDINE: And we have been hearing estimates of various costs. Do you have a range of the cost to the website using this technology?

MR. LUCAS: What we have right now is somewhere between 10 and 20 cents per name. So, it's based on a per-name model. We're looking at a bunch of different models that could impact that cost. Say, for example,

take credit unions. A credit union may provide this as an option, you know, for being a member. So, it may be subsidized by sites that are not necessarily online sites but sometimes even offline sites.

MR. MEDINE: Last question, which is how do you verify that, in fact, you're dealing with a parent?

MR. LUCAS: Again, through the digital certificate.

MR. MEDINE: But what -- you issue it under what circumstances, because of the presence of a credit card or what is it that leads you conclude that somebody is a parent?

MR. LUCAS: When the parent fills out their Persona and they indicate they want to create a Child Persona, the information that's provided, when it's a credit card authorization or a digital certificate from another organization, we then use that to verify. We also send a confirming e-mail and we're looking at also sending a land-based mail for confirmation.

MS. LEVIN: And one more question, just for those of us who are perhaps not as adept at understanding how these systems would work, if I'm a small business and I have a website directed to children, how would we connect to each other, and I have a consumer that comes to my site, a child who wants

their parent to sign -- to give their permission, how would it work?

MR. LUCAS: Well, if the site is what we would call Persona-enabled or certified, then the site essentially pays a fee to use the information and to be set up. What we do is we essentially take their privacy practices and convert them to code so that we can understand what their privacy practices are so we can match them against the usage preferences. So, the site pays a fee for doing that. That's if you're enabled, and there are certain things we can talk about if you're interested that are included in the ability -- in the site being enabled that are different than just a site being -- being just out there.

MR. MEDINE: I guess put another way, we have heard some concerns raised during the day about driving children away from sites because of the difficulty of obtaining and providing consent. What would the child's experience be on a website if the website asks the child for information? How would that exchange take place?

MR. LUCAS: If the site, again, is certified, it's automatic. The whole process is automated. If not, then the request goes through the adult's Persona, and what happens is when you start your computer, you automatically can load the Persona technology. So, what

you would do is get a flashing message on the PC saying you have a message, and then what happens is the parent would respond to that.

MR. MEDINE: So, again, just to summarize, then, from -- if the child was using the technology and it was an enabled site, essentially they would become almost an immediate approval if the parent had authorized that kind of information to be transferred.

MR. LUCAS: Right, and I know that maybe there are some people that might have some constitutional issues with the filtering and blocking capability, but the other capability of the child's Persona is for the parent to embed the sites that they want the child to be able to go to and then on a site-by-site specific basis approve what type of information can be transferred.

MR. MEDINE: Thanks.

I want to turn now to Jeff Johnson from Equifax to -- Equifax, as I understand it, is working with the banking industry to develop digital signature technology, and the question is, is that technology capable of being applied in the context of providing verifiable parental consent?

MR. JOHNSON: David, let me first of all add my thanks to the FTC for pulling together this workshop and inviting us here. I will preface my comments by telling

you that I'm the general manager of a new commercial entity that is designed specifically to solve the problems that we're talking about here today. So, obviously I am relatively biased about whether our solution is workable.

But with that as a preface, we are, in fact, engaging in a new entity that is designed to provide a higher level of security for a range of e-commerce applications, and that would include all aspects of the financial services industry, banking, insurance, et cetera, those that are protecting all sorts of different types of transactions and information, such as medical records, online auctions, and while we do not have a specific application in the COPPA area, I think that, as I described what we do, I think there's certainly a great deal of relevance here.

Our basic business model is to provide an on-behalf service, so we are a service provider, to corporations or those that wish to provide these services. So, Disney or Nickelodeon or Time would be our customer. That range of services would include some of the pure technology devices that we're talking about today, things like digital certificates, smart cards, but please understand that from our perspective, that is simply the technology aspect of it, and the real

difficult part -- and we have gone about it time and time again today -- is how do you bind that digital credential to an individual, and that's really the piece of the business model where we probably believe we bring the greatest aspect of our piece of the solution.

And by the way, the -- the movement all the way to a digital credential is not necessary. If you wanted to stop short of that and use things like PINs and passwords which have been used for many, many years in the technology world as security devices on an interim basis, there certainly is some loss of functionality, but as you try to find an evolutionary process to move into a safer Internet environment, that certainly is a viable option.

Our customers are basically those people that are facing a series of issues, be them legal or regulatory or public perception or financial, in terms of trying to safeguard transactions. If you think of the Internet and you think of the security issues that you are basically trying to solve, they are a couple.

First of all, you're trying to identify both ends of the transaction, who are the parties at both ends, make sure that the communication is being done in a confidential manner and that the data coming through has not been altered or in any way modified.

Over time, with some government help and lots of other things, that whole network will allow you to have contractually binding obligations, and we're a step away from that in some of these technology aspects and some of the regulations and case law and things that will have to come up about what will fall in that place.

The solution that we have developed I would place on today's spectrum at the higher end of the trust model, substantially higher than simply getting an e-mail address or asking for a, you know, simply the receipt of a credit card number, yet what we're trying to do is provide a solution that is convenient -- reasonably convenient, is highly accurate and is of reasonable cost. So, we're trying to find the right balance of all those issues. You can always argue about whether it's too expensive, too inconvenient, but that's the attempt that we are trying to solve, and we are very firm believers that any solution is going to have to be completely online.

Now, you'll have to have some kind of a fall-back system to deal with the exceptions, but if you're not looking for a solution that is basically an online solution, you're missing the whole direction of where this industry is going. You have to be able to deal with virtually, you know, the vast, vast majority

of these on an online basis.

The process, let me take you through a general process. A consumer would come to a web page, and let me just -- we have used Time and Disney, doesn't really matter, but our customer's web page and indicate that they want to do a transaction. That customer of ours would hot-link the customer over to a web page that we run on their behalf. It would have the look and feel of our customer. So, if it was Disney, it would continue to look like a Disney site.

We would give them a welcoming screen that explains that we're worried about their safety and security in doing transactions, and would position the process that we're going to take them through, which is an authentication process, and would gain their consent at that point in time to go through that process.

The consumer would fill out some application information. We've talked about it today. It is highly personal information. It would include name, address, Social Security number and a whole series of personal information. That would be passed to us securely online from a technology standpoint. We would compare that data through a series of very complex and very sophisticated data algorithms.

First of all, we'd clean the data up to make

sure we have standardized addresses, and we're doing two things as we work through this process. First of all, we're cleaning the data, making sure that people that can't type very well are not disadvantaged, but by the same token, we are starting to score the data. We are looking for basically a match between the consumer-provided information and information that will come out of various databases. Those databases will include third-party databases, possibly databases that the customer, our customer, has, and our databases.

To help you understand, obviously, we do have very large, very complex and highly regulated databases. The FTC is someone who knows us, and we know them very, very well. So, there is a component of information here that is highly regulated, highly personal, but basically what we're doing is a compare.

A lot of conversation has been had today about do you really want to now share your credit card number with somebody new? We have this information. So, it's not a situation where you're proliferating it to new people. You're basically exposing it to someone who has it, and what we're doing is a compare process, not a -- you know, not a gathering process.

Based on that information, we formulate even deeper questions, and we proactively pose more questions

to you and ask you to answer additional questions that can, again, come out of our database or our customer's database, and what we're doing is we're gathering your answers and we're comparing the information that you provided based off of a database that is a known database and a respected database.

We basically score your answer, and based on your score, our customer will make the determination as to whether your answers are adequate, is the match close enough based on their particular transaction.

We talked about sliding scales today. I will tell you that if you think about the span of the customers that we're talking to, between financial service institutions, online childhood privacy, access to medical records, these transactions are vastly different, and the risks of exposure if you're wrong are greatly different, and our system has the ability to expand and contract and make this either a simple or more complex process.

You can also raise that. You can ask more questions, deeper questions. You can also raise that score cut-off to the ceiling if you're really very concerned about the outcome. That's the basic process. If you're verified, you move on to the next, you know, set of transactions that you might want to do with that

provider.

We suggest to all of our clients that if you are not verified, for some reason there is a decline, that there needs to be an alternate method in place, and that alternate method can take a lot of different forms. It can be to mail things in or you call an 800 number or do different alternate steps, but certainly you want to be able to authenticate as many as you can online, but you need to have an alternate method that you think is valid.

MR. MEDINE: Jeff, how do you translate this into the children's arena? You have described how I as an adult might get authenticated to a website, that I am who I purport to be.

MR. JOHNSON: Yeah, we have had conversations with a few people in the audience today, and our component of it is one aspect of it. What our component does is it verifies the identity of the parent, we believe very accurately, relatively quickly and not with that much hassle. The issue that it does not help with, I'll be very candid, we have no idea how to match Jeff Johnson with the kids.

Now, whether or not you do that through kind of a legal obligation, Look, I know you're Jeff Johnson, and you're telling me Tommy is your kid, click here, and

I've accepted that as a binding issue. We do not have the ability to do that level of verification at the child level, but we do have the ability to give a very, very high level of assurance that you are talking to the adult and not the child, and I think the comment earlier about false positives and false negatives is a very, very powerful framework to think about, because the real issue there is the very precocious 11 or 12-year-old who decides that I'm just going to cheat the system.

I mean, I think that's probably the bigger dilemma. There is a dilemma with a parent that says, You know, my next-door neighbor wants me to verify his identity, and I'll do that. That's an issue I don't have a solution to that.

MS. LEVIN: If I could ask, Jeffrey, what percentage of children -- let's say that teen or the precocious child who wants to falsify it and they put in their name, how likely is it that you would have data on that child?

MR. JOHNSON: It is very unlikely I would have data on the child unless -- especially given the, you know, the age group that you're shooting for here.

MS. LEVIN: And in terms of the general American population, what percentage of adults would you have data on so that they could actually --

MR. JOHNSON: Well, now, you already know the answer to that, but I'll -- we have data files on approximately 200 million individuals in the United States, another 100 million in other parts of the world, and the data, however, just to make sure people do understand, that runs from what we call a very thin file up to a very rich file. So, as they say, a 19-year-old who has a very -- you know, probably, you know, less credit relationship generally would probably have a file with us,, but it would be thin, but that comes down to a little bit of our customer's decision on how you are going to run an algorithm. I don't think you are going to get a lot of 19-year-old parents looking to get 11-year-olds access to the Internet. I mean, it's just reality to say that.

The other thing I mentioned earlier is that we have other databases that we can access. The issue of creditworthy versus, you know, say the lower economic denominations that don't have necessarily a credit relationship may have a check-cashing relationship, may have a bank relationship, and we have access to files of that nature, as well.

MR. MEDINE: We have heard a lot about efficiencies both from the parents' side and the website's side. Does a parent have to go through this

process of registration every time their child visits a website or do you give them a digital signature that they can then use?

MR. JOHNSON: No, the clients we have talked to to date or the prospects we have talked to have thought through either they would verify them once, issue either a digital certificate which gives them the ability to then come back and just use the certificate the next time around, or using, again, a PIN or a password if they don't want to make that leap into this technology, which is a little bit -- you know, I know it's -- we had some comments earlier, and VeriSign is a company we compete with.

The technology is there, it does work. It's not the easiest stuff to deploy, it hasn't been deployed widely, and most people say, Gosh, if I could use a PIN, I know how to use PINs, I've got PIN mechanisms already in my applications, I'd rather use that today.

MR. MEDINE: And then briefly, how practical would it be to deploy the technology and roughly what would the cost be to the parent and the website?

MR. JOHNSON: Okay, our business model is not to charge the end user in terms of the consumer. Our business model is to charge the entity. Now, if they choose to pass that expense down, that's -- that would

be their decision.

For a website that's operating at a reasonable volume, the application I'm talking about here, just the authentication piece, is probably in the, oh, $3 or $4 range, depends on the volume. If there is a dilemma based on what we've heard today, it is very hard to deploy this at a very small volume range. Our -- you know, the work in terms of setting it up and working through the client, and if they have 400 customers, this is going to be a real challenge for us. It's basically designed to be a mass market, very large deployment.

MR. MEDINE: Turning to Kevin O'Neil from KPMG, you might discuss a little bit about the role of intermediaries from your perspective in terms of obtaining parental consent.

MR. O'NEIL: First, by the way of introduction, I'm the manager in the information risk management practice at KPMG, specifically I've been working on privacy services as they're evolving in a global marketplace that we see at KPMG as something reaching across the planet. Essentially we help clients, multinationals especially, dealing with the European Data Protection Directive and not simply a U.S. focus, because our clients really are global players.

Just as a way of introductory remarks here, also

KPMG is an auditor, and at the end of the day, we guard the guardians. If somebody is a certification authority, guess who watches them to make sure that they're following the security practices, et cetera? We're the ones who actually dreamt up the security policies and practices essentially for VeriSign, and so we audit them against those practices to make sure that they do their job as they state publicly to many organizations. So, in our trust model, you have got to have somebody watching those individuals who are issuing these digital IDs.

First, let me provide some context on emerging technology and business model, which could provide a solution, more accurately a framework, for addressing the need, the requirement, to protect and mediate the informational privacy interests of parents, children, businesses and governing authorities.

Myself and others within KPMG and without the firm, our clients, our partners and our competition, see an evolving privacy marketplace, a new hybrid industry with new and old players hoarding a set of innovative solutions, and yet to many companies these are very instructive technologies -- destructive, excuse me. They look at these business models that are being offered by intermediaries, and they find them very

threatening to themselves. Disintermediation is the word that they use.

Okay, I am going to leverage some of the ideas by Clayton Christian (phonetic) in his recent book called The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, and we see this failure occurring right now as companies react to privacy in what we would consider not a strategic mode.

All right, destructive technologies, privacy-enhancing technologies, business models that are innovative opportunities for a few are becoming wake-up calls to those who fail to recognize the intrinsic advantages in adopting these technologies and offer new, interesting digitalized assuring services to protect the consumer's information, is the word.

So, several firms are in earnest pursuit of meeting Christian's exhortation, to look again, don't allow yourself to be blinded by the familiar. Don't fixate on your current clientele, but ask yourself, who or what is driving a new market reality and how do I position myself for this paradigm shift, because shift happens, all right?

All right, a key catalyst to this new market reality is that a global regulatory infrastructure of informational privacy, and more to the point,

informational self-determination rights, are being codified, put into practice in some 50 nations, and with strong ongoing debate as to the definition, structure and assurance infrastructure necessary to protect and enforce this evolving corpus of digital rights and commensurate digital responsibilities.

MR. MEDINE: If I could interrupt you, if perhaps you could just focus your comments specifically on the children's context. Do you see essentially an evolving role for intermediaries or do you see that as not the model in which to --

MR. O'NEIL: Well, as a software designer, there are what are called user cases, and I picked up a little case study. Do you want me to walk through this?

MR. MEDINE: Okay.

MR. O'NEIL: In the digital world -- excuse me, in the physical world, mom tells Jonathan to be home by 5:00. Mom insists Jonathan not to speak to, associate with Mark. Mark just recently instructed his younger friend on the subject of scoring with chicks. Mom did not approve.

Jonathan complains and tells his mother Mark is the best trick bike rider in the neighborhood and he's teaching me some really cool maneuvers. Mom thinks that's not the only tricks he's teaching her son. Mark

advised Jonathan to get a new bike with a new competitive equipment on board. Mom says, Who is this kid pitching a $700 bicycle to my kid?

Now let's go digital. This is an online world. How does mom control this environment essentially that's surrounding her child? Trick bike manufacturer called Cool Bike Manufacturer operates a community of trick bike masters. They host free e-mail, chats and other networking tools to enable kid-to-kid interactions.

In return, bike manufacturer wants to know who's got what equipment, our competitor's, theirs, and other data about children in order to help them design the next generation cool bike. I mean, manufacturers need this information, specifically about children, how they are interacting with this device, et cetera. This is like adult consumer products.

Jonathan also wants to meet someone, as mom has now ordered him to find a new mentor. He wants to meet someone who knows his stuff, is a real master and can teach him and his other aspiring bikers, and he'd like to find who else in the neighborhood he can practice with. Jonathan wants to utilize the community search mechanism to find other kids in the community that have certain attributes.

You see, children sign one another's personal

information agents and they attest to each other's, quote, "mastery of cool bikes," so it's not adults saying that these are kids; these are kids saying to each other are children.

Okay, mom enrolls Jonathan in the community via personal information agent she just got for free from her bank. She has a digital ID from her employer and one from the bank and now sits down with Jonathan and authors his personal information agent. Mom authors some data in governing rules, like your data is come home by 5:00, interaction rules, which says you can only interact with children from your elementary school.

Cool Bike Manufacturer can utilize, according to mom's rules, specifically, granularly, age, height, weight, and the last date he purchased a TRX-3000. And if they want more to talk to my broker, the infomediary, because what I want is some value in return for the use of my child's information.

Guess what happens? That $700 bike is now $535, because she has now just exchanged some information for some value return, and that's what I see the market demanding right now.

I'll just close with that.

MR. MEDINE: Okay, thank you very much.

And then moving on to your neighbor here, Austin

Hill, who comes from our neighbor to the north, Canada, to make it an international forum. We appreciate your thoughts on these questions.

MR. HILL: Thank you, and thank the Commission for having us.

I'm Austin Hill. I'm the president of Zero-Knowledge Systems. Zero-Knowledge, not that we don't know anything, just that we don't know anything about our customers. So, we are a developer of disruptive technologies, mainly privacy. We develop privacy solutions for consumers focused around end user empowerment and the ability to not have to put your trust in a good site or a bad site, a good player or a bad player, but to be able to control your privacy yourself, a parent, a child, and not have to rely on trusting anyone, including Zero-Knowledge.

So, just in hearing some of the comments today, I was reflected at what a pain I was to my mother. I was the child you all dread. I regularly found ways around any rule that was set up. I grew up online, and when I was spending too much time on online, the phone was taken away. I ran a phone line through my window down the basement. I mean, this was a normal course of activity.

So, in looking at these areas, I always

appreciate the innovative nature of children to find a way to get what they want, to be what they want, to do what they want. So, I think the comments today about having to involve kids in making this a fun thing is very, very important, because I also believe that the problem does not just exist on one site.

The problem is not that Disney is abusing information. When we look at privacy and we look at some of the concerns in talking with parents, we look at things like news group, you know, something I say in a news group today as a child of 14 may be there when I'm 28 and I'm going out and looking for a job. So, my opinion on a very, you know, heated issue, political issues, my comments on a web-based chat room, will they follow me forever?

And some of the ideas of using digital identities to digitally sign that almost make the problem worse, because we lose the ability to -- if you want to call it redemption, I certainly went through various stages. If everything I did in junior high was still following me around, getting venture financing to start a business would have been difficult.

So, I appreciated the fact that a lot of my digital communications are gone. I appreciated the fact that I was able to separate myself, and a lot of that

was because I used pseudonyms, and I grew up online and bulletin boards and communities where handles were the accepted form of communication.

I met friends, I made relationships. Some of them I knew who they were in real world, some of them I just knew them in the digital context, and that was a very strong relationship. I was able to gain reputation, credibility, based on my pseudonym, and no one needed to know who I was. It was never, ever asked for.

I sometimes went into bulletin boards where I had to prove certain aspects of who I was by filling in questions, was I knowledgeable in this area, but I provided a handle.

So, Zero-Knowledge is focused around the goal of providing parents and children digital pseudonyms that are untraceable to anyone except the parent. So, even Zero-Knowledge does not have the ability to break the privacy, because we don't know.

So, the way our solutions work is it's installed on the desktop. The privacy is universal. It's for good sites, bad sites, doesn't matter if the site gives off anything at all. It plugs in essentially to your Internet connection and it acts as a local filter to say who are you going to be while you do this, and so it's a

really simple pallet.

I think everyone here has talked about the requirement to make this very easy. I think -- I think that is a very strong lesson.

So, a simple pallet that says, Who do you want to be? Where an adult identity is associated with a password and some of the methods that we've heard from Equifax or other services that can issue a credential that says, This is a real world adult identity, but that real world adult identity can create a pseudonym that allows a child to go online, interact, set up relationships, have persistent and ongoing relationships with people, without ever having to reveal personal information, which we obviously encourage.

Now, at the same time, our product, because we use digital signatures for pseudonyms, in deploying digital signatures, it does not have to verify true identity. You can have a digital signature that verifies this is a child or this is a child with a permission slip or this is Aquaman, the same, you know, child who was here last summer and has come back again to play. Those can exist, and so we deploy digital signatures.

And inside of that model, there is a lot of room for flexibility in adopting what are called credential

mechanisms. Actually, in the eighties, the scientist who worked a lot on privacy systems, David Schoen, who was behind DigiCash, wrote some interesting papers on how to provide authentication and verification without having to give up your privacy, which is something that's been talked about a lot today.

And the way a credential mechanism works, the best analogy, is imagine, if you will, an envelope that has a window and is carbon lined. Inside of this envelope I have my ID, Austin Hill. Now, I can go to my bank, I can go to the Government of Canada, I can go to the driver's license bureau, and I can get a signature on the outside of my envelope saying, "This verifies that this is Austin Hill who lives in Montreal." They verify that.

Now, I can also go to my bank and say I have a credit limit of this. I can also go to another organization and say I'm a member of Blockbuster. Those are all my credentials. Those belong to me.

Now, at the same time I can create a pseudonym for my child, Aquaman, and I can decide to allow a site only to see that pseudonym and the credentials signed by the Government of Canada that says an adult has signed this, and the Austin Hill part is never revealed. I can choose what's shown in that window, and the technology

to allow this is there today.

There's a lot of questions on infrastructure issues and multiple parties getting involved, but those technologies exist, and so I guess if I would encourage everyone here, it's to look at solutions that don't force people to give privacy up, convenience up, again, the goal of trying to get verifiable parental consent, and to realize that in most situations you don't know -- need to know who I am.

Identity is a very, very slippery thing, and when we go online, we have the choice of remaking a lot of this. You don't need to know my address to do business with me online. If I choose to ask you to ship something to me, I will give you my address, or I will give you my universal shipping ID from UPS and FedEx, both of which are on the way in the next year. So, you don't even know the address. You know the shipping ID from UPS or FedEx that I give you.

So, there are a lot of choices in how we develop these systems, and if we choose to make privacy part of it, then I think we can develop privacy systems where people are not required to access that data, and especially in the area of children's privacy, I'm somewhat concerned in the idea, in the infomediary model, where I'm selling my child's data to get better

pricing on something, because I don't know if all parents or all people involved actually are informed at what they're actually giving up.

We saw this with the free PC craze, you know, a $400 or $500 PC, and you have my entire personal information for, you know, five years, ten years? What is that worth? What's the value judgment? And I think we have to look at solutions that are easy to deploy that don't require giving up personal information.

MR. MEDINE: Thank you, Austin.

Taking you back to the children's environment, you've obviously offered a system for allowing children to interact with websites without revealing their identity. You also posed the situation where maybe the child has won a prize that has to be shipped to the child. How does -- will your system facilitate that website obtaining the verifiable parental consent to reveal that offline contact information?

MR. HILL: Yes. Essentially what happens is because the child identity is uniquely tied to a digital credential from the parent, the parent can set the flag to be all communication to my child goes to me, and that can also include requests for personal information. So, a parent can leave the computer, know the child can log in in pseudonymous form. If the child has to submit

personal information, that request would be routed to the parent's pseudonym, and the parent has individual pseudonyms, so the e-mail addresses for each individual are different.

So, the parent could receive an e-mail request saying, Do you want to release this information, and the parent with their digital signature, which would be boot-strapped by some sort of mechanism, whether it's Equifax or the Government -- I think one thing that we have to acknowledge is that the digital certificate infrastructure is going to evolve regardless of child privacy online. I mean, there's currently over a trillion dollars being day-traded online. There is going to be a requirement for digital certificates and proof of identity in those areas, and those same credentials could be used in any one of these scenarios. There are good standards for digital certificates.

MR. MEDINE: Evan Hendricks, you have heard a lot of discussion about where the technology is going through digital signature, intermediaries. Do you think this is the right direction to provide adequate protection for children? Are these the right solutions? Do these go in the right direction towards meeting the laws, requirements, or are we heading in the

wrong direction?

MR. HENDRICKS: I'd like to answer that, David, but first I'd like to thank you for this opportunity to appear before the FTC and to say, people, it's easy to forget the Federal Trade Commission has done more to advance the protection of privacy than any U.S. Government agency in history, and I think it should be commended, and these sort of workshops are part of that.

As someone who has followed privacy since 1977, as a baseball fan, it's almost been like watching me come up through the minor leagues. Just when you're about to get to the major leagues, you came out with last week's report where you did not recommend general privacy laws for adults. So, back to the minors for a little while, but again, you have to commend Commissioner Anthony very much for going straight to the allstar game with the clear recommendation for the kind of rights that all Americans want and deserve.

MR. MEDINE: Of course, we are here in the middle of a rulemaking proceeding, which ought to give you some comfort and warmth.

MR. HENDRICKS: Yes, and all of this is to answer that question to lead to where that rule should go. Yes, what we're hearing is very important, because

you're talking about the goal of protecting privacy is to really be based on the radical notion that information be used according to informed consent, and I think all of these models are very useful, because each one of them is trying to set up a usable model.

Information can be used with informed consent. And because children are involved, I think we need to have an extra special care in making sure that it's verifiable.

I think it's also important to know what's the context of -- that we're dealing in here. It's important to put it in context. I don't know if anyone saw -- since we're holding up books and publications today -- the latest issue of Privacy Times has a story which was on the table this morning about -- we investigated the industry that's selling high school kids' names and addresses, and it's any time you buy a class ring, get your yearbook picture taken, get your tuxedo for the prom, your driver's license, the SATs, all of this is leading to the activity of high schoolers' names and addresses being sold to some companies who specialize in it, like American Student Lists, and some of the companies buying this information are scholarship scam companies.

So, we have a lot of information being collected

and sold about children without their consent or the parents' consent, and I think the lesson here and the context is that if there is a way to make money off of personal information, some companies are going to do it.

Here we're talking about business models. We had this morning versus this afternoon. Quickly I'd like to mention that one U.S. bank had a business model where they were taking people's credit card numbers and selling them and their names to telemarketers, and those telemarketers -- U.S. bank got $4 million plus 22 percent commission, but they also got sued by the Attorney General of Minnesota, and they had to pay back all those gains pretty much as part of the settlement, and they're also the subject of a class action suit.

So, I think it's very important what Kevin said, there is a change in paradigms here, and it's not the technologies always that are changing. It's the fact that people's evolving care about privacy, that what was an acceptable business practice is no longer being looked at that way, because certainly this was something that they thought was okay to do, just like Allensis (phonetic) was the company, for those of us here in D.C., that was getting prescription data from Giant and CVS pharmacy, and as soon as that came to light, the

program was ended, and they too are the subject of a class action lawsuit.

So, these are business models that basically didn't work out, and it's because they were not based on informed consent, which takes me back to why I think I like what I'm hearing here, is that we are talking about implementing the goal of informed consent, and I think when you talk about change -- Kevin's changing paradigm, you know, a stock tip for everyone here is that those companies in the information age that are going to use personal information based on informed consent are going to be the winners, and those that are going to continue to try to use personal information, children's or otherwise, without informed consent are going to be the losers.

MR. MEDINE: Okay, thank you.

Deirdre Mulligan from the Center for Democracy and Technology. Earlier -- I would like to hear your views specifically, but earlier Jason Catlett talked about the Platform for Privacy Preferences as something that will always be a future technology. I was wondering if you could update on, if you are aware, where that technology is headed in your view and if you think that that will offer some solutions as another technological approach to some of the issues we're

wrestling with today.

MS. MULLIGAN: Okay, if I can take privilege, since we only have 15 minutes left, to start with my comments and finish with that.

MR. MEDINE: Absolutely.

MS. MULLIGAN: I really want to go back to first principles for a second. As written, the statute requires parental consent in two radically different contexts, okay? The first, which is what almost everyone has been discussing today, and it's where a website that's operated for children in the commercial context wants to collect something like name and address to deliver something to a child.

Okay, we're talking about potential marketing uses, we're talking about a business collecting information very specifically about a kid, and that requires parental consent, and as Jason said, there's some balancing there about how many false positives, et cetera.

The second is a very different context, and it's the one that I think merits a lot of attention that has not been given to it today at all, because it implicates some very serious First Amendment issues for children, and Austin was talking about the ability to participate using a pseudonym. Underneath this statute, for a child

to participate in chat or e-mail or a bulletin board pseudonymously requires parental consent, because the kid is enabled to disclose personal information. That's the reading of the actual language of the statute.

Now, I think when we look at that, we have to say there are some very different balancing that has to go on, and somebody can correct me if they think I'm wrong, but I believe that everybody who's worked on the statute would agree that that's an accurate reading.

MR. MEDINE: Well, I don't think it's -- our job is really to hear you today, and obviously we will take your views under advisement as we proceed in the rulemaking.

MS. MULLIGAN: Okay. Well, what the statute says is that participation in an activity that would enable a child to reveal personal information to others online requires parental consent, and that's regardless of whether or not the website is actively or passively trying to collect information about a kid.

Now, when we're talking about privacy and we're talking about the goals of this statute, it was actually to minimize the impact on children, to minimize the data collection and to ensure that when it did happen, it was appropriate to the purpose and that it happened with informed consent. I would suggest that reading a

parental consent requirement to require something akin to Equifax verifying a parent's identity and then having another thing that not only identified this as a parent but identified the relationship between the parent and a child in order for a kid to engage in a pseudonymous chat subverts the intent of the bill, right?

And so what I want to suggest is that in order to look at what kind of consent mechanism we're going to use, we can't do it in the abstract. This is not a battle between protecting kids and protecting marketing; that this bill actually really addresses some serious questions about how children are going to be able to use this medium, and I think that we really need to step back.

MR. MEDINE: Does it -- to clarify, are you proposing, then, that pseudonymous interaction between a child and a website be excluded from coverage under the act?

MS. MULLIGAN: I'm actually suggesting that people try to step back and look at this in a context-specific method rather than very loudly declaring a position on one side or the other without looking at some of the serious and very potentially significant interactions that this bill is intended to regulate,, and you know, this is a really serious

activity, and this particular issue, you know, Leslie Harris at ALA brought it up earlier, I don't think we've heard a single comment other than Leslie on this particular issue, and I think this is -- we know that kids, what they really want to do is communicate with each other. Yeah, they want to enter contests, but what they really want to do is communicate with one another, and I think we have to figure out how this is going to impact on that.

To bring that back to the technologies that we've been talking about today, I think Austin was making some very important points. When we talk about digital certificates, when we talk about verifying or authenticating, we can be talking about a whole bunch of different things. We can be talking about identity verification, which is what we were talking about here.

Austin was talking about relationship or identifying that this is, in fact, a parent, and this parent has a relationship with this child, and this parent is allowed to enable this child to participate without the website necessarily knowing anything about the parent or the kid other than they are related, okay? And in the context certainly where the website isn't going to be collecting any other information, they are not going to be collecting name and address, that is

probably a much more appropriate mechanism of providing for consent, because it really minimizes and protects privacy on all ends.

We've heard some -- I'm sorry, and you were similar.

MR. BATYRBAEV: You mentioned on this side, so I wasn't sure who you were referring to, so I wanted to speak to the fact that we don't actually keep any information on the parents --

MS. MULLIGAN: Oh, Equifax.

MR. BATYRBAEV: For instance, the account, bank card or credit card number doesn't even leave the browser or doesn't even travel anywhere, and we really think we struck the medium between the industry concerns and the privacy concerns that -- because we talked to the industry before we devised that --

MS. MULLIGAN: No, I was referring to Equifax.

But when we were thinking about setting up -- you know, there are a number of different models, but some of them deal with where's the information, who's dealing with the information and who's holding onto the information. And we have some centralized system, if you think about AOL as a fairly centralized system, there is one point of consent. This raises a number of questions. Are they collecting transactional data about

everywhere a kid is interacting? It raises some additional privacy concerns.

What are the protections on how that data is used? Are we creating a very detailed, vast pool of transactional data that right now has very little limit on law enforcement access? You know, what kind of pools of data are we collecting if we're talking about site-by-site verifications we're not going to create those same kind of longitudinal profiles that we have in something like an advocate's database?

So, in looking at these there are a whole lot of different questions. I think a lot of this is promising, but there are a lot of questions and they have to be looked at specifically.

MR. MEDINE: I guess again just to come back to the theme of efficiency, one argument is allowing an online service like AOL to gather the parental consent and be the intermediary with websites is an extremely efficient method because AOL can verify that someone is a parent through credit card transactions and so forth and then easily give out or not give out the consent as directed by the parent. You think that's a troublesome model?

MS. MULLIGAN: I don't think it's troublesome. I think that you have to look at it carefully. There's

a model such as you can have -- I issue a certificate and I give it to you and it's useful at many different websites, but I actually don't know where you're using it, and Austin was talking about that. I don't think AOL actually is tracking what different service vendors people are interacting with on their service.

So, I didn't mean to impute that if anyone took that, but you have another -- if you think about the credit card model, it's an authentication device. It proves that I am able to pay for things, but they very actively track everyplace that I use that credit card, okay, and so they have a lot of information about what I'm doing online. So, they're just very different models, and they are very -- they're appropriate or inappropriate depending on the situation.

I think many of us, if we're talking about access to medical records, I want the Equifax system, you know, but if we're talking about my kid being able to engage in a pseudonymous chat, I -- you know, I'm not sure what method -- I think I'd probably rather the service enable me to make sure my kid isn't disclosing information, educate my kid not to disclose name and address information, you know, and monitor. I don't know that I'd want to have to get permission, parental consent, Equifax verification in order for my kid to

participate in a -- in an anonymous First Amendment activity.

MR. MEDINE: So, does that suggest -- lots of comments earlier in the day about a sliding scale for certain -- essentially a degree of verification depending on the kind of information and its use?

MS. MULLIGAN: And the activity. I mean, I think that we're really -- one is talking about collecting data from children for specific purposes, and the other is talking about there's a risk of children if you enable them with a telephone or a modem or an ISP to disclose information about themselves that others who are seeking to do them harm may pick up, and I think we have to figure out how to deal with that in a way that doesn't suggest that every time a kid wants to speak, they need their parents' permission.

MR. MEDINE: Priscilla Regan from -- we will come back to P3P in a minute, but Priscilla Regan from George Mason University. We have heard a lot about developing technologies. What's your perspective on that and essentially how do we force technology with a standard that -- and the statute that requires use of reasonable, available technology?

MS. REGAN: Okay, thank you, David.

I think the one response I have to what I've

heard this afternoon is that it worries me that in order to get verifiable parental consent, we may move to a system where we really require parents to compromise their privacy, and I guess in part here it's that the Equifax system that causes me to raise that concern.

I think we need to remember that in public opinion surveys, as well as in what we've seen in the behavior of individuals, people are reluctant to go online if they're going to compromise privacy, if they have got to give out personal information, and we're trying to develop an Internet where both parents and children are comfortable going online.

The model that the law adopted is one that says, you know, we protect privacy by parental notice and parental consent with the thought that we're trying to limit or, you know, give parents and children control over that flow of information. And I don't think we want to lose sight of the notion that we're trying to minimize the collection of information.

I think the notion of pseudonymous communications is a very valuable one. I think it's important. I think it's how kids tend to communicate online. They like the notion that they're not -- something like that. That's their way of interacting. I don't think kids are likely to give up medical

information online, so the sliding scale kind of approach that was talked about this morning I'm somewhat worried about, because I think that there's some very basic information that has to do with name and address which is what you really want to make sure that kids don't disclose. So, the sliding scale may not be -- may not fit that.

MR. MEDINE: Okay.

Steve, what about -- I guess some of the greatest concerns are about the safety and security of the children. How do these various technologies address that concern?

MR. LUCAS: I should have mentioned when I talked about our Persona product, we do have the ability to provide consumers, both children and adults, with what we consider to be anonymous profiles, more on the pseudonymous. We're looking at providing various levels of anonymity.

One of the concerns that we have is if we provide what is sometimes referred to as factual anonymity, where it is really impossible in most cases to verify who the person was, that we're concerned that we wouldn't be able to provide legitimate law enforcement agencies with information in the case of someone being stalked, either the child or the stalker

themselves.

I can tell you as the former CIO of Excite, had we not been able to do this in several cases, there was one case in particular where we were able, unfortunately post an abduction, to be able to find an individual, but also, we would not have been able to avoid several cases where an abduction was likely.

So, I think we have to balance the technology with the ability to be able to, you know, to be able to find, in the case of a legitimate request by a law enforcement agency where there's a potential threat to a child, be able to identify who that child is, but I agree with the notion that, you know, from almost every purpose on the web, until the point in time when you actually have to commit to a transaction, there is no reason to know who the person is.

It's kind of like when you walk into WalMart. If the greeter greeted you instead of saying "Welcome to WalMart," "Let me have your credit card information in case you want to buy something," I think we would all be upset with that. I think you can use the same analogy on the web. You shouldn't be asking for information unless -- I like the European Data Directory language, you know, information for the specific and unambiguous use of data.

MR. MEDINE: We are going to run until about 4:30 since we started late. Austin and then Evan.

MR. HILL: One point that I'd like to address that I think Priscilla mentioned, as well, in looking at the issue of privacy, specifically child privacy, and then backing up and saying that we want things like parental consent, I think it's important to back up and remember the context in which we're promoting privacy.

This was an internet that was never ever developed to do what we're doing on it, okay? It was never planned to get out of the lab. It just happened. There is no privacy in the infrastructure. There is no authentication in the infrastructure. The packets are not secure. And the amount of information being currently pushed online and the encouragement to just, you know, get online, you are going to miss the boat, do it any way, don't worry, is causing parents to lose their privacy as well as children.

I mean, the GVU study, if it's any indication, shows that, you know, the current preferred method for privacy is lying. Fifty percent of web-based forms, you know, people lie. This is not building a very healthy economy that allows for privacy and accountability and reputation and verification. So, I think we need to go back and look at what role do things like digital

certificates, encryption play, and I can't stress enough the role of encryption.

If the FTC does want to influence anything, they might want to help support some of the moves to lifting some of the current controls on encryption technology that are probably the best tools for protecting privacy, but certainly we've located in Canada specifically because Canada has decided that encryption and protection of privacy is more important to the global infrastructure than restricting encryption, so those things have to happen in the infrastructure, and from that point I think it's easier to look at issues like consent, pseudonyms and the rules that are associated with it, and we can certainly focus on certain parts of the technology.

Deirdre was mentioning, you know, not allowing people to release personal information. That's something we have obviously built in so a parent can say I never want my child's pseudonym to be able to transmit our address or our phone number, and a parent can set that up, and it happens at the local computer. So, it doesn't matter if it's a good player or a bad player, it just can't go out.

But like I mentioned before, I was a bright child, and I would expect any, you know, reasonably

intelligent 13 or 14-year-old to be -- named Bob to be able to type "B dot dot dot dot O dot dot dot dot" to get past pretty much most engines. So, I would think that the real importance is educating our children and making sure that the standard on the infrastructure is privacy as opposed to no privacy, which is certainly not where we're at today.

MR. MEDINE: Thanks.

Evan?

MR. HENDRICKS: Well, I think when I spoke of context I was trying to make the point that there are some organizations that if they can get information on children, they will develop an industry around that and buy and sell, there will be traffic in it, and that's why I feel that the whole point of this, what should come out of this, is the strongest possible rule for verifiable informed consent.

What we're hearing today, most of these are part of a -- well, it's like fraternities. They're Greek letters, they are alpha or beta, and they are promising, and we hope they come into being, but right now we're dealing -- it's futureware. Right now we don't have the mechanisms, so we're still -- to get verifiable informed consent, we are going to have to have some kind of an offline step.

Now, for the issue of chat rooms, I think I agree that kids should -- if parents want to consent to their kids entering a chat room, that should be special consent, but in terms of sliding scale, it should be actually a higher level of consent, because you're consenting to the child entering the chat room, and then you're -- also there's got to be a warning to the parent and to the child not to post information and -- but if they do, they are allowing for a certain risk that if they don't adhere to a certain level of common sense, they are going to do that.

You can't really legislate that, but when you talk about sliding scale, I agree with Priscilla, I think that sounds like dangerously like a slippery slope, and I don't think we want to go down it.

MR. MEDINE: And how do you resolve the view about the strongest protections with the statute's mandate about reasonable verification with the best available technology?

MR. HENDRICKS: Well, technology includes the telephone and the fax machine and the mail and all those things, and it has to be -- verifiable comes first. I mean, verifiable is the operative word in there, and I just don't feel satisfied that in the current context, partly because, like we said right here, that the system

was not built for this. So, to say we're trying to put a round hole in a square peg, so to speak, but basically, no, you need to -- technology includes the technology that's offline, too, and if that's what we have available, then that's what's available.

MR. MEDINE: Oscar and then Deirdre.

MR. BATYRBAEV: Thanks.

I kind of skipped my introduction, and before I became chairman of eOneID.com, I worked in a number of high-tech companies, all in the security projects and PKI projects and so forth, and some of the comments I wanted to give is about the -- how sometimes complex the PKI technology becomes, even for people in a company like Hewlett-Packard. Ten percent of the people called in the help desk when the digital batch product was rolled out just this year from my information.

So, basically the public infrastructure or PKI and digital certificates, like many of the industry members expressed, speaking from my background as a software engineer, although I want to see it widely deployed, is just not widely deployed right now, and there are difficulties, let's say, Internet Explorer IV, even number four, on the Mac platform does not support client certificates.

Now, also, the AOL number three, which uses

Internet Explorer III, does not support client certificates, and there are millions of people who are sitting on AOL-3 client as a means to access the Internet. So, the -- the AOL -- AOL -- the e-mail system which AOL uses does not support signing e-mail with digital signature either, even number four, version number four, and AOL is the biggest provider of online access, as you know.

And it's not only complex, it just also is not supported by the technology, which is browsers. It is supported more and more now, but it's still not widely spread, as the lady from the Library Association was talking about, we don't want to -- and other people, we do not want to preclude people who do not have the latest technology to have access.

MR. MEDINE: So, what lesson do we draw from that if consumers don't have adequate technology and if some of the newest technological developments are highly complex, where should we go in setting a standard?

MR. BATYRBAEV: We should go to a simpler solution. I mean, I -- you know, to give a plug for our company, we do have a simpler solution which does not use digital certificates, which does not use public infrastructure and which also allows companies in the industry to license the -- our technology, if they don't

want to mess with our intermediary role, per se.

We do have intermediary product, as well, in development, which does not use digital certificates or public infrastructure. So, it's like don't try to say that the solution has to -- well, obviously you guys never say that, but the -- it's like if industry and consumers say that the public infrastructure is not yet mature and widespread, then there would be another solution.

There's always a technology solution to any problem if -- given the incentives and so forth like you said, and if one solution doesn't work, then other solution will work, even if it's our example or other companies which may emerge example. And that's -- and also I have heard some comments about 13 and 14-year-olds. I do not think the statute deals with 13 and 14-year-old people. It deals with people under 12.

MR. MEDINE: Under 13.

MR. BATYRBAEV: Well, under 13, yes. So, the sophistication level may be a little bit less, and the -- the notion of most enterprising children defeating certain systems is okay as long as 99.99 percent of children who were not most enterprising will -- privacy of those people will be protected.

MR. MEDINE: I guess we are going to exclude

Austin from that group.

MR. BATYRBAEV: Oh, he is a really smart guy, so I mean the....

MR. MEDINE: Okay, Deirdre?

MR. BATYRBAEV: And I'm not sure what age group he was in when he was doing this.

MR. MEDINE: Probably in the age group we were talking about.

Deirdre?

MS. MULLIGAN: You had asked me just to talk about Platform for Privacy specs. The final spec has not been approved, but there are some people working off of I think the concept of what is behind P3P, and I think if you talk to Steve Lucas, I think if you talk to Austin, so the notion of enabling people to set their own -- make their own decisions and to make sure that they're communicated and to kind of enable privacy in an automated fashion is definitely moving ahead, and I think that, you know, the P3P activity has helped move that direction.

The question is whether or not there's going to be a standard platform, and it's kind of the same question, is there going to be a PKI infrastructure? Well, we all hope so, because a whole bunch of inoperable systems is really not a good end game.

MR. MEDINE: Well, just to let me repeat for a minute, which I guess enables the consumer to set their browser, do you see that as a possible solution to protect children by setting a browser so that you only visit sites that have certain privacy policies with respect to children or use it as a consent mechanism for visiting sites and allowing information to be collected?

MS. MULLIGAN: Yeah, I mean, P3P is a specification, it's not a product, and that -- the same way I couldn't evaluate digital certificates, are they going to be useful here, I couldn't say is the P3P going to be useful here. You certainly could design an application that would be useful in the same way you could design digital certificates that are useful. You could develop a product that I would say no, you know, so it really depends.

But I just want to throw out a scenario, if I might. You asked for, you know, people are saying a sliding scale. I don't think a sliding scale is the right analogy, but I think a context-specific decision about what's appropriate is exactly what parents do all the time, and so, for example, if there is a website that's designed for children and they enable, you know, some kind of chat or bulletin board, interactive

activity, it's fully monitored 24/7, they only allow kids to do it after they have read something and kind of said that they've read it. They don't actually say who they are. It's done with pseudonyms. They are not collecting any identifiable information, and they have actually instituted some limits for the, you know, not the brightest kids on the block, but for most kids, they are not going to be able to type in information.

Do we -- are we going to require a, you know, Equifax version of parental consent, or are we going to go say that there might be some other way because we want the kids to be able to interact? And I think those are the kinds of things that I would hope that the Commission would look at, because I think that they are different than whether or not you're specifically collecting information that you're going to use tomorrow for marketing, you know, that there's just different costs to the kids of those false positives.

Is it I'm not going to be able to talk or is it I'm not going to get, you know, the prize? And I think they're a little different.

MR. MEDINE: Okay. Kevin and then Steve?

MR. O'NEIL: Just a thought, just a -- I went into a restaurant just a few days ago, and I have never noticed the sign, and it was rated B, and it's Persian

food, and I love Persian food, so I eat there at my own risk. It's not an A-rated place.

And I'm just saying in terms of privacy and the trust market that is evolving, can the FTC say instead of a staggered law, could you essentially establish levels of trust and let the marketplace decide where the kids are going to go and where the kids are going to play? But what we're seeing right now is that instead of ISPs, there's an industry called ASPs, application server providers, and they're hosting lots of companies who cannot afford, you know, hundreds of thousands of dollars worth of equipment, and so they essentially subscribe to a, quote, "kosher site," a secure site, and they utilize those services.

Your business model, Austin, could you host a bunch of sites that offer kids, you know, et cetera, and they will -- and you'll be essentially an ASP. You will host these sites, and you'll be the one who will be compliant with the FTC. I mean, there's just a different way of cutting this.

MR. MEDINE: Okay, thanks.

I am going to take the last comment from Steve and then we'll have the open mike session, and Steve, if you can just really again clarify when your kids version might be ready for the marketplace.

MR. LUCAS: Okay, again, an aggressive schedule would be sometime in the fourth quarter of this year, probably more realistic, after going through a series of very strong beta tests, probably first quarter next year.

I just have two quick comments, though. The first is I mentioned that our business model is based on the premise of being able to track using information on the web. We think that's critical. When any information is released on the web, we track the URL, what information was released, whether or not it was an exception, what the stated purpose of the information was used for, the time, the place, all of that information, and the parent can drill down any of that information. So, we think reporting is a way to catch the bad actors, in a sense, along with doing traditional kinds of approaches like seeding databases and other things.

The other thing I would like to mention is the role of access. To me access is critical. It is going to be critical I think not only in the United States but it's clear it's going to be required in dealing with the Europeans. I understand the issues of access of, you know, again, the authentication and the nonrepudiation, but access is one way to solve the problem that Austin

mentioned of 40 percent of the data being falsified, which I think consumers do to provide a false level of anonymity.

If consumers had access to information and they are responsible for data cleansing, the biggest cost of managing data on the web, which is that process, is not eliminated, but it's certainly impacted positively, and the advantages and the cost savings could be passed along to the consumer. And when sites -- when companies say that they can't provide access other than for the authentication of nonrepudiation reasons, I think that, you know, we can deal with it at some point in time.

I find it, to be honest with you, somewhat ridiculous, the reason being is that we can spend billions of dollars to data mine the hell out of consumers, but we can't spend the money necessary to provide basic access? I find that to be a real conflict. I don't understand how that can happen. I propose that if we spent a fraction of what we use in terms of funds to create the data mining applications, we could solve the access problem pretty quickly.

MR. MEDINE: Okay, thank you.

Now, let's -- if anyone in the audience would like to get up, you may just want to be stretching after being here for a long day, but if you would also like to

ask a question.

Okay, thank you. Equifax, for the record, is up and available now.

MS. AFTAB: Parry Aftab, but I'm not commenting as a cyberspace lawyer, so I'm taking that off so Ron can be the cyberspace lawyer for the session. I'm commenting as executive director of CyberAngels and a child safety expert, and Deirdre had commented on chat.

When I see the different levels of parental consent, however we do it, I think the highest level of parental consent has to be in chat, and although we can see adults being able to chat as a free speech issue, I think with children we need to recognize it's a safety issue and that the reason it's been broken into two pieces when the FTC has regulated this is one is deception, people are using information, sharing it with others, and the other is safety, the unfair practices.

And so that even if kids are coming in under a pseudonym, in a live chat situation, not a bulletin board, because somebody can screen the bulletin board, but in a live chat that is not time-delayed, and only Juniornet proposes a time delay and maybe KidsCom -- yes, KidsCom is doing a time delay, but it's very unusual for that to happen, because there's like a five-second time delay and it burns people out in a few

hours. So, time delay is not being done.

It depends on the kids and how well we train them and how well we train the parents and what we have kids do. Often they are sharing information and not realizing it. The name of their school team, the name of their school. A lot of the things they don't realize will allow the bad actors to find them, and in my role in CyberAngels, I help parents when kids have been abducted and abused and I work with the FBI every day on these issues, so I want to be sure that when we talk about levels of consent, that as important as free speech may be to a kid in a vacuum, we need to recognize that safety is a very important issue here, and the parents need to recognize that their kids are chatting, even with fully monitored chat 24/7, that the parents need to recognize that there is a risk there, that certain information will be given by your children inadvertently or unintentionally to someone who is masquerading as a kid on the other side of the chat, and that's just a comment.

MS. MULLIGAN: I am well aware that there are two separate issues here, and the issue is what the statute ends up addressing, because it can't say we are going to ensure that kids don't disclose information to other people when they talk to them. It says we are

going to get parental consent.

Now, is parental consent necessarily going to stop the kid in the chat room from disclosing information about themselves? No, but what we've created is a sense that what we're going to do is hopefully engage parents. I think it's great that we're going to engage parents. I think there is a risk.

There are -- there's a large segment of the population that gets access through libraries and schools and doesn't have computers at home, and if we design a consent mechanism that may not be verifiable, because I don't know exactly what is, right, but is more difficult, more cumbersome, perhaps even it's an e-mail based, but the parents don't have a separate e-mail account from their kids, or it's a fax-back or whatever it is, that we could have an impact on kids' ability to interact, even in the classroom setting where there is probably a teacher there, okay?

And I'm not saying --

MS. AFTAB: I think it's a risk that parents need to talk about and the option is time-delayed chat. We'll talk later, but --

MS. MULLIGAN: But the solution is broader than the potential problem, and perhaps there's ways to kind of nuance it and get at the problem.

MR. MEDINE: This may have to happen offline.

MR. BATYRBAEV: I just want to say that there is a way for parents in our system who do not have Internet access to give their verifiable parental consent whose children do have access from schools and libraries.

MR. MEDINE: Okay, thank you. We are going to have to move on. If you could identify yourself.

MS. CRAWFORD: I'm Susan Crawford from Wilmer, Cutler & Pickering. I'm here on behalf of Juniornet.com, and Parry has mentioned the company a couple of times. We filed comments here, as well.

Part of the session is devoted to talking about alternate business models. Juniornet.com is a subscription-based service that asks for advanced consent based on credit card information, monitors chat rooms and provides terrific content to kids, including Highlights, Sports Illustrated, and the message I'd like to bring is that parents are extremely interested in the service, and early acceptance is high.

So, parents are willing to pay for good content associated with a safe online environment. It looks like the Internet, but you don't have access out to the rest of the Internet.

MR. MEDINE: Thank you.

MS. RICHARDS: Hey, Jeff Richards, Internet

Alliance. I'll be real quick.

As a former epidemiologist, in our discussion of false positives and negatives here, we should be really careful not to strain an analogy. In fact, it's really important to us. It's really important not to have parallels. You used to have to kill a rabbit to do a pregnancy test or to see if someone had syphilis, and that was a very high standard. It was a very sensitive and specific test and required gruesome things done to animals.

The tests that are available now, including home pregnancy tests, may not be as accurate. Consumers may have to be educated on all of those issues, but there's clearly a marketplace demand and educatable adults who can deal with things.

Now we're talking about children and how will you test our methodology. That's where I think we should really go, is how we test what we do, how we look at choices. Medical testing today more and more looks at the realm of choices and affordability, so that the total picture can be made available and accessible, which are issues I think we're very much talking about here today. So, I caution us, be careful about extending that analogy too far.

MR. MEDINE: Thanks.

Just again to reiterate Lee's comments earlier, that we would be happy to receive submissions during the comment period on the proper approaches and the methodologies to be used to assess the level of protection here.

MS. CATLETT: David, could I just add here, I was not advocating cutting the kids in half.

MR. MEDINE: Okay.

MR. IZRAK: Mark Izrak at bizrocket.com.

I hate to bring this up this late in the day, but I think there's a whole side of this that isn't addressed, and that is that how do the parents know if the site is a good site to enable -- that they would enable to have that information? And that's what we're trying to offer, because we have a search engine that's tied to a public forum, and what the public forum allows is anybody to go in and tie to any URL any comments, compliments or file complaints that we help to resolve with the other side, with the website.

So, this gives a forum for people to be able to go to to check and see what other comments have been placed about this particular site before they go and say, Okay, I want my child to have -- I want my information available to this site to do with what they want to do with it.

MR. MEDINE: Thank you. We haven't obviously touched on the notice provisions in the law as well as all of our consumer education responsibilities.

Yes?

MR. MENGE: Good afternoon. My name is Eric Menge. I'm with the U.S. Small Business Administration.

Regardless of what the FTC finally comes out with in its final rule, whether it's sliding scale or alternate technologies, one thing that's clear to me is it's going to impact thousands and thousands of web pages and potentially thousands and thousands of small businesses, and because of that I think the education is a crucial part of this, that regardless of what the FTC finally comes down with, that they need to let the small businesses that will be impacted by this rule know.

There is a section as part of the Small Business Regulatory Enforcement Fairness Act, SBREFA, Section 212, which requires a federal agency prepare a compliance guide, which is an easy-to-use, clear and plain language guide to nonattorneys, nonlawyers, people that aren't here in this room today, that can know what exactly is required, what isn't required, whether a pseudonym by itself is okay.

I think we already had that question earlier

today, but that's the sort of question that would be answered. So, I just wanted to encourage the FTC to look into a compliance guide whenever it completes its rulemaking.

MR. MEDINE: That's an excellent suggestion. We do that, of course, in other areas and we would be happy to work with the Small Business Administration to prepare those materials.

MS. CLARKE: Jorian Clarke from Circle 1 Network.

One of the things we need to think about are long-term impacts of the decisions we'll be making. We're here in Washington having a debate about the impact of violence in entertainment and we have seen recently in children's behavior in schools. When my son was growing up and he broke the baseball -- broke the window at school with his baseball, I didn't encourage him to go to the school and tell them Aquaman did it. He -- it was important for him to identify himself and take responsibility for his actions, and so I think we have to look at pseudonyms and anonymity and try to decide what will be the impact long-term for kids.

MR. MEDINE: Thanks.

And the final comment?

MR. CASTRO: Seeing as I'm the last person

standing between you all and dismissal, I'll try to be as quick as possible. My name is Luis Castro. I'm with a company called smartgirl.com. It's a website for teen girls, it's an advertising-free website for teen girls. All the content on the site is by the girls who visit it. They fill out surveys and do reviews on products, issues that are of interest and of concern to them.

I wanted to first of all just say I appreciated the comments that were made today around a couple things that were important to us. One was the idea of looking at the context in which information is used and the context of the site itself. We think that's important, because the information, any information we collect is not provided to third parties. It's for, you know, newsletters, it's for message boards. So, I think that's an important thing to take into consideration.

I also appreciated the comments about making sure that we don't trample other privacy issues or the privacy rights of others, parents, for example, in making sure that we're protecting the privacy of children, as well.

A final thing I just wanted to touch on was our demographic is 12 to 19, so we're one of those sites, like others out there, that the predominant demographic of ours is not under COPPA, but we do have visitors who

are, and we have situations obviously where we would have a check box for kids who are under 13 to check so that it, you know, we need to collect information from them. They would need to get parental consent.

My question is, our liability when a child who is 12 years old decides to pretend she or he is 13 years old and what if at some later point it's found out that this child actually is 12 years old and has come into a site or into our message boards which is for 13-year-olds, how responsible is the site for that fact?

MR. MEDINE: Well, the law does have some -- without giving an interpretation, the law does have some provisions that address reliance, reasonable reliance on what the child visitor tells you on their visit to the website, on a site that's not directed to children.

Good, thank you very much for your comments.

I'd like to re-introduce the bureau director -- first, thank you all of the panelists for engaging in interesting discussion, which will be very helpful to us.

(Applause.)

\- - - - -

CLOSING REMARKS

- - - - -

MR. MEDINE: I'd like to re-introduce the bureau director, Jodie Bernstein, for some closing remarks.

MS. BERNSTEIN: Thank you very much, David, and let me be very brief, of course, but first of all I want to thank all of you for coming and participating. As I said initially, this has been a very valuable process that we have used in the past, and I think this one was maybe because all of you have participated in others, we've all gotten better and better each time, because it truly was a learning experience for me and for our staff and hopefully for all of you.

And while I'm at it, let me, as I often do, I'd like to give all of our staff a nice big fat bonus like all of you do when your stock goes up, but we don't have any stock yet. Hopefully --

MR. KAMP: IPO.

MS. BERNSTEIN: IPO for the FTC, how about that?

UNIDENTIFIED SPEAKER: Spin off your website.

MS. BERNSTEIN: Now you're talking. It's very good. It's very good.

Well, short of having a bonus for my folks, how about -- this group did a phenomenal job, a round of applause.

(Applause.)

MS. BERNSTEIN: And I do appreciate the number of folks who I presume voluntarily said what a good job the FTC does on listening to the public and on trying to inform itself. That will be in the record, so we can take some credit for it. So -- and I only had one other sort of smartass remark to make, because I always like to have one, and that's for Evan, and I guess -- I couldn't resist it. The Privacy Times giveth and the Privacy Times taketh away, but we appreciate it.

I tried to tell the Chairman what your analogy was to the baseball, because I was just in there, but I blew it all together, so you'll have to write it down for me in order to make it.

MS. AFTAB: It's in the transcript.

MS. BERNSTEIN: Somebody else explain it to me and then I can explain it to the Chairman, good.

MR. HENDRICKS: It was a real homerun.

MS. BERNSTEIN: That's good enough. That's good enough.

I think there were some kind of consensus views that emerged today, and -- but I should mention, again, this is a rulemaking, it is on the record. We had two commissioners with us today for a good part of the day. They're not here right now, but, of course, it's a decision-making process that we're engaged in, which is

somewhat different than other workshops that we've had where -- where we could be, I suppose, more -- more informal in the way we go about making decisions, but I think -- I think it worked very well today, and I know that they both mentioned to me that they felt very well informed.

So, a few conclusions that I think emerged. One, and this is not a terribly serious one, but I think all of us are convinced of the innovative nature of children, which I think is an important general concept to keep in mind. One of my folks was busy confessing to me today about taking money out of her mother's purse but not taking her credit card out. So, we know that there are lines to be drawn about the innovative nature of children.

But more seriously, one that I thought we had -- I heard with anonymity was given the rapid growth of Internet related products and services, which you all agreed on, the rule should be flexible enough to encompass new consent mechanisms as they emerge. I think we all agreed that the technology is changing, it is emerging, the new mechanisms are coming and we need to be hopefully as flexible as we can so that they can be encompassed.

Secondly, that there is a need I think and a

desire for products and services that will help entrepreneurs and who are often small business to obtain parental consent at a reasonable cost. Another issue for small business seemed to be that we need to consider educational opportunities for them to know what the rule is and how to comply with it without -- without stating how we might go about doing that. We have done guidance documents or informal pieces in the past for that very purpose, and I think we would certainly give that a high priority.

Another point, there's a wide variety of e-mail-based mechanisms ranging from click-back e-mail to e-mail with a digital signature, and I thought there was a consensus that each should be evaluated separately for compliance with the statute.

Certain activities I thought we heard, for example, participation by a child in a chat room or disclosing data to third parties, require a high level of assurance that the person providing consent is the child's parent and they warrant greater protections than other activities. I think that's a very important one, and I think I heard a large measure of consensus around that point.

We need to educate parents and children about the tools that are available to protect children's

privacy so they can be partners in the consent process. And finally, and this is an important one for us, application of the rule will continue to be an interactive process, both interpretation and application, and the FTC will depend on industry, consumer groups and others to educate it on new and developing technologies, available consent mechanisms and how the rule is working in practice.

I thought each of the panels were very instructive today, and certainly the first one, which told us what was happening now today was as important as the remaining two. Each of them made major contributions, I think, to both the record and to our learning process. So, we will continue this interactive process that we have engaged in.

I would urge you all to remember that the record -- that the record will be open for further comments until July 30th if you wish to file additional comments and to continue your own interaction with our staff, who are open to listening and to answering questions or comments as you may have.

Again, our thanks. Look, it's ten minutes to 5:00. We could run a happy hour, I suppose. I don't want to hit up anybody for that.

So, again, our thanks, and we'll see you all

again, I'm sure, in the future.

(Applause.)

(Whereupon, at 4:50 p.m., the hearing was concluded.)

- - - - -

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: P994504

CASE TITLE: CHILDREN'S ONLINE PRIVACY PROTECTION

HEARING DATE: JULY 20. 1999

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: 7/21/99

_____

SUSANNE Q. TATE, RMR

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 VANCE