

>> Mamie Kresses: Okay. Let's go ahead and get started on the Parental Verification panel.

>> Male Speaker: Parry.

>> Mamie Kresses: Should I yell at Parry?

>> Phyllis Marcus: Our leader's in the back?

>> Mamie Kresses: Yell at Parry? So, this panel -- panel 4 -- is kind of a COPPA specialist panel. Many of you, perhaps, have never had the joy of considering all the different methods of parental verification and looking at them closely and wondering what works and what doesn't. But what we'd like to do is take a little bit of the panel, the start of the panel, and go through the methods that have been outlined in the Rule. They're not exclusive. The rules never are meant to confine anyone to those methods. But talk about whether they're being used, how they're being used, are they effective, and do they still make sense. And then move into considering other potential methods and the pluses and the challenges of potential new methods. So, in this regard, also, we really would encourage audience participation and questions, and we'd also encourage ideas. So if you've been thinking, "Why hasn't anybody ever thought up this perfect parental verification method, speak up. Okay. Oh, let me introduce the panel. Sorry. Okay. To your left, we have Jules Cohen, who is the Senior Trustworthy Computing Specialist with Microsoft. We have Rebecca Newton, who is the Chief Community and Safety Officer of Mind Candy, Inc. We have Martine Niejadlik, who is the Senior Director of Risk and Business Intelligence at BOKU, which is a mobile-payment system. And then over here, we have Alan Simpson, who is the Vice President of Policy for Common Sense Media. And Ron Zayas, who is the Chief Executive Officer of eGuardian. And then Denise Tayloe, who is President of Privo, Inc., which is -- has one arm of Privo, Inc., which is a COPPA safe harbor. Okay. So, let's... Okay, so, just to take a minute to look at the verified parental consent requirement of the Rule, and there is a general standard which is basically that operators must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. And that requirement -- the methods have to be reasonably calculated, in light of that technology, to ensure that the person providing consent is a parent. And then on the other side of the slide are the methods that are laid out in the Rule and,

again, were not meant to be exclusive but were deemed to meet those requirements. So, here we are, however many years later, and the online world has changed a lot, and the offers -- there's a lot more potential things out there, so we want to look at the old and see how they're working and then look at the new. So, let me start with Rebecca Newton, and I want to start with the "email plus" standard. And "email plus" -- the Rule designated that where the collection of information from a child was only for internal purposes. So it was for purposes of the website or the online service and not to be shared with third parties or to be publicly disclosed, either by the website or by the child. But that was -- At the time the Rule was put into effect, that was considered a less-risky, a less-disclosing method of taking personal information. And so the Rule carved out an exception that where the information was only to be used for internal purposes that one could send an e-mail to the parent with notice, allow the parent to confirm by e-mail that they had received the notice and that they were consenting, and then to follow that up with either another e-mail, a phone call, or a variety of other options. But this was not considered an adequate method for situations where personal information would be disclosed publicly. So, with that, Rebecca, does "email plus" actually meet the standard of ensuring that a person providing consent is the child's parent?

>> Rebecca Newton: Well, that's a tricky question. But I think, as well as any of the other, it meets any of the other standard. You never know that it's really a parent, and I haven't done any of the science behind this, but just from being in this business for 16-plus years, I think that it's fair to say that a percentage -- I don't know what -- I can't be accurate about the percentage -- of the registrations are kids, using their e-mail addresses or possibly putting in their parents' e-mail address. But I do see, where I work now, a fair amount of bounce-backs. These are e-mails that aren't legitimate, that say things like mymom@herwork.com. [Laughter] And so they want to -- I see a fair amount of that every day, and so that sort of speaks to Dr. Gwenn's point about they want to tell the truth. A certain percentage want to do the right thing and want to tell the truth. So it's as valid as, I think, as any of the other methods.

>> Mamie Kresses: So, in your -- Hold on. Is this one working?

>> Phyllis Marcus: No, this is the --

>> Mamie Kresses: Oh, that's the one --

>> Jules Cohen: It was.

>> Phyllis Marcus: No, it was working.

>> Mamie Kresses: Can you hear me?

>> Male Speaker: Yeah.

>> Mamie Kresses: No one's ever accused me of being really quiet. So, in your experience, then, has "email plus" -- do you think it has the same assurance of actually reaching a parent as any of the other -- as the other methods in the Rule?

>> Rebecca Newton: I think it's as valid as the other methods, yes.

>> Mamie Kresses: And so let me turn that, then, to Alan. Do you have any experience from the parents' end and have any knowledge of the effectiveness of "email plus"?

>> Alan Simpson: Not directly, but I'd echo Rebecca's point that the standard may be a little too high recognizing that we know that kids will cheat the system, in some cases but that a lot of kids don't want to. I mean, the whole point of verification is obviously making the best effort that we can, and there's no such thing as a perfect effort. We do get a fair amount of parent feedback on our site around "What my kids are doing that I didn't know about." So that's not a direct aspect of "email plus." It's just more a matter of the challenge that all of these technologies and all of these approaches will face.

>> Mamie Kresses: And so we wanted to touch on "email plus" first because "email plus" has had a long history. It was supposed to be a very temporary solution, and we extended it because we didn't come up with other technological choices that worked with the same ease as "email plus". And then we ultimately, in our 2007 report, said that "email plus" would be a permanent standard

for the foreseeable future. And so it's interesting what you're saying, Rebecca. Do you feel that the -- Would you say that "email plus," if it has the same reliability as other standards, do you think that it still makes sense that "email plus" is limited to -- for internal uses.

>> Rebecca Newton: I think -- I mean, I just am probably gonna say the same thing over and over. It's as valid as the other I think it's -- Yes. I think it's as valid as the other methods, and I think it still makes sense. Unless we adapt available technology to and take a whole different sort of turn on this and get -- go for real parental verification as much as we possibly could, it's -- Otherwise, there's no -- It's the most valid thing we have, other than available technology, which is out there now.

>> Mamie Kresses: Let me ask a slightly different question. Jules, actually. Do you have any experience from Microsoft on whether or not -- how consumers -- not just parents but computer users, generally. How do they view the distinction between internal uses and external uses?

>> Jules Cohen: You know, I don't -- I don't have good data to suggest that they think about them differently or they think about them one way or the other. I would note that I think it's a valid distinction, because in the internal case, you have one org holds the data, and they'll have stewardship mechanisms to manage the data. In the other model, where it leaves the org and it leaves whatever stewardship mechanisms exist, you have much, much looser reins on what happens with the data. So, as policymakers, we're thinking about sliding scales for different kinds of risk. This distinction seems to map pretty clearly to two different kinds of risk.

>> Mamie Kresses: Mm-hmm. And actually, Denise, I wanted to ask you, too, from your experience with Privo, whether or not you -- following up on what Rebecca said about "email plus" and whether it's a reliable method. In your experience, do you have a comment on that?

>> Denise Tayloe: Well, I would say that I respectfully disagree with Rebecca that it is as good as the other methods. I don't think any of the methods are perfect, as Alan just mentioned. But if the goal is to use reasonable methods in light of available technology, and 10 years later, the best we can do is send an e-mail to a parent that a child provides us and get a click-back, I would say that

we -- industry -- haven't done a good job of adopting new methods, creating new methods, and that people are heavily relying on it. So, that's one thing. The second is that if you're supposed to be reasonably assured you're dealing with a parent, I would say that most of the methods don't do that, and that "email plus," in no way, even allows you to say you're dealing with an adult. So, yes, kids have credit cards, but most don't. Other methods that are available that we're gonna discuss later will help to do identity verification to at least know that you're dealing with an adult so you can make the leap of faith that it's like to be a parent who's asserting that child. So my thought is "email plus," as an industry, we need to start moving away from it and find other methods, and the quickest method that I see is let a parent short-code a message back from their cellphone and use that as the mechanism, as opposed to clicking a link. Let a child give a parent e-mail. If they don't have a parent e-mail, more kids know their parents' cellphone than know their parents' e-mail address.

>> Mamie Kresses: And do you think that doing that SMS type thing would give you more assurance that it's a parent or the same as "email plus" or less?

>> Denise Tayloe: I think it would give you more assurance that you're --

>> Mamie Kresses: That's because --

>> Denise Tayloe: It's not the kids' -- I mean, kids absolutely have cellphones, but at least there is a cellphone tied to a parent somewhere in the -- or, tied to an adult somewhere in the path. And you can tell whether or not the short code's coming back from a Verizon or a Sprint or an AT&T versus, you know, a throwaway phone.

>> Mamie Kresses: Phyllis.

>> Phyllis Spaeth: But how do you know that it's coming back from a parent, as opposed to a random child?

>> Denise Tayloe: Yeah. Well, I would just say that you have absolutely no assurance with an e-mail. You have a little -- At least we're moving up the scale versus sort of staying and waiting for it to be perfect.

>> Phyllis Spaeth: Denise, I have no quibble. In fact, I think "email plus" is --

>> Denise Tayloe: It's a joke, and everybody knows it, yeah. Yeah.

>> Mamie Kresses: Was that clear? [Laughter]

>> Denise Tayloe: But it's good enough for internal use right now. I mean, we're not trying to get the kids over the border. We're trying to let them know when the next Nintendo game comes out or something.

>> Mamie Kresses: Okay. And so let me turn to Martine. Martine operates BOKU, which is a -- It's a mobile-payment system. So this might be sort of a loaded question, but if "email plus" is a sufficient method to -- assuming, for the moment, that it is a sufficient method to get permission for internal use -- does it -- should the standard for a simple method be limited to e-mail, or are there other equally facilitated methods, besides e-mail, that would work for these purposes?

>> Martine Niejadlik: Hi. Let me just say a couple things, I think. First of all, prior to BOKU, I was actually at PayPal, and I used to manage risk detection for PayPal. And when I think about laws and the Internet, the first two words that come to mind are "scalability" and "global." So, is it global, and is it scalable? And if we're going to have rules that apply to the Internet and enforce those on these companies, now think about every country also having different rules, which is something we're dealing with right now. It's got to encompass both of those things. Now, I think "email plus," I would agree, is not as strong as some of the other methods, but when you sort of intersect practicality with safety, you know, it's really one of the only ones on the list that I think is a viable option for people. So I don't know if it's an appropriate time to sort talk about mobile -- what BOKU is doing --

>> Mamie Kresses: We'll get into it. But when you have to mesh practicality with safety, what do you mean by that?

>> Martine Niejadlik: I mean something that's completely automated, right? Where a human being is not getting on a phone with a parent, is not looking at a fax machine, is not -- Something that does not require human interaction, that's completely automated.

>> Mamie Kresses: Okay. Does anybody have any other -- We're just trying to touch slightly on each of the existing methods so we have time to go into other things. Does anybody have any other observations or question on the "email plus" method, whether or not it should be limited to internal uses only, whether or not it works, whether or not it's time for it to go, as Denise would say. Anybody have any comments? Yes, Parry?

>> Parry Aftab: I'll be loud. [Laughter] I'll be loud -- The mike. I think we need to recognize the practicalities of all of this. And as you know, we've been in this space forever. So, as you move out of "email plus," and Denise and I, I think, will disagree on this one, because it's a great way of getting parents out there to do something. They're uncomfortable with credit cards, and a lot of people in this country don't have them. And I don't want to lock children whose parents don't have credit cards off of the Internet. So they don't know what a fax is? So they -- Licking a stamp is just beyond everyone. The kids on to a new site by the time a letter arrives. Unless you can find a new way of doing this -- And "email plus" works. Right now, it works. Easy way in, easy way out. It could be automated. And so when you've got 8 million, 10 million, 12 million users in a kid's space, it allows you to do something. But we need to recognize it may not be time to kill it. It may be time, as we start looking at this, to expand it.

>> Mamie Kresses: And by that, you mean what?

>> Parry Aftab: I think as we start looking -- You know, the whole sunset provision -- we thought this would be out there for like two and a half minutes. But the reason it's still there is because it does something none of the other ones did. So, when we move from \$45 a kid to \$15 a kid, do you cop a compliance on verifiable parental consent, and parents just aren't doing it unless the kids

pretend to be their parents. We need to find something the parents will do. Parents will send an e-mail. And so we need to find that maybe there's a way to expand it so it's even beyond where it is on something that's a bit more verifiable.

>> Mamie Kresses: Okay. And I think Gwenn has a statement or question.

>> Gwenn Schurgin O'Keeffe: I just wanted to echo quickly what Parry said. I was about to say the identical thing, so I'll just truncate it really quickly. As somebody who also talks to a lot of parents and sees the technology gap, parents, Denise, I agree with most of what you say, but texting just won't work right now with today's parents because there is a huge technological gap in this country that we just simply have to embrace. We have to embrace it, we have to hug it, we have to notice it, we have to name it as the experts, because you know what? Parents don't text. And you know why? Because they're barely on the cellphone themselves. We have a lot of parents in this country who don't even own cellphones themselves because they can't afford it or they just don't know how to use it or they're intimidated by it. But they do use e-mail. Every parent in this country uses e-mail, even the unsophisticated ones. So let's not make this into more than we have to. Let's keep it simple. I do agree that someday we need to go to other technologies, and I love texting myself, but I'm with Parry on this one. I think we need to go the e-mail route.

>> Mamie Kresses: Okay. Let me go to Shai, and then I will go to Amanda, and then I will go to you, and then we'll move to the next topic.

>> Shai Samet: Okay, so I'm gonna agree to disagree. I'm going to agree with Parry. I'm also going to disagree with Gwenn to some degree. I think -- By the way, Shai Samet. I run a privacy consulting firm, and I've done a lot of work on COPPA over the past 10 years. I think "email plus" has served a very beneficial purpose. And somewhat unrelated to what the law actually requires, what we're finding is that many of the kid-friendly websites, especially those for younger kids, who have designed their chat functionalities so as not to allow personal information to go through, are still using "email plus" to notify and get parents involved with the fact that their kids are using those sites, and that's an extremely valuable benefit and I think one that could carry easily carry over to SMS. I don't -- I'm a parent. I have four kids, all under the age of 13. And I own -- I use

my cellphone. My mother only uses her cellphone. Doesn't use e-mail at all. So I think we'd have to look at that data more closely before we determine whether or not SMS is a viable mechanism. It is true that kids know their -- My daughter knows my cellphone number. She does not know my e-mail address. But then again, also, the fact that she doesn't know my e-mail address usually requires her to call me to the computer and say "Hey, dad, what's your e-mail address?" and through that, I get involved, as well. So there's a lot of mixed data out there and a lot of opportunities here, as well. But to get rid of "email plus" would be a very dangerous proposition, especially given its benefit for those sites that are using it.

>> Mamie Kresses: Okay. And somebody said "data," so, I think, if we can pass the phone to Amanda...

>> Amanda Lenhart: I'm Amanda from the Pew Research Center. And we've done some research on how teens and parents and families use mobile phones, and, in fact, in many cases, families are more likely to have a mobile phone than a computer -- in fact, particularly with low-income families who often do not have a computer at home or who have a highly shared computer. But they do have mobile devices. And so again, this begs the question, of course, whether these kids are gonna be going on websites and whether, if you don't have a computer in the home, whether you actually necessarily need to be able to deal with some of this verified parental consent. But parents are actually more likely to have cellphones than other adults. They're more likely to use them to text their kids. So, they don't always know how to text. There's a substantial subset of parents -- about 25% or 30% -- who don't text at all and don't know how to text, and so they don't use that. But a lot of parents are actually drawn into texting by their children. Also, parents of younger kids now are in that generation of people who actually do text and actually text more than older adults. So I wouldn't totally eliminate text-messaging and SMS as a potential way. I would add it on. I would not substitute.

>> Denise Tayloe: Yeah, it's about options. I certainly didn't mean to say one. I'm all about providing options.

>> Mamie Kresses: Okay. And do you still have --

>> Male Speaker: Nope.

>> Mamie Kresses: Nope. You're all done. Okay. And way in the back, and then we'll move to something else.

>> Male Speaker: I think Parry's onto something. And I think we should definitely be keeping "email plus" as an option. Recognizing that there isn't really any way of authenticating anybody online, I think we should be at least exploring the possibility that lots of companies -- mine included -- are starting to get the opportunity to have multi-factorial ways of making educated guesses about who people are online, what their ages are, what they're up to, et cetera. And it seems to me that the FTC would do itself a great deal of good to allow for continued exploration by companies into this area because I think you'll actually find that companies will have the opportunity to do more verification in the future.

>> Mamie Kresses: Well, and just to kind of build on what Tim has said, we do interpret the general standard that you see up on the slide as the baseline standard. And so the methods that satisfy the rule are illustrative. Only, they are not meant to be exclusive. And the general standard does provide for the kinds of exploration that you've suggested. Now, it might be, and we'll certainly talk about this, that people are too nervous to try something other than which is set forth in the Rule. But, you know, we have to meet this baseline standard, that we have to at least try and ensure that it's a parent. But it wouldn't be meant to preclude exploration. I mean, it is any method, reasonably calculated, so it was never intended to be an exclusive, you know, list. So let me know to Peter, and then let's --

>> Ron Zayas: Mamie, if I can just intersect for one second. The thing I think we keep missing here is that the intent is to get parental consent. And that seems to be very absent from the net effect here. There is no way to verify that it's a parent. There is no way to verify that the kid isn't making the address up or doesn't know the address or whatever the case may be. I think phones are a great way to do it, but nonetheless, if the intent here is to get verifiable parental consent, the fact that a system works but doesn't do that means it's not a very effective system to use.

>> Mamie Kresses: Okay. And, Phyllis. You already had a turn on this one. You gave up your turn, but we'll let you go anyway.

>> Male Speaker: I was trying to be efficient. [Laughter] Going back to the point you just made about being conservative. I advise a lot of companies in this space, and I would never advise one of my clients to do anything beyond what is on the list, for fear that it wouldn't be acceptable. I mean, to say -- Because the standard says "to ensure that the person providing consent is the child's parent," and that's the point that was just made. And living up to the "ensure" is virtually impossible. But it's really impossible, outside of the six things that are there from a legal standpoint.

>> Alan Simpson: But aren't we all kind of agreeing that the six things there don't really ensure...?

>> Male Speaker: Yes.

>> Male Speaker: It's the whole point. I'm agreeing with you that those don't work, either.

>> Denise Tayloe: Liability protection.

>> Male Speaker: But from a liability perspective, for my clients, at a thousand bucks a pop, I'm not going to tell them to go beyond that.

>> Mamie Kresses: Okay. Let's do this. Let's move on to the other existing methods up here, and we'll try to go through them fairly expeditiously. So, it is not a rhetorical question, but I want to know if we are seeing people still using the print-and-send method or an equivalent of that, or the print-and-scan. We, a couple years ago, Phyllis and I, revised our website -- the agency's COPPA website -- to... [Laughter] ...to say that we would recognize a scan as a print-and-send, obviously, in the modern world. But, Denise, in your experience, is that a format that is still being used, and why or why not?

>> Denise Tayloe: Okay, so, yes, some people use it. If you try to use it as your sole method, you'll fail, miserably. If you only offer things like credit card, you'll scare the bejeebus out of people, and they not having choice to do something less personal is a problem. So, here's my experience. We offer five methods as a sort of standard -- last four digits of social, driver's license, credit card, print-and-send, whether a fax or in the mail, or a phone call, and consistently, we get about 7% that will choose phone and a print form, 82% that'll choose last four digits of social, 'cause it happens in nanoseconds, it's automated, and then the credit card is very low -- 4% or 5% -- driver's license low because it's just hard data to get. So, I would say that I would not want it to be taken off the table, because I think that if I'm looking at choice, and the fact that I can do something offline, makes me feel more comfortable, maybe, about choosing something that's online or that's automated.

>> Mamie Kresses: Okay. And just so we are all on the same page, when you collect the last four digits of a Social Security number, what other information do you take from the parent to make that work.

>> Denise Tayloe: So, it's up to the relying party's site that uses the service -- what level of assurance they want, the minimum data that you need in order to decide whether you've got an identity is last name and last four. But typically, a parent account is a first name, last name, a zip code, a date of birth and the last four. And then, of course, just like credit cards, the last four are not retained. So you hit the data aggregator, you get data back, we pine through. If we can find a match, then we process a pass, we flush the last four -- we're left with a parent account that has an e-mail address associated. So from that point forward, the parent can permission off of their e-mail.

>> Mamie Kresses: Okay. Thank you. All right. And then let's go to credit-card use, too, and then we'll go into some new methods. So, Jules, do you know, to what extent in -- Well, let me ask this to Rebecca. I think this would be better for that. So, Rebecca, to what extent is the credit-card method being used for verification, and also, so we can think about both issues, is it being used the way the rule contemplated that it has to be used, in connection with the transaction rather than just as an identifier?

>> Rebecca Newton: Well, we don't use it, so... [Chuckles] But I went out and did my own research, and I went on the 11 top kid sites. And out of those 11 sites, four used -- four demanded or required fax-back or -- that's what we call it -- print-and-send for a required credit card or some kind of a membership transaction. Three of them used "email plus." Nobody used the digital cert or toll-free. So, I mean, I think it's just that -- I'm just gonna be singing this same song. It's as -- I see a lot of credit-card fraud every day on our site -- a lot -- and it's kids taking their parents' credit card and also people buying credit cards online. So I think it's just as -- It's used, but on some of these major sites, four the top 11, but I think it's not as any more valid than any other site. And the one point I want to make is that it -- I think it also, in a lot of cases, for kids, it forces them to lie about how old they are. And so, you know, we know that that's something we talked about this morning, and that's true with a lot of these methods. But in my opinion, "email plus" doesn't force as much lying as the rest of these methods, in my observation, as well.

>> Mamie Kresses: Okay. And does anybody on the panel -- I'll throw this out to anybody -- have a thought on -- well, I think what you've said probably goes to this -- but whether a small transaction fee in connection with consent is something that parents are comfortable with or not?.

>> Denise Tayloe: It's what Yahoo! does. If you identify yourself as 12 and under, they process, I think, it's 50 cents. They take the transaction fee out, and they donate the rest to NCMEC. Now, for a number of years, they were just doing an algorithm to see whether or not it was a MasterCard or Visa number which didn't have a transaction, and I don't see as many people doing that now. And, Jules, what do you guys do at Microsoft? Don't you use a credit card?

>> Jules Cohen: We use a credit-card number today.

>> Denise Tayloe: Yeah. And I agree with Parry. There's 50% of them -- There's some huge percentage of parents that don't have credit cards, and it's a tough method if it's the only one you give people.

>> Mamie Kresses: And are you -- Do you get any feedback on whether people are comfortable with that?

>> Jules Cohen: I haven't seen any feedback. And I'm not the expert. I have some experts in this - expertise in this space, but I don't have data on that one.

>> Martine Niejadlik: Jules, are you guys charging or just authing?

>> Jules Cohen: Right now, we're just authing, but there's a process in place to move that to the other standard.

>> Mamie Kresses: He's gonna do that tomorrow. [Laughter]

>> Martine Niejadlik: So, just an FYI for people, just coming from the payments industry, the card associations -- they've always said that it's not okay to just auth a card without a charge, and they're actually starting to crack down on that now.

>> Mamie Kresses: And we don't think that's okay, either. I mean, the Rule was intended for a transaction, and there's a little bit of discussion in the Rule about why that's the case, and a part of that is that, with a transaction, you have some recourse, too, that you will get a bill, if something sticks out, you would investigate it. you know, if it's a dollar... We don't know how practical that is, how much it's being investigated, but the language of the rule actually requires a transaction. And that's been something that we've been educating people on in the last few years because it has come to our attention that there is some lack of clarity there. Ros?

>> Female Speaker: I would just suggest that if you're going to charge...a transaction fee in order to get verifiably 100%, that's not going to work. In the promotion industry, where we want to possibly allow the child to participate in a sweepstakes, you're gonna have a situation, potentially, to win the lottery at that point. [Laughter] So, in complying with COPPA, you're violating all of the 50 state lottery laws.

>> Denise Tayloe: Well, "email plus" is good enough for sweepstakes and promotions and all the internal use. I don't know anybody that asks for...

>> Female Speaker: Or if it's within an exception.

>> Female Speaker: Independents have the operators using --

>> Mamie Kresses: You mean if they're gonna share it?

>> Female Speaker: To go further, and also, if you collect user-generated content, perhaps you kind of use the exception.

>> Mamie Kresses: Okay, Parry, and then we want to move on.

>> Parry Aftab: I'll just be fast. I represent a lot of the newer companies now that are looking for COPPA-cleared communities and that kind of thing, and they're all trying to charge a dollar or 50 cents, and they're trying to donate it back to Cyber Safety and the rest of it. Huge pushback. Parents aren't doing it at all. So if you're doing it, it's nice to say you're doing it, but if you don't have a backup that's going to work, you're out of business.

>> Mamie Kresses: Okay. And, Alan, do you have -- What was I going to ask you? [Laughs] Oh, I know what I was gonna ask you. Do you have any sense of whether the use of a credit card still provides as much assurance of a parent or an adult, let's say, as it may have 10 years ago?

>> Alan Simpson: I don't think it's changed much. I mean, I went back and looked at this after we talked about that earlier. Those numbers have been -- College kids, you see a huge boost in credit-card or debit-card ownership. But when you talk about under-13, those numbers aren't really significant. So, does it prove -- Again, what standard of "verifiable" are we looking for here? It's as reliable as anything else. And it's not likely to have somebody under 13. It's a very small number.

>> Mamie Kresses: Okay. Did anybody-- Yes.

>> Male Speaker: From RelyID. A couple points to throw in. One is that a lot of credit-card companies and banks now are moving purely to online statements. The way you used to know that you had gotten a charge against your credit card is you got an envelope in the mail, and, yeah, you opened it because it came in to see what was in it. Now it's more you have to click onto the e-mail that they sent you saying your online statement was available, go to the website, remember your login and password, and then scan through a couple pages worth of transactions. I think that's much less reliable, in terms of ensuring that a parent knows that transaction ever occurred. And all the kid has to do is sneak downstairs and get mom's wallet, right? So there's less of the feedback loop than there used to be. The other point is that, I think the credit card associations are moving strongly away from using credit cards as authentication, period. Visa has come out with a statement saying that they don't want it used for age authentication, right? Which is just a step from identity authentication.

>> Mamie Kresses: Okay, thank you. And, Alan or Denise or Rebecca, any of you, are you hearing many complaints about parents, about kids, falsifying verification?

>> Rebecca Newton: Well, yeah. I get some. Out of 70,000 a day, I think I maybe average a half of one a day or something like that. So, I mean, it definitely -- I mean, this is a different question, I guess, than you're going to ask about deleting PII. Is that right? You're not asking about that?

>> Mamie Kresses: Yeah, no. We will get to that. Yeah, but my question is whether, are parents calling and complaining, "Oh, my kid used my credit card without authority," or, "Somehow my kid got on there, and I never consented"? Are we hearing a lot of complaints?

>> Rebecca Newton: Some of that. I wouldn't say a lot, but I definitely here it.

>> Mamie Kresses: Ron.

>> Ron Zayas: One of the things we did -- not a formal survey -- but we went to about 100 different schools, and we matched the parents and the kids to the schools, and we asked the parents, "How many of your kids --" and these are between middle school and elementary -- "How many of your kids have a Facebook or MySpace account?" And almost universally, the parents said, "My children don't." And then we matched it up with their actual children, and we asked them, "How many of you have a MySpace?" And about 60% to 70% of them did. So, I don't know if it's so much "Are parents complaining that they're not getting asked?" or that they even know it exists would be the better question.

>> Mamie Kresses: Okay. Great. Okay. So, let's move to the last. In the Rule, there's also the language about using a digital certificate that uses public key technology. Where's that at?

>> Rebecca Newton: I've never seen it any place, so I don't know what happened.

>> Mamie Kresses: What happened? Jules, do you have some -- just some brief thoughts on what happened there, or didn't happen?

>> Jules Cohen: So, a couple thoughts on digital certificates, in general. One of the -- So, the way to think about digital certificates is that -- They're generally the analog to the cards that you have in your wallet. So you have a bunch of identity tokens in your wallet as an adult, and they represent different things that people have said about you. Your driver's license says the DMV says you passed the test to drive. The AAA card in my wallet says I'm current with my AAA membership if I have one. My student I.D. says something else about me. Those are certificates in the real world. So digital certificates would be, essentially, the same thing, analogous to each of those things in the virtual world. And they can carry the same kinds of identity information about the bearers, you know? A set of claims is over the age of something, has brown hair -- whatever the claims may be -- as a student at some university. And so, in the context of COPPA, what a digital certificate might do is allow somebody who has been issued the digital certificate by an approved issuer, like Denise or somebody, the ability to present that token at a bunch of relying parties, a bunch of sites who will accept it. So it's more of a vehicle for conveying the trust that's been created during an issuance process, during a proofing process, than necessarily a proofing process

that would stand alone. And so the interesting question is, where are they? And that technology was nascent 10 years ago. It continues to be nascent, and part of the reason for that is that there haven't been -- There haven't been huge needs over the last 10 years, although we're beginning to see them now, that would drive that kind of technology into consumers' hands, into citizens' hands. The kinds of needs that we see are the kinds of ones that we see here, where you need to get a reasonable proof of something -- in this case, verifiable parental consent -- at a reasonable level of assurance -- you know, how strongly do you want to know that that is the case? And we see similar needs in other industries that are, I think, gonna drive some of the adoption of this stuff. Denise has done some pioneering work in this space. Microsoft, actually, has spent some time with her, collaborating. But, you know, in places like healthcare, in places like finance, in places like tax and government transactions, as those kinds of things move online, I think we'll see more needs to use digital certificates in a significant way, and that might help bring it in a more meaningful way into this space. But at this point, it's rather nascent. We can talk a little bit more about it, I think.

>> Mamie Kresses: Do you think that, you know, the popular-- rising popularity of OpenID and services like OpenID or Facebook Connect, Google Buzz, and all the other ones that I can't think of, whether or not that, in any way, could push a movement towards, you know, using some sort of digital certificate or I.D. for parents?

>> Jules Cohen: So here's the way I would think about it, is that there are lots of ways to issue I.D.s. OpenID is an I.D. My driver's license is an I.D. And those I.D.s are only as good as the strength of the issuance process. And so one of the things that I think policymakers need to grapple with is, you can apply a very robust issuance process -- the kind you get when you go through -- you get a passport or driver's license -- to an open I.D., and that would be a very strong process, backing a not-so-strong usage. A different way to say that is, you can issue me a very strong credential, but if there isn't security attached to it, after the fact -- if it's just a username and password and I can give it to you or I can give it to Denise or I can give it to Ron, the subsequent uses aren't very robust, and that's sort of challenging. Or I could attach it to a smart card or something very robust, and then I end up in a place where I have much -- a much higher level of assurance that the person coming back is the person who was actually issued that thing to begin with. So, things like Facebook Connect and OpenID and info cards and the various technologies in this space are all

great things to pass around claims about people that have been made, but they're only as strong as whatever offline or online issuance process backs them. So we end up in this same place. I can issue you a very strong digital credential based on "email plus," but it's only as good as the verification that occurred up front. So they're a vehicle for disseminating proofs.

>> Denise Tayloe: I would say Facebook Connect and OpenID and all of that, though, works great for the parents. So, earlier, somebody was talking about how Facebook Connect works. So if you said, "Hey, parent, we need you to create your parent account," you can use your Facebook logon to do that. Most parents, or a lot of parents, now have Facebook accounts. You can suck up the data about them from their Facebook through the API that's provided, present that to the parents so they don't have to fill in any of the information, then layer it with -- it's either an e-mail to them that they click. Now you have an "email plus." But they can now do this with their Facebook account, logging on to deliver the consent, going forward. So I think those things actually play in in creating the accounts, as well.

>> Mamie Kresses: We got a comment just a couple days ago about advocating for the use of E-SIGN for parental consent. And actually, this is something that we thought about. It's not uncommon to just now type your name in to forms. And, Alan, how do you see -- Do you see the use of E-SIGN as workable for providing reasonable insurance of parents?

>> Alan Simpson: I think it's a reasonable place to look because Jules' point is very valid. I mean, all of these are undergirded by "How robust is the system beneath it?" And, actually, when you were talking about that, I had a flashback to friends of mine, but not, of course, me, faking their I.D.s back in certain ages.

>> Denise Tayloe: Right.

>> Alan Simpson: All of these things can be built around, but having something better, having something like E-SIGN where the balance between accessible technology, easy technology, and some more -- some greater level of verification is where we're, I think, aiming. The perfect won't be reached, so is E-SIGN an option? Would it get more parents engaged? I like the point that

someone made earlier about not even just -- Some of the benefit here of notification. At least getting parents engaged in the fact that, "Your kid is now going to this site." "Okay, maybe I didn't really get an informed consent there, but maybe I got a slightly greater awareness on the part of that parent, but this is what my kids are doing."

>> Mamie Kresses: And with that, would you want to see an opt-out, as far as, your parents -- your children -- "Your parents are engaging on a site..." [Laughter] Would you want to see an opt -- Do you think it would be sufficient to give parents an opt-out in certain circumstances?

>> Alan Simpson: I think it would help a lot. I mean, that's the sort of shorter-term engagement that we can kind of guess, in this space, that those things might be helpful. Getting an 18-page document isn't going to work. Being asked to print out and sign and fax, obviously, has only been taken up by so many.

>> Mamie Kresses: Mm-hmm. Okay. Let's go into mobile phones, and we're going to delve a little into Martine's experience. And I really do welcome questions and comments, too, as we face new possibilities and we closely consider them. So, obviously, it's been said many, many times that mobile phones are becoming a central mode of communication. And we know that they're being used as payment devices, as well. In other parts of the world, it's been going on longer than here. So, you know, I want to ask the question, what role can they play in parental verification, and when? When would it work if there's a role? So, let me just start with you, Martine, and if you could, give a little background on what you're contemplating for the potential mobile-phone method.

>> Martine Niejadlik: Okay. So, first, let me just say that mobile obviously comes up a lot. And it can mean many, many different things and can be used in many different ways. And even when you talk about mobile payments, which is what I say we do as a company. If you talk to PayPal, they'll tell you they do mobile payments and it's actually very different from what we do. So let me just take a minute, quickly, and just describe what it is that we do and then what we're thinking about, in terms of authentication. Some people joked earlier about texting "American Idol" and didn't really -- weren't really too familiar with that or hadn't had that experience. I'm going to take

you into another experience now. So pretend you're on Facebook and you're playing a game -- "Farmville." Who's heard of "Farmville"? [Laughter] Lot of people. Okay, good. And so you want to buy a tractor for your farm, right? You want your farm to be really great, and you want to get a tractor 'cause you're tired of mowing the lawn, and the tractor costs \$5. And so one of the things that you can do now is you can pay with your mobile phone, and what that means is that we will charge direct to the carrier. So there is no credit card, there's no bank account. The way the flow looks is that you say, "I want to buy a tractor," you click on "Pay by mobile," you give us your telephone number, and then what we do -- For every transaction that comes through the site is we send an SMS message to confirm that it's actually you who is giving us the phone number and I'm just not giving Rebecca's number, and then you have to reply to that text message, and when you reply, we go ahead and we bill the carrier. Billing, by the way, the way we do it, of course, through a platform called premium SMS, which is something that has existed for a long time for purchase of ringtones and other things that people use on mobile, so we're leveraging that now to offer mobile payments as an option. We're particularly focused on digital goods in virtual worlds and social networking, in that whole sort of space. And one of the main reasons for that today is because the carriers charge a very large fee to be able to use one of these payments, and so it doesn't make too much sense in the physical world, at the moment, but we certainly see it moving in the direction and, very quickly, that it's gonna start applying to many other areas, as well. So, the fact that we're in social networking and digital goods and all that sort of stuff is the main reason I'm here today. We certainly recognize, as everybody knows in the room, that there are children who were using these services, despite the fact that Facebook says you have to be 13. And particularly because we're a payment service, we feel the responsibility to ensure that children are not spending exorbitant amounts of money online, right? Buying all this stuff and playing these games. And so what we are contemplating doing now is to introduce another step into the payment flow, whereby instead of just directly texting the child to confirm that it's -- they want to make the payment -- the child's got the phone, so, sure, great. Let me make a payment" -- we would instead text the parent. We may offer e-mail as an option, as well, if that continues to exist, ask the parent if we have consent to, "A," collect the phone number from the child to do the billing, and then, "B," to process the transaction. We see, actually, some super-interesting things in utilizing this technology. Number one is that one of the downsides, I think, of e-mail is that people can create many, many, many, many e-mail addresses. You can't really do that with a phone. I mean, yes, you can buy

prepaid cards. They're not very popular in the U.S. They're more popular internationally. But it still would be a burden to go and buy many, many prepaid cards to try to get around that. So it's very sticky, right? As soon as somebody gives us a phone number and gives us an age, you can't really just go back and say, "Well, no. Let me give you this other phone number," because that's not your phone anymore. So that's one of the big benefits. Two, we're doing this actual physical-device verification, which is extremely unique. I've been in the fraud space on the Internet pretty much since it existed, and lots of companies now are issuing these tokens -- like you have your little PayPal token you can carry around in your wallet. The fact of the matter is nobody has them and nobody wants to carry around 50 of these things on their key chain. So this is a physical device that has already been issued, is available to people, and people have it, which is wonderful. And so by doing this type of verification, it's much different from just asking questions -- you know, "What's your mother's maiden name? What your password? What's this? What's that?" And then you get people who try to steal that information or guess that information, those sorts of things. So that's a big benefit, as well. Today, in the mobile industry, there are tools available, and we actually see there being even more tools available. So, in the U.S., for example, I think pretty much all the carriers offer the ability to block premium SMS. So when a parent issues a phone to a child -- and they may or may not realize today that that's a payment instrument. They'll figure that out eventually, soon. They have the ability to say, "Well, I don't want this physical device to be used for payments," and they can issue that block. And already -- just yesterday, actually -- heard that there were other countries that are getting on that bandwagon, as well. So that's great. It's a very global payment option, so we today are live in 60 countries with almost 200 carriers, and we reach 2 billion people out of 6 billion in the world, so there's 2 billion people that have phones that could pay through our service that are SMS-enabled, et cetera, et cetera. So that's fabulous, as well. A lot of people have phones.

>> Mamie Kresses: So if you could -- I want to ask you the question first, and then I want to ask some other folks on the panel, too. What do you see as -- Looking at the standard that it has to be a method reasonably calculated to obtain verifiable percent and reasonably calculated to ensure that the person giving consent is the parent? What do you see as the challenges to having that level of assurance, and what would you like to see from other -- What would you like to see from the carriers or the device makers, et cetera, if there are challenges, that would change those challenges?

>> Martine Niejadlik: Mm-hmm. So, Mamie and I chatted a little bit about this. I think another thing that we're sort of thinking about is. when a child is coming through to process this payment, should we bill the child, or should we bill the parent? Right? We now actually have the opportunity to do either because we've collected the phone numbers of each one. So, if, for example, we introduce the option of, "Well, let me just bill the parent," the child is certainly going to be less incented to provide their best friend's phone number because their best friend's going to get in trouble when that charge shows up on their bill. So that's one thing we're sort of thinking about. I think there's benefits to billing a child and billing the parent, and that's something I think we'll probably test to sort of see what the acceptance is. I think, in the mobile space again, there are tools, like the blocking and the premium SMS, that's out there. We actually also got notice very recently that at least one carrier in the U. S. is planning to build a zip-code verification tool. So one thing we could do is pass in a zip code, and we could find out if that was really the zip code associated with the plan. So we could say, for example -- We could even look -- do it location-based, right? You could say, "Well, give me the zip code of the child and give me the zip code of the parent," and if those are in two totally different places or neither one of them verifies with the carrier, that could indicate that, "Well, maybe this isn't really the parent." You would expect if the kids and parents on the same plan, they're probably gonna have the same zip code, as well. So lots of little things like that, I think, that are coming out in the industry that'll make the verification even stronger, but even today, with the charge happening in combination with the phone, and just to your point, Gwenn, about parents not really using SMS -- I think a tendency to use SMS is probably also a little bit different if I'm just picking up my phone and I'm just texting you versus I have my phone and all of a sudden it beeps and it says, "Oh, your child is trying to do something. Are you okay with it? Respond yes or respond no," I'm probably much more likely to be able to do that and follow those instructions than just sort of creating my own SMS.

>> Female Speaker: You look at 30% of parents that, as you mentioned, are a lot of parents not using texting, so, you know, I was making, obviously, a sweeping generalization, but when I see parents come in to a clinic, for example, or just walking down the street or even in my own town in Massachusetts. which is a nice, middle-class town, you'd be surprised how many parents still aren't

embracing it. So it's somewhat cultural, somewhat socioeconomic. We can't make full-blown generalizations, but 30% is still 30%. That's a lot of people.

>> Mamie Kresses: Let me ask Alan, and we'll take some questions from the audience. What do you see -- I shouldn't say "what do you see." Do you see challenges from either the reliability standpoint or parents' acceptance of a mobile system like this?

>> Alan Simpson: I see opportunity. I mean, there are the same challenges for all of these things, but in the earlier discussion about mobile, and we talked about this a little bit in our earlier call, and I've talked with a number of people about it, but I don't see why you don't have mobile-phone companies already out there proactively saying, "Hey, when you come in here to get five phone, we're going to make a hunch that you're doing a family plan. Do you want to register those phones to specific ages?" Totally an option. The FTC obviously wouldn't mandate it, but why not enable those phones so that you know which one belongs to the parent, there is a signature on those phones, you know which ones belong to kids that are under 13. I'm not a technologist, but some of this stuff seems -- The fact that we are increasingly moving into a space where we can pay for things with our mobile phones means we can do a lot of other things with them, as well. And I see a lot of opportunity there. I fully appreciate Gwenn's point, but none of these things solve for every family.

>> Female Speaker: Right.

>> Alan Simpson: Adding technologies that would, right.

>> Female Speaker: What you said is perfect for safety.

>> Alan Simpson: For safety, for a better verification that, "Okay, this phone --" Again, this should be an option. But why not have a family phone system where we know that these phones are kid phones that belong to this phone, which is a parent phone?

>> Mamie Kresses: Mm-hmm. And, Ron, you look like you had something to say.

>> Ron Zayas: Yeah. I think that it's a great layer for three different reasons. Number one, it's an opt-in from the parent. By saying at the point of purchase when you're buying an iPhone or you're buying any type of a mobile phone or an iTouch or anything else -- not that I'm a heavy Apple person.

>> Alan Simpson: No.

>> Ron Zayas: But you're making it aware of the parent that here's an extra protection. Sprint -- We have both AT&T for our phones, and then we have Sprint for our children's phones, and they do a very good job of saying, "Look at all the things we have for kids' phones. You can locate them. You can limit their amount of time. You can do all these things with it. It's a great marketing for the phone companies. It's a great way to make the parents aware. Second, the opt-in is good because now the parents who want to put this protection put it in, and the ones who don't, don't.

>> Alan Simpson: Right.

>> Ron Zayas: The second thing is that it can apply to lots of different areas. Cable connectors can do -- Your cable provider can do this in many different ways, too. Obviously limited to the computers, but you can have a token where they log in, or the child logs in, or the computer IP comes in, and right away, you can log a computer and say, "This is a computer that my child uses, and I want them to know that." The third level, though, here that needs to be very important, and if it becomes one of these standards where the FTC can help promote this, is if you say to the Facebooks of the world and the MySpaces, "This is something that's available. This is something that meets this requirement, and we think it's a good way of doing this," it puts a lot of pressure on the content to not only say the token exists, whether it's an open I.D. or whatever it is -- the token exists -- but on the other end, if the token does exist, you probably should be listening for that token, and you should probably be respecting that. That's a very strong rule that, when you put it on top of the other ones, ends up covering a lot of people.

>> Mamie Kresses: Okay. Uh, yes. Peter.

>> Male Speaker: There's clearly a lot of vendors trying to solve this problem, okay? And the big problem is the cost of going beyond "email plus," right? It's kind of the elephant in the room. No one wants to do the big authentication piece because, the cost of acquisition of a user is so high that when you do that piece. But all the different providers have got solutions. I would urge you -- this is a plea to come up with a protocol, lay it on top of OpenID or XAuth or OAuth or something like that, that allows all the providers to exchange the policy information, what the parent wants, to that site, either be it as simple as authorizing it to use outside or to say, "I allowed him to use this type of chat level," or, "I allow them to make purchases on the site or make friends on the site. But that's something the FTC could get behind. They can't get behind the vendor. They can't say, "Hey, use this vendor or use that vendor." But you say this is the protocol that will allow parents to shed policy requirements to that site. And that's something I'd like to see -- everyone get together and say, "Look, let's build a protocol." We're not in that business, but you guys all are, so...

>> Mamie Kresses: Okay, yes.

>> Mark Bohannon: Mark Bohannon with the Software & Information Industry Association. The only problem -- Our industry is one of the biggest fans of using encryption digital technology to authenticate. The problem, though, is that the standard that the gentleman just uttered is not the standard of COPPA. And that's the problem we have, which is, "How does the infrastructure of digital certificates ensure that the person providing consent is the child's parent?" That is a very unique standard which would require, based on our experience -- and I worked in the federal government on this issue when you all were still trying to put together a bridge certificate policy. That's not just a technological invest. It's a broader investment about a structure that verifies that. And that's the challenge we're gonna have with trying to take commercial models, which may not need to have that level of insurance, that it happens, in applying it to the COPPA standard. That's the fundamental problem we've got with ever having it be pervasive.

>> Ron Zayas: But nothing up here would meet that standard today, so...

>> Mark Bohannon: Because of the nature of the digital-certificate technology, it's held to a higher standard because these things get as close as possible. There's no equivalent in the digital-certificate environment.

>> Mamie Kresses: Okay. And did you still have that thought?

>> Male Speaker: Yeah, I was just going to go back to the voluntary offering. The voluntary offering up of information and in designating individual devices as children's devices. Since Heidi's not here to speak for the telecom industry, I'll step in. Going back to our sessions, to what extent, if that's not in any way regulated, if it's not required, if it's not designated as being authorized, to what extent does that type of provision of information to the telecom carrier constitute constructive knowledge, or actual knowledge, and to what extent do those telecom carriers have to process that through all of their systems and to any of their suppliers? The question is, how far does that have to go if you give that knowledge?

>> Mamie Kresses: Okay. And then let me turn the question back to you. We were talking about a lot of sort of at-purchase ideas, which are, you know, great ideas, and, you know, we've heard talk of them before. But let's just assume for the moment that we have a parent who, you know, gave their kid a phone, but, you know, they got it at the mall and they want to be out of there in five minutes and they didn't do any of that. And now they have a phone and they want to use it as a means to getting payment. And we'll assume for the moment that they're a law-abiding child that identifies themselves as being 11. Rebecca, do you see -- In that situation, do you see any concerns with the use of mobile -- or how do you equate it, as far as liability to other systems?

>> Rebecca Newton: Well, in that instance, I don't think it's anymore reliable than any other method. I think in the instance of where they've gone in and they've registered and they've said, "This is my kid," then it's obviously -- or to me it's obvious -- that it's much more reliable.

>> Mamie Kresses: Okay, and are there -- And I guess I would throw out, too. Are there -- I think Martine raised a lot of suggestions for ways to increase the reliability as the technology develops.

Are there other suggestions on using mobile and, at the same time, you know, insuring adding layers of reliability?

>> Jules Cohen: I think part of the problem that we're seeing in the market is that the methods on the right-hand side of the slide up there don't actually achieve the general standard that's on the left. But because everybody knows they can do what's on the right-hand side, no one has a marketplace to serve. So as somebody mentioned earlier, the conservative approach is pick one or two or three of the things on the right-hand side and let the kids lie, instead of going out and searching for something that actually achieves what's on the left hand of that slide. I think one approach for the commission might be simply to get rid of its listing of methods and fall back on the standard that the general standard is the standard and use some discretion about not enforcing that strictly until there's good technology out there. But signal to the market that what's currently acceptable isn't gonna be.

>> Mamie Kresses: Okay. Well, that's doing a lot of things, so changing it just to the general standard and sending a signal and probably scaring a lot of people in the room. [Laughter] But, actually, that is one of the questions that we wanted to touch on today, and we'd love to hear other opinions. What is the better way to move forward and what is the better way to give guidance? Is the better way to give guidance to simply have the general standard? Is it helpful to enumerate possibilities and potentially add more to the list? Or is it better to get rid of the list? So, you know, for a couple minutes, we welcome thoughts on that. Parry.

>> Parry Aftab: The real problem here has always been, from the beginning, is -- you never know if you've got a parent. And not only if you've got a parent, you don't know if you have the custodial parent, who has legal rights over this kid. And the only people who know that, if the kids are in school, are schools. So they're the ones who know which parents are really parents, who has the authority, the people who are on the forms, the people who do that. And until somebody works on a model that can deal with schools and not offend FERPA so that you can conform -- And I think as we're looking at this mobile technologies, finding schools that will partner with you -- Maybe if we just start with some of the private schools they don't have to contend with some of these issues. If you turn around and say to parents, "You can authenticate with the school, one-time authentication,

we'll know that you're the parent. Thereafter, you have it." You're starting to see that model work. It's not scalable at 425 million people on Facebook, but it will work for the sites that are 500 million to -- 500 million -- 500,000 to 2 million, which is a lot of the preteen stuff. It's a good way to get there, but unless you work with the schools, you're never gonna get the stuff, 'cause nobody else has this information.

>> Mamie Kresses: Okay. And we are gonna go right to that in a second. I just don't want to preclude the opportunity, if anybody else has a thought on whether the standard should be broad, narrow, longer, shorter. Sheila.

>> Sheila A. Millar: Yeah, I think there are two things. One is that the different methods that satisfy the Rule are related to the information collection. So you allow for "email plus," where you're only doing intro marketing to the child. The other more robust methods involve data sharing and disclosures. And so I think we need to keep those different marketing opportunities or different disclosure issues in mind when we think about the methods that satisfy the rule. I think having the enumerated methods, which people are accustomed to after 12 years of dealing with COPPA, remains helpful, but exploring new methods, whether it's new ways to look at digital signatures, where you can actually sign on your computer, or mobile technologies, mobile-phone technologies -- all that is worth exploring. But I think we have to go back to certain methods. You may require more robust methods for different types of data-collection use than others.

>> Mamie Kresses: Okay. And I think we had a question here first. Then we'll go to Phyllis Faith. Right in front of me. Oh, goodness.

>> Male Speaker: It's Mark again. Let me just say that I feel like it's déjà vu all over again, 'cause I feel like we're repeating the conversation from when the Rule was first adopted, which is -- the problem with just going with the general standard is read literally. You would have to provide a birth certificate and DNA sample to meet the standard. Everyone realized that was absurd for a lot of reasons. It didn't achieve the goals of the act and it also was just impractical. So the methods, again, to repeat -- and we can go back and check the transcripts from 10 years ago -- these came as

close as we can to creating a legal nexus that suggests "better than nothing, that the parent is the person signing this or doing the things that are there."

>> Mamie Kresses: Okay. Phyllis, can I bump you? 'Cause the other Phyllis just told me how little time we have left. So let's save it till the end of the discussion. So, Parry raised the school model. And, wow, Ron had something to say about the school model. So, you know, and, again, because I poorly managed our time here, Ron, if you could give us just a brief synopsis of, you know, what you're trying to do and a little bit of what you see as the opportunities and the challenges.

>> Ron Zayas: Very quickly, eGuardian came up with the idea or worked with -- everybody comes up with different ideas -- of going through the schools and saying, "The schools is a great place to verify. They know the parent. They know the custodial parent. They know the age of the child." And it's very hard to fake. You can't just say, "Well, I screwed this one up. Let me create another child at another school." You just can't do that. So we worked with the schools, and originally, there was some pushback from the schools of dealing with a private entity and saying, "Why would we give you that information?" And the legal hurdles were cleared, you know, because, again, the parent is initiating this. The school's not giving out the information. The parent is initiating the information -- the school is verifying it. But realistically, we found a nonprofit should do this. A private entity should never have this information. We looked at people who were trying to buy our company, and we realized they were trying to buy us for the wrong reasons. A nonprofit, a third party can have this information, but that information exists. Tap into that information, tie into an open I.D., or tie it into a type of token or certification, and you now have something that you can uniquely give to a parent, who they can control, and they can opt in and say, "If this exists, places like Facebook should read it and MySpace, whoever else." If it exists, if the parent or if the unit, the phone, whatever it is sends to you an I.D. that says, "This is a child, and I'm the parent," that should override anything the child types in. And, again, obviously, our company does this, but it's not the point of our company doing this. This should be open to everybody, as you were saying, open to every company that's out there. But we have that information, at least in the U.S. and in most western nations. It exists, and if somebody just pushed it a little bit, if somebody said, "This

could be one of the ways to meet that," I think you'd see a lot of websites starting to take that information.

>> Mamie Kresses: Adam.

>> Male Speaker: Question on that point. Adam here with Progress & Freedom Foundation. I do wonder if we want to make schools into DMVs for kids, because there are liability questions and privacy questions that pervade the use of personal information about kids. And if we made this the new COPPA standard, I mean, we'd be requiring, you know, checkpoints at every school door for credentialing kids to say, "You've got to hand over information," to do what? I mean, that puts the schools in a really difficult bind. It also raises the question of -- is there greater potential for identity theft because of this? And then, of course, there's the question about -- Are we incentivizing kids, instead to lie about their age, to trade, to barter in digital credentials? I mean, older brother giving to younger, whatever.

>> Mamie Kresses: Let's do this. Ron, can you back up a little and tell us, actually, what information you get, who you get it from, who verifies it, and then what people either carry in their heads or in their hands.

>> Ron Zayas: The parents tend to provide -- First of all, it's always initiated by the parent. The parent has to say, "I want to verify my child." So the parent would say the child's name, the child's age, who they are, and a physical address, and a signature. And there's an electronic way of doing that. We won't go into that. But the school then gets the information and verifies it. By the way, schools do that today. There's the YMCA. There's soccer. There's lots of different areas where you have to verify the name and age of child, and the school is the way to do it, and they already have a process for doing it. They already have an individual there, generally, who's bonded to be able to do this. So the liability already exists or the function exists to do that. The second thing is that once the parent does that, then they're issued an I.D., and that I.D. should not have anything other than the parents' e-mail, their verified e-mail tied to it. So you're not pushing out information on "this is Bobby Smith." That should be an anonymous token. It simply says, though, that now that it's tied to this log-in, if there's ever a problem where we need any verification, we know the e-

mail that we're going back to. And if you do that, I think you're protecting a lot of information. The parent can even release and say, "You know what? I want to release my child's age," which automatically gets updated. But it's the parents' decision to decide what gets updated. And, by the way, you could have different levels. For one type of website, you might want to release other information. For some, you might only want to release the most basic information. But it puts the control back in the parent.

>> Mamie Kresses: Okay. And I think, John, you had a comment on this procedure, as well.

>> Male Speaker: Yeah. Just kind of the broad comment that, you know, imagine we could come up with a system that provided a unique digital certificate for all school-age kids in the country. I actually still don't understand how that works in practice for sites like Facebook or MySpace that are, in fact, intending to reach both older minors and adults. Because, I mean, you know, a child gets on and says, "I'm 18 years old." And, so, you know, do we have to go verify and identify all 400 million Facebook users in order to be able to force those who have these identifiers to come up with it? You know, so, it can work in some scenarios, but I'm not sure it works on a Facebook.

>> Ron Zayas: And we see it as -- We worked very closely with Facebook, by the way. We didn't get anywhere, but we worked very closely with Facebook. [Laughter] And now that Chris Kelly's running for attorney general of California, we haven't got his full attention. The main thing here, by the way, is not necessarily that you go backwards, but it's tying that I.D. to certain -- If I say, "I want that I.D. sitting on my child's computer," then when my child uses that computer and goes to Facebook, it's being transmitted then. If I say, "I want it on their phone," it's being translated then. And if I don't want to have it on their phone, then I don't do it and my child's free to do whatever I want. But the idea would be that as Facebook gets somebody coming on to their site that's saying, "I am on a protected or I have an I.D. that's being transmitted," that they would listen for that I.D. and that now they know who the parent is. That's the whole idea there.

>> Mamie Kresses: And, Jules, do you have any thoughts on how -- Whether this is a useful system and, if so, how it could be furthered? It sounds like -- You know, Adam's raised the concern, you know, a privacy concern. And John has raised more of a technology concern. Do you

have any thoughts on either of those and whether this could be used in some way that would avert those?

>> Jules Cohen: There are certainly ways. So, generally speaking, the schools are an authoritative source for some pieces of information, just like adults. You know, there are other institutions that are an authoritative source. And if you want to -- If, as a policymaker, you want to say, "This is the level of assurance that would be required for this kind of a transaction," then it might be interesting to look at schools as a source of that information. We've talked about this in the past, you know, as a group. The thing that I think is important is to separate the method of getting that level of assurance of the school or the DMV or the "email plus," whatever the method is from the technology that's used to convey that piece. So the technology that's used to convey it might be a phone or it might be e-mail or it might be a smart card or various different levels of assurance. But that's the piece that the technology can manage and the technology can manage how secure that is, how privacy-friendly that is. And there are a bunch of policy levers that you can tweak inside that technology ecosystem. But I think that the key thing is to separate the technology decision that are made from the policy decisions that are made about the proofing process and what is the right level of assurance. I think separating those two helps sort of keep the conversation going.

>> Mamie Kresses: Okay. And I hate to do this, but I'll take two questions or thoughts, and then we have to stop. I think Kathryn's hand was up first. Oh, yeah. You know what? That's right. That would not be right. Phyllis has been waiting, and then we'll do Kathryn. Go ahead.

>> Female Speaker: I'm gonna be very quick. But I was just wondering -- and I know we've discussed this, Mamie -- that in light of the fact that all new computers now come with internal cameras and internal mikes, what about using something like Skype?

>> Mamie Kresses: Mm-hmm. And that's a very good point that we were gonna get to. So I'm glad that you raised it. And Kathryn.

>> Kathryn C. Montgomery: Well, I mean, this is a very interesting discussion. Whenever we go down this road, I start getting the heebie-jeebies, I have to tell you. As a parent and as a privacy

advocate, a lot of these solutions sound like they may, you know, raise more problems. And some people have, you know, raised that question, as well. I want to ask a couple questions. One, you know, we know these methods are imprecise, you know, faulty. From the beginning, we knew that. Has there been any assessment of how they're being used, how effectively they're being used, what works and what doesn't work? And I had to step out for a few minutes, so if you addressed it, I apologize. And secondly, you know, to what extent are parents opting into things they don't fully understand? 'Cause one of my concerns is that these methods -- Everybody's focusing on these methods in order to, you know, maximize data collection, and I want to ensure that the principle of minimizing data collection is adhered to here and the focus on marketing safeguards for children.

>> Mamie Kresses: And those are good questions. And, you know, we don't have any data on that and we can't really answer the second. But these -- You know, again, I think a lot of good thoughts have been raised from a policy perspective, a technology perspective, and a parental acceptance, and other things. So I really, again, as in every panel, we urge you to comment from any of those perspectives. And, you know, if you know of others that should be commenting, to get the word out. So we're gonna end this panel and move on to panel 5. Thank you. [Applause]

>> Phyllis H. Marcus: Okay, guys, we hadn't intended to give you a break, but that was pretty unfair of us. So I'm glad everyone got to stretch. And we are completely in the homestretch now. I'd call up the panelists for panel 5. I think Parry's heading up. Do we have Parry? Okay, good. Good, good.

>> Female Speaker: You're sitting next to me.

>> Phyllis H. Marcus: [Laughs] "Come sit, come sit." Good. Okay, I really thank everybody for hanging in there with us. This has been an enormously substantive day, and I know it's a lot to wrap your heads around. Mamie and I often joke that COPPA is Talmudic in its complexity. And so we've dealt with a lot of brain benders today, and we'll deal with just a few more as we talk about COPPA's exceptions to parental consent. I'd like to introduce our panelists. On your left is Parry Aftab, the executive director of wiredssafety.org. Next to her is Izzy Neis, the director of user engagement for Gazillion Entertainment. Then Dona Fraser, the director of privacy online for the

Entertainment Software Rating Board. Mamie is directly next to me. To your right, Susan Linn, the director for Campaign for a Commercial-Free Childhood. Then John Smedley, the president of Sony Online Entertainment. Ros Kitchen, partner at Cohen Silverman Rowan. And finally, Peter Maude, chief technology officer for Crisp Thinking. In this panel, we're gonna talk about COPPA's exceptions to parental consent, which were actually built into the statute. I'm going to put an enormously densely worded slide up. You do not need to memorize it or read it now. I am small enough that I think I'm not blocking the little bit of language at the bottom.

>> Mamie Kresses: And you also have it in your --

>> Phyllis H. Marcus: And you have it in your packet. But suffice it to say that there are some exceptions built into the statute, where the requirement of prior parental consent would not come into play, primarily for an operator's collection of a child's online contact information. And just as a reminder, the rule defines online contact information both as an e-mail address, an I.M. identifier, or -- I didn't have the slide in front of me. It would be other means to connect a child online. But not as expansive, necessarily, as when we were talking this afternoon about personal information. I'd like to start with a basic question for those of us at the table, myself excluded, actually, who were there at the beginning of COPPA, as to why Congress built in any exceptions to verifiable parental consent. Parry?

>> Parry Aftab: Okay, when it comes to the oldest person at the panel, I tend to fit there. So we were there in the very beginning of when COPPA became law and when the FTC said, "If you don't listen, we're gonna make a law." And everyone said, "Yeah," and didn't listen, so they made a law. We need to understand that in the beginning, it came out against marketing. It all started with KidsCom.com and then the CME letter that Kathryn's talked about, and it was all about marketing. What information are you collecting from kids? How are you using it? How are parents engaged? What do they know about what you're doing? During the process, however, it also became about safety. And because FTC has dual-prong, on both consumer protection and safety, jurisdiction, it became about protecting children from sexual predators. And you have to remember we're talking about 1997, 1998. That what was everything was about on the Internet. Everyone was afraid that the children would be abducted immediately if they met anyone on the Internet. So as they started

looking at what we can do, we recognized that we wanted to protect children from giving away too much personal information online and communicating with Internet sexual predators who would immediately come to their house and abduct them. And an awful lot of that had to do with offline contact information. "Where do you live? How can I find you? How will I find you on the street and grab you and steal you?" And so a lot of it came from there. At the same time, we recognized that if we were going to get parents involved in whatever was going on and tried to get their consent or notify them, we had to reach them. And we were concerned that any other way wouldn't reach the parents unless we did them through the kids. So we had the ability of the sites to collect certain kinds of information for certain limited purposes and deal with it in that way. At the same time, we're protecting children from sharing offline information. We further recognized that there was a need for the sites to protect themselves -- the security of the sites themselves, the safety of the children while they were there. And if parents weren't giving consent, did that mean that these children would be lost forever in cyberspace? And so as we looked at the exceptions, it was you don't have to get prior consent. You can keep it under certain circumstances. And here, more than any other place, you will see that you deal with use, not information. So although we deal with offline contact information there, a large part of it is, "How are you using the information you have?" And so we see more of that in this section than you do in others. So it was very practical and fear-based as we're doing that. Now we recognize cyber bullies are kids who go to the kids' school, and they know where you are all the time. There's less of a concern about Internet sexual predators. It's a serious risk, but not as prevalent as others. And I think that sometimes the exceptions are eating the Rule.

>> Phyllis H. Marcus: Okay, and we will definitely discuss that in this hour together. Dona, do you agree or is there something you'd like to add?

>> Dona Fraser: No, I agree. I think that, in addition, Congress, I think, just did not want to unintentionally interfere with a child's ability to enjoy the Internet, as well as be able to access timely information, either from their schools or libraries or things like that. So I think there was certain consideration given to that, as well.

>> Phyllis H. Marcus: Kathryn or Angela? What do you guys think?

>> Kathryn C. Montgomery: I don't know remember in our discussion so much of a focus on safety. You know, Parry's right -- that was the kind of, you know, era that we were in. There was a lot of public debate about it, and COPPA got discussed in that context. But as I recall, it was to try to create some balance between ensuring an online experience for young people that was -- You know, that would allow them to interact and enjoy and be online, but to do it in a way that circumscribed the ability of online marketers to effectively target them and to maintain ongoing communication with them. So I remember examples -- And, Angela, you can correct me if you remember it differently -- but I can remember discussions about creating an online newsletter, for example, that you'd like to be able to have and get and could we do that? My concern was always, "Is that an online newsletter that's basically a marketing message that's gonna come to them every day or every week?" But it was really framed more in the context of educational content, informational content, and a good experience.

>> Parry Aftab: But the chat part about posting personal information had to deal with Internet predators. It's the nature of you came at it from the marketing -- I came at it from the child safety.

>> Kathryn C. Montgomery: And you're right -- it was a kind of set of hopefully, you know, practical ways to deal with some of these things. Angela, would you agree? Okay.

>> Phyllis H. Marcus: Is that -- You know, for a variety of reasons, neglect of online contact information was seen as possibly slightly less of a privacy concern in this context. And I'm wondering if that's still the case. Susan?

>> Susan Linn: Well, I was struck by what Parry just said -- that what we found is that sexual predators are less of a concern.

>> Parry Aftab: Not less of a concern, less of an overhyped concern.

>> Susan Linn: Yeah, right. No, no, I'm supporting what you said, but I think that the converse of that is that marketing to children has escalated just exponentially on the web, and that's really

where the primary harms are. And I think that we've hardly touched on marketing today, really, and what we haven't talked about are the harms of marketing to kids. And I think we need to at least say that marketing research shows that marketing is a factor in childhood obesity, eating disorders, precocious sexuality, youth violence, the erosion of creative play, which is the foundation of learning, and also the acquisition of materialistic values, the false notion that the things we buy will make us happy, to say nothing of underage tobacco use and alcohol use. So I think, you know, that I, you know, share Kathryn's wish that children have a nice, happy, fun, productive, educational time online, but I really think that we have to deal with the marketing.

>> Phyllis H. Marcus: Ros, what do you think?

>> Roslyn J. Kitchen: I honestly disagree with Susan, because I think that, generally, as COPPA has evolved and more and more responsible companies are reading the statute and thinking, "Oh, my gosh, what do I have to do?" They're tending to take a step back and saying, "You know, we might have a couple of kids products out there, but we're not -- Our target audience is not the child. It's the mom who's going to the store and buying it or dad who's going to the store and buying it." And so they are, from what I've gathered and from my clients, I'm seeing less of a push to market to the under-13s, more of a push to market to their parents, for sure. But and a lot more responsible -- You know, the companies that are sending people here today, the companies that pay for me and other people to represent them -- they are the ones that are kind of making sure they comply, because they are a direct children's website or they are directly involved only with that space in the marketplace. So they have to market to children. There's no way around it. Or they're saying, "We really don't have to do this by virtue of the products, the information, the services that we offer." So they're taking a step back.

>> Phyllis H. Marcus: Dona, are these exceptions widely used?

>> Dona Fraser: I think that they are. I think, primarily, you're probably looking at the ability to obtain verifiable parental consent and the one-time use for the companies that we deal with -- those are the ones that I think are mostly used.

>> Phyllis H. Marcus: Okay, and the one-time use -- we affectionately call it the one-time-use exception. It is number 2 on the screen behind me, which permits the collection of online contact information for the sole purpose of responding directly to the child one time. The information is not to be used to recontact the child, and it's to be deleted by the operator immediately thereafter. So you see the use of the one-time-use exception in your experience.

>> Dona Fraser: Right. I think you're looking at password reset. You're looking at tech help. You're looking at send-a-friend things, those types of things, one-time uses. Ros?

>> Roslyn J. Kitchen: "Why don't you offer this product in green? I really like green." [Laughter]

>> Phyllis H. Marcus: But in addition to the one-time inquiry by a child, what about what we call the multiple-use exception, which is number 3 and the most densely worded of the exceptions. Do you see a lot of use? This permits an operator to collect the online contact information from a child to be able to communicate with that child more than once, but immediately after communicating with the child the first time, the operator has to send the parent an opt-out notice. Ros, do you see the multiple-use exception come into play?

>> Roslyn J. Kitchen: Initially, in the promotion industry, this exception was being used quite widely with regard to sweepstakes entries. But more and more, as we've kind of moved towards the collection of user-generated content in connection with a contest, for example, we're not -- You really don't fall within the exception. So if you're being responsible and you're reading the statute fairly narrowly -- And you guys know I take a fairly conservative position, especially with regard to sweepstakes and contests. But when you're talking about children's entry into that and what information they have to provide, this online contact information, which can't be used for any other purpose -- Well, if you're in connection with a contest and you're collecting user-generated content that perhaps they're putting video on a website, where they have identifiable features in that video, it's more than online contact information. And the marketer isn't going to go to the trouble of doing all of this if they can only use it in connection with that contest. They may want to go beyond that.

And if they've got -- You know, and so they'll take other steps to get parental consent without falling under this exception is the things that I'm seeing.

>> Phyllis H. Marcus: What about Kathryn's example of newsletters and ongoing communication with a child?

>> Parry Aftab: That's where we're seeing it used most often is newsletters, eNews, alerts, new products, information about a new feature on the site, something really cool that's come up. And so we see that repeated newsletter or notices to the kids at the site.

>> Roslyn J. Kitchen: Signing up for a catalog.

>> Parry Aftab: Yeah.

>> Roslyn J. Kitchen: Being sent a catalog every month.

>> Parry Aftab: An online catalog, sales, that kind of thing, new offerings in virtual worlds. "Now you can buy a new tractor. Now you can buy a new fish. Now you can go to outer space."

>> Phyllis H. Marcus: Izzy, what's your experience?

>> Izzy Neis: I'm pretty well immersed -- Ooh, let me see if I can grab this a little bit. I'm pretty well immersed in the industry in general for kids. I have my e-mail all over the place, as, like, logging as a child, 'cause I want to watch how safety is used and practiced in follow-up. For the most part, I'm not as concerned about the collection of this kind of data for companies that are built for kids, because they understand these limitations. They're following the rules, for the most part. And if they don't, they usually get their hand slapped relatively quickly because everybody's very concerned about making sure we stay with safety. Where the concern comes with marketing-type collection of data isn't so much in this process. It's more what everybody has been talking about all day long -- about data mining and all that -- And that doesn't have, necessarily, anything to do with this directly, what we're talking about at this time. So getting off on that tangent probably isn't

ideal for this conversation. But for the most part, everybody's dealing with newsletters, alerts, just as Parry said, 1v1 e-mail contact. So it's basically customer-service stuff like, "I lost my potion. Where's my potion?" You know, you tell the child, "Well, here's your potion," that kind of stuff for whatever game they're playing.

>> Phyllis H. Marcus: Sure.

>> Female Speaker: 'Cause I wanted to know how this all turned out. So, am I hearing you correctly that kids are being targeted, then, with e-mail communications for products and with advertising?

>> Izzy Neis: No.

>> Female Speaker: I mean, I'm asking Parry, actually, 'cause she's --

>> Parry Aftab: Oh, I wasn't sure. I wasn't sure. What will happen is -- Yeah, well, it's not -- I don't know that it's targeting specific kids. It's targeting all kids. So if you are on XYZ virtual world and they have a new character that you can now earn, they'll say, "There's a new character out there, and you're gonna have to earn 2,000 points or you'll have to do that" or "There's a new section of the world that has these new things that you can engage with." What we're seeing is the multiple-use exception. It's the constant communication about the world, about opportunities, about newsletters, about alerts, about a whole bunch of different things. And it's not profiled targeting to kids in that specific instance. It is information that's out there about anything new that's happening at the site.

>> Phyllis H. Marcus: Wait, hold on Kathryn. Well, wait. We're definitely gonna get to misuses. That's my next question.

>> Kathryn C. Montgomery: I worry that this will create some loopholes.

>> Phyllis H. Marcus: Okay, well, we're getting there. Guilherme.

>> Male Speaker: Quick question about the newsletter issue, as well. And I'm wondering if people have more information on how they work. My understanding is most of e-mail newsletter services actually track whether the e-mails have been read. They track what links people are clicking on. Would that information collection fit under the exception of, you know, "Here, this exception is only for online contact information." That means that I shouldn't be allowed to track whether the e-mail's been read and whether any links have been clicked on from the e-mail. Is that correct?

>> Phyllis H. Marcus: Well, maybe, maybe not. Dona.

>> Parry Aftab: From an operator's perspective, it's very hard to narrow down to an individual which person -- And it's kind of costly to be like, "Okay, I sent out 30,000 e-mails to people who have opted into the e-mail. Now I'm gonna track down to this one person, see if they opened up the links." It's timely and not necessary. You don't really see that happening in operations.

>> Phyllis H. Marcus: Dona, let's talk about misuse. Is there -- You know, what your interpretation of this narrow exception is.

>> Dona Fraser: I think that you have companies that are -- Oh, thanks. I think that you have companies who are collecting the information and using it in ways that clearly are not intended. They're not giving the parents notice. They're not giving them opt-in or opt-out consent. You may be -- And where's Denise? I don't know. I don't see Denise. Oh, there she is. Okay. She and I have talked about this on multiple occasions. I'm gonna use the example that we've talked about, which is a company that, you know, sends out a birthday-notice e-mail. The next thing you know, they've collected your e-mail address simply to notify you on your birthday. Next thing you know - - Which should only be one time a year. But now, next thing you know, you're receiving 10 e-mails in a matter of two months. So those types of things are happening, where there's no disclosure of that information, where there's no -- They have not told you from the outset what they're going to do with that information. They've only told you that this is simply for a birthday club or a birthday newsletter.

>> Female Speaker: Technically, adding the date of birth to the e-mail. So if you're gonna use notice and opt-out, you're supposed to have first name and e-mail address. When you add a date of birth, you've added a piece of information that you're aggregating against that. It should step you up to "email plus." If it's stepped you up to "email plus," then they could ask for permission to have this sort of interaction. But instead, they're using notice and opt-out in place of "email plus" and adding this other data. And the other big one is user name and password against an e-mail address. The e-mail's for newsletters, but the user name and password is gathering points and likes and dislikes. So it's not that every kid gets the exact same newsletter. They get something tailored, based on when they were last in that game or how many points they might have or what they can do.

>> Dona Fraser: Right. And I think that -- I mean, there are companies who are obviously using deceptive practices. Whether or not it's an intentional act, I think, is we don't really know unless we're dealing with those companies specifically. There are some who are just not aware of the law.

>> Phyllis H. Marcus: Just not aware of the law or perhaps reading this exception more broadly than it was intended?

>> Dona Fraser: I think it's both.

>> Parry Aftab: Confusion. I think lots of confusion.

>> Dona Fraser: I think it's both.

>> Parry Aftab: The e-mail part -- they get them all mixed up.

>> Female Speaker: And copycatting -- they think that they can steal the privacy policy from the other site. It's a big site that sometimes gets it wrong. You guys have nailed a couple big brands -- right? -- that have big, fancy lawyers. And then other little companies are following them, saying, "Well, they do it, so I should do it." But they don't understand that, you know, Club Penguin actually does a really good job of deleting a whole ton of data that you type on one end and doesn't

show on the other, but the little new site that looks at it says, "Well, they're using "e-mail plus," so I can use "e-mail plus," even though I have a black list, not a white list." It's copycatting, you know, bigger companies.

>> Parry Aftab: Most of them have no idea what they are doing with information. They really don't have -- They haven't mapped data, haven't mapped information, and that's part of the problem. They think it's just a newsletter, and they haven't thought it all through, and that's a big problem -- big companies and small companies alike.

>> Dona Fraser: I think because they don't know they have to, honestly. I just think there are so many people who are ignorant to the fact that this law even exists.

>> Roslyn J. Kitchen: And I would also say, too, that a lot of big companies rely on third-party vendors to provide this service, and there are huge companies relying on these little, tiny vendors that don't go get big, fancy lawyers, or, you know -- and so it's kind of this trickle-down effect. Nobody knows what anybody else is doing, and everybody thinks, "Well, because it's so-and-so, they must know." But they are relying -- you know? So, it's...

>> Parry Aftab: And games and virtual worlds have changed everything.

>> Roslyn J. Kitchen: They really have.

>> Phyllis H. Marcus: Susan, what do you think?

>> Susan Linn: The multiple-use exception is the one that really troubles me the most of all of these exceptions, and it troubles me for lots of reasons, one of them -- I'd like to go back to cellphones and texting and the fact that kids are contacting these companies. I mean, all these com- - Like, McDonald's, for instance, had a "text McFlurry" campaign, and kids are seen either being encouraged to text just about everywhere they look, so they're contacting these companies, companies are getting back to them. Then they can keep doing that or they can keep, you know, going back without getting parental permission. That's really, really troubling to me, because the

parents aren't gonna have any idea of what's going on. Once a child has a cellphone, there's no way that a parent's gonna know what that child's doing on the cellphone. It's really -- I mean, it's really, really difficult. So, once we get to mobile marketing, I think that some of these loopholes and exceptions really need to be closed, and that's the one that troubles me the most.

>> Phyllis H. Marcus: Fair enough.

>> Female Speaker: Phyllis, can I comment on that really quickly?

>> Phyllis H. Marcus: Sure.

>> Female Speaker: I'm not sure if many folks know, but I have no idea what the McFlurry campaign was. Can you hear me? Okay.

>> Phyllis H. Marcus: Yeah.

>> Female Speaker: But when they create those sorts of campaigns, what they're doing is they're doing it through a short code, and so "McFlurry" is something that has been assigned to McDonald's, in that particular case, and Haiti is another example that the Red Cross used when there was disaster in Haiti, and et cetera, et cetera. And in order to get a short code, which is the entire way our company operates, you have to go specifically request through the carriers -- You have to submit a campaign, and you have to say exactly what it is you're gonna do, and they specifically approve that -- that one thing, and you don't get to use that short code for anything else. So, just -- just a tidbit of information. I mean, presumably --

>> Female Speaker: If they don't get the child's cellphone number or they can't contact the child again, or --

>> Parry Aftab: Give her my card. Give her my card. I want to talk to her.

>> Female Speaker: To create their parent account. We get the cellphone number and the carrier that it came from, so is that typical? I don't know if that's typical or not.

>> Female Speaker: You would -- You would receive -- You have to receive that as part of receiving the message, but there is an organization called the MMA, which is the Mobile Marketing Association, and they have rules against what you're able to do with respect to SMSing people, and you can't just randomly SMS them with marketing messages. You're not allowed to do that. So, if somebody's doing that in a short code, they're violating the rules and they can have their short code turned off.

>> Female Speaker: Can you take the cellphone number? Is there a rule against taking the number that you received and doing a data lookup of targets or Axiom or Equifax or any of the other guys that have the cellphones? I mean, every time we make a purchase online and we give them our cell phone, that data now goes to Axiom, who has 300 million of us sitting in their database, and you can -- Legitimate purp-- Marketers can legitimately submit a cellphone or submit a phone and get back the data that's associated to it, if they exist. Are there rules about that, do you know?

>> Parry Aftab: I'd have to check on that specifically. Most of what we do is a response to our own message and not just inbound, you know, receipt randomly of messages.

>> Phyllis H. Marcus: So -- Okay. We could go on this thread for a while, but I want to get back to the exceptions themselves, and what I'm hearing in the room is that this multiple-use exception should be read very, very narrowly. Do I see some assent on that? And if people disagree, I'd like to hear that. But what I've been hearing from people is that it should be read strictly to include only a child's online contact information, so if we're getting some other piece of personal information from a child -- for example, their cell phone -- that would be outside of this exception at the outset. There's someone in the back.

>> Female Speaker: I don't disagree with that interpretation at all. What I think is interesting is you can look at those ads and the exception or a loophole that's being misused, or you can kind of look at this as being kind of almost like a lower verifiable parental-consent method, because it has

this opt-out requirement. So, it might be interesting to think about this -- Instead of them being misused, maybe people -- Instead of looking at this as people are trying to rely on the exceptions too much, maybe this is a reason for why we should expand the list of approved parental-consent methods and provide more granularity, like maybe "e-mail plus" filtering or "e-mail plus" parental controls, so that people move outside of relying on these exceptions and go more the parental-consent route.

>> Phyllis H. Marcus: I would say yes, but, in this instance, these exceptions are set forth by Congress, so this is not a change that we could make here at the commission level. They were carved into the statute themselves. Go ahead.

>> Mamie Kresses: If that's a comment, if people want to comment on added uses in this regard, certainly, they should do it, and if people want to comment on, you know, restricting it, certainly, they should do it, because everything is open for discussion.

>> Phyllis H. Marcus: And one last question for the people on the panel with respect to this -- Is it possible that what marketers and other operators thought was that they could build on top of the collection of online contact information, other items of information that are not considered personal under the rule, so that perhaps there was a misunderstanding that they could collect zip code, for example, which is not enumerated as personal, and they could put that on top of online contact information and then personalize a message to a child and wouldn't run afoul?

>> Parry Aftab: Yeah, and, Phyllis, that's what I see often enough. With even sophisticated people, they think that they can do this because it's non-personally identifiable on other things and it's attached to e-mail. What we need to remind them is it's like the Midas touch. You got personally identifiable information? You touch anything else, it becomes gold. And they don't understand that, and that's been part of the problem. But they think it's, "Okay, that I understand that this child likes baseball and this child has this account and other things because I'm only asking for this piece of personally identifiable information." I see that 80% of the time when I find problems.

>> Susan Linn: I think that's a really good point, Parry, because one of the things that is concerning is that younger and younger children are engaged in virtual worlds where you bring a lot of yourself into the world, and so these companies are getting lots and lots of information about children's preferences, and, I mean, it's really troubling with that information combined with whatever personal information that they're allowed to collect, and that's concerning. They can learn a lot about these kids.

>> Phyllis H. Marcus: So, I'd like to move on to another very hot topic, which is that of chat, and it seems that chat in kids' spaces has become an increasingly popular feature, and with many sites offering some format of filtered chat, I'd like to talk about how children's sites that offer chat are handling the parental-consent process, and I'll start, John, with you.

>> John Smedley: So, I'm from Sony Online. We make a game called "Free Realms." We've had just about 12 million people come through, and probably 90% of them are kids. And --

>> Phyllis H. Marcus: Just to clarify, that's kids under age 13?

>> John Smedley: Yes.

>> Phyllis H. Marcus: Okay.

>> John Smedley: What we found is that the smartest thing to do is to use a white-list chat method and apply it to everybody. You simply cannot have a really safe place where a 14-year-old and a 12-year-old are going to have a conversation with open chat. It's just -- I don't believe that's possible. I've been making these games for, you know, 12 years now, and I've got four kids under the age of 15. And, in fact, I've been bitten a few times by a few sites. One of my daughters got asked to be somebody's girlfriend, which I was thrilled about. She was 11, so it was great. [Laughter] It's -- It's a tough thing, because kids want to chat, but there's no possible way to keep them safe without doing some kind of a white-list chat. They are smarter than we are, and a black-list chat simply doesn't work, and we've seen both sides of this, and that's just the conclusion we've come to.

>> Phyllis H. Marcus: So, I'd like you to describe what you mean by "white-list chat" and then talk about what Sony does on the parental-consent process, and before you do that, I just want to draw everyone's attention to this slide. Under the rule, an operator would be deemed to have collected information not just when they actively collect information by requesting that a child submit her information online but also where an operator enables a child to post her personal information -- for example, in a chat room or on a message board or by other means -- and then we have an exception. Except where the operator deletes all personally identifiable information from the postings by children before those postings are made. And so what that means is that when an operator strips out personally identifiable information before it goes live on a site, then that operator won't be deemed to have collected that information. The information will never have been disclosed to the public. And so conceivably, in that case, an operator won't have had to obtain parental consent for that use if the operator isn't collecting anything else. And so what, John, you're describing is a white-list chat, and what is that, exactly, and do you have to get parental consent?

>> John Smedley: So, our view is that you do not have to get parental consent because we're never, in any way, shape, or form, letting a child give any kind of PII whatsoever. So, we do not -- For example, our message boards -- we do not let under-13s post, period. We took the safest approach. In our chat, you can only use words that are pre-approved. Does this make it really messy and hard for kids to communicate? Yes. Do they try to get around it? Yes. Are they successful? No. And it's a constant battle, because they're trying to come up with a few ways, and you have to constantly be trying to think ahead of what they are. For example, "Oh, so, let's not use numbers so that people can't communicate phone numbers." Well, you'd be amazed how many kids out there know Roman numerals.

>> Izzy Neis: Or "fort, fort, hive, sticks, Steven, ate" -- a-t-e.

>> John Smedley: It's a never-ending battle. But we decided that the right way to fight it is simply not to let kids chat. They're basically picking from a pre-approved list of words, period, and we're making it that simple. And we're applying it -- because this game is directly designed for young

kids, we've made the choice that we don't want older kids to be able to communicate with the younger kids in any kind of, you know, really easy manner.

>> Phyllis H. Marcus: Peter, what's your experience here?

>> Peter Maude: I think, you know, our experience is that white list gives you that better protection, but, you know, there are ways around it, and the examples we've just been given -- "sticks, heaven" to give out numbers -- if I give you two communication tokens, a one and a zero, I can give out personal information. I mean, it takes a lot to get around it, and there's no way that could end up in a marketing database, right? But it goes out. We need to accept where, you know, the limitations -- If we're gonna have communication, the smart kids are gonna find ways around it.

>> Phyllis H. Marcus: What's the difference between a white list and a black list?

>> Peter Maude: The white list is a pre-approved list, so it's safer because you can't give out a street name -- right? -- because it's not on the list. So, I couldn't say, "It's the intersection of Chestnut and High, Folsom and Fillmore" -- right? -- because those words wouldn't be in the pre-approved white list. Now, there are ways around that. Salt Lake City's a great example, okay? You can describe Salt Lake City in words that are on the white list, but it takes some doing. So, we think that the kind of white-list approach is safer, but there's no panaceas in terms of absolutely nailing, eliminating personal information going through chat.

>> Izzy Neis: Yeah, there's a lot of -- Sorry. That got really loud. There's a lot of different ways of doing it. White list is a good example. There's also ways -- I'm kind of managing almost a black-list, white-list approach as well. You can have dictionary chat. The point is you have to understand what's in your lists. You have to have a full grasp of what you're providing for your community, because, like, some of the issues I've come across -- say you have a sports site for the kids, and what the operators of that sports site don't understand is numbers equate all sorts of varieties of PII's. Like, you may say, "Okay, well, you know, three digits in a sentence is fine, because those three digits don't equate a phone number." All you have to say is, "Hey, my digits are 815," enter that, then have another one go through -- "455" -- enter that, and then finish off the -

- There's tons of ways around it. It's just being smart. Now, aside from disallowing kids straight off the bat, there are other Jedi mind tricks, if you will, of allowing kids to feel like maybe they're -- they're not as frustrated, because the problem that we have as operators for kids' sites is kids get frustrated. So, they see a word redDED out, and they can't type it anymore and they're mad, right? So, what are they gonna do? They're gonna phonetically spell it out, and, man, can I give you tons and tons and tons and tons of examples of that. It becomes a nightmare, and it becomes a nightmare for your lists to manage. There are other ways of allowing the user to think that they said it, so they type what they're trying to say. Maybe they see it, but no one else in the room sees it. I mean, if you've been to Club Penguin, about -- this is just my guess -- about 60% of what you think you you're typing, no one else can see. And that's not educationally fantastic, because kids are like, well, they think they can say it. They think they can say it anywhere. But the grander problem is kids don't understand why they can't tell you. Like, they grow up knowing their basics, right? You have to know your phone number, you know, if you ever get lost. You have to know these things. They hold their personality very close to them. So, if they're in a world, sharing any information about themselves is kind of exciting, you know? So, how do you protect them? If you say to a kid, "Okay, so I'm going to black-list or I'm going to not allow the word 'street'" and they're trying to say, "I want to go out. Let's go to Main Street," which is maybe a room in the world, that becomes very frustrating if they get a pop-up message that says, "That language is not allowed. You're on 30-minute silence." They're like, "Ahh!" You know, that's not fun. So, how do you allow them to feel that way? And that's why some sites, like, say, Club Penguin, allow the Jedi mind trick of the author saying it. No one else in the world says it. Have post-talk moderation tools on the back end that find that, and then you, as operator of the site, can then decide, "Is this child innocently trying to talk about something, or is this somebody who's trying to get personal information out of children?" Because that person then broke your T.O.S. Get them out of your world. So, sorry. My little tangent there.

>> Phyllis H. Marcus: Dona, I want to -- You know, we have this very strict requirement.

>> Dona Fraser: Mm-hmm.

>> Phyllis H. Marcus: And, you know, the rule says what the rule says, and unless all information is pre-stripped, it is considered to be a collection.

>> Dona Fraser: Mm-hmm.

>> Phyllis H. Marcus: And so what kinds of rules of the road should we have at the FTC, and what advice should we be giving? Because we get this question all the time about what formats of chat are permissible. And, frankly, the questions come from people who are trying to figure out if they can offer chat without obtaining full-blown verifiable parental consent, which, as we've discussed during the day, is seen as somewhat of an obstacle to some fun, enjoyment, and instantaneous enjoyment by kids.

>> Dona Fraser: I think John has it right in regards to what "Free Realms" is doing. You know, there's no open chat. I think once you are engaging children in open chat, you must get not just parental consent, "e-mail plus," you must get some form of heightened verifiable parental consent, because you don't know what kind of information is going to be exchanged or disclosed, and if you're not monitoring that chat room, if there's -- If you're not doing what Izzy was talking about, where you have somebody who's just typing in and it's not popping up on a screen first and it's just instantaneously going out there, then you must obtain that verifiable parental consent.

>> Phyllis H. Marcus: Peter, what do you think? I mean, you know, we get a lot of questions from people who want to know about automated systems and whether their automated systems are good enough under COPPA.

>> Peter Maude: I think, you know, you can never take people out of the equation. You can deal with the scale. Our solutions help deal with the scale. I think one of the issues is to not look at a very narrow "is this line of content of problem?" You need to look at the person behind the content. And that's one of the things that we do. If you are constantly trying to get personal information from people, your score in the personal-information threat will rise. And that means it brings that person on to the radar of the moderators to say, "Why does this person keep asking for personal information?" Another important point is to always take what they attempt to say and use

that, 'cause intent is so important. You may be filtering it, but if they are trying to give out personal information, you need to let them know. So, even though it goes red and they don't get to say it, we still look at that and say, you know, "Stop doing this. Stop giving out personal information." Or, if it's worse than that and we're seeing the kind of, you know, profanities, even though it's not going through -- the offensive, profane words -- we still say, "Hey, stop doing this. You shouldn't be talking to people in the world like this," even though it's not --

>> Parry Aftab: I think it's important, though, that we separate the law from safety.

>> Peter Maude: Mm-hmm.

>> Parry Aftab: And what you're talking about is safety.

>> Peter Maude: Yeah.

>> Parry Aftab: And COPPA here has something very specific. The question is, can the kids share personally identifiable information through the use of technology? And if you're using it with seven tabs down, white list only, you're smart about what you do, understand the use of numbers all of their symbols and all of their code, in this case, they're not going to be able to share personally identifiable information for the purposes of COPPA. The problem here is you've got white lists, and you've got white lists, so a lot of people put them together and think they're fine, and they are not high quality. They don't understand what they're doing, and the right ones that work for the purposes of making sure kids can't share this stuff are old-time things that have been out there for a long time that kids have tried to break forever. I mean, when you look at Neopets and some of the older ones that are out there and Toontown -- the first time -- before COPPA, in 1998, Toontown had a dropdown menu that I designed for Disney 'cause we couldn't figure out anything better in 1998. So, the world has changed now, but we -- unless we come up with standards on best practices on white list, on what parents are allowed to expect at a site, we're in a lot of trouble.

>> Phyllis H. Marcus: Ros, is there any room here for safe-harbor situation? I mean, I'm definitely hearing white lists as kind of the gold standard, but Peter raised some other issues, some

post-- posting chat or moderated, live moderated chat, which Izzy was talking about, too. Is there a construct that we can use here where we check down a list and say, "Okay," or "In these instances, it's gonna be good enough for now, but you have to make your list or your filter better each night"? What do you think?

>> Roslyn J. Kitchen: I don't know if I'm the best person to answer that. I have to be honest. But, um... I'm gonna pass on that question.

>> Phyllis H. Marcus: Okay. Dona, what do you think?

>> Dona Fraser: Well, I was gonna go back to the point that we were making before in regards to engaging parents. I think that we're leaving out the parent in this whole process, and I think that if you're going to have a site that's engaging children under 12 years old, you have to engage a parent from the outset. I think setting up parental controls the same way that we do in an offline environment with handhelds -- it can be used in an online environment. That's what we advise our member companies to do is set a parental control so that the only information you're collecting from the child at the beginning is the parents' e-mail. After that, the entire account is set up by the parent.

>> Izzy Neis: Mm-hmm.

>> Phyllis H. Marcus: We've got this kind of strange situation that I think Shai was pointing out during the last panel, which is sites that don't have to collect information from a child about the parent but are choosing to contact a parent and notify them. How does that fall within COPPA's --

>> Parry Aftab: Good policy.

>> Phyllis H. Marcus: Well, it's good policy, but we end up in this strange situation where the site might be risking a COPPA violation, because they're collecting the parents' online contact information from the kid for a different purpose.

>> Parry Aftab: I want to just add on best practices, if I can just answer that last question, and it's my add of the day. We have something called a socially safe seal, the best practices seal that's being offered. And a lot of the people in the room and a lot of the people not in the room have applied for it. And we actually go out. We audit the site. We look at the white list, we look at the black list, we try to break them. We check the training and vetting and certification of moderators and their practices from start to finish. If they do that and they do it right, they get the seal, and if there's a safe harbor, that's a great standard that we can start looking at. Do they know what they're doing? Can we trust them with our kids? And if not, then they're gonna have to go through verifiable parental consent, and good luck. And I think we need to start looking at that standard and find others like it.

>> Phyllis H. Marcus: I think that's -- is that Amy?

>> Amy Pritchard: Yes.

>> Phyllis H. Marcus: Oh, hi, Amy.

>> Amy Pritchard: Hi. I'm Amy Pritchard. I'm an attorney, and I'm also the C.E.O. of Metaverse Mod Squad. And, you know, I would say with our company, we have spent hundreds of thousands of hours with these kids and have hundreds of clients. And so I've seen -- What I'm worried about is the white list, good, black list bad. It's case by case. I have worked with horrible white lists, as Parry pointed out, and I've worked with absolutely iron-clad black lists. So, I just want to go on record as saying let's look at the filter itself and not the label.

>> Phyllis H. Marcus: This is a very hard standard for us to apply, because what ends up happening is, you know, 1-800 Mamie and Phyllis. [Laughter] And then we're asked by operators to --

>> Mamie Kresses: And we don't even charge.

>> Parry Aftab: That's because you own the COPPA site for the FTC.

>> Phyllis H. Marcus: I mean, you know, we're asked to assess a filter and a chat room that we don't have enough information on. We are not, you know, spending 100,000 hours with kids in a room trying to figure it out how to crack it, and then everyone is pointing to some of the other operators and saying, "They do it this way. Why can't we do it that way?" So, I think -- You know, my entire body of questions here is aimed at trying to figure out if there are some articulable rules that we can put out there with respect to chat, which is this increasingly popular feature of sites that would help website operators but not obviate COPPA's original intent.

>> Parry Aftab: It's only gonna get harder. And it's not a rule. It's a combination of things so that if you've got premoderation and you're tracking reputation, you're dealing with different things, you can find things faster beforehand, and you can stop them afterward. So, it's not -- As you were talking, and, you know, I have a great deal of respect for you. If you've got really well-trained moderators, you can deal with a little bit less technology. If you don't, you need a lot more technology that has to be updated. So, it's kind of this flow, and at the end, you look at the whole thing.

>> Amy Pritchard: No, we need great technology. We always need great technology.

>> Parry Aftab: No, but you know what I'm talking about.

>> Amy Pritchard: Yeah, but it's definitely a piece. So, it's -- What I'm concerned about is a piece is going to be a stand-alone -- yes, good, no, bad -- and that's where we get dangerous. And also, if we lock down chat to, let's say even just a dropdown list, because, let's face it -- if you really want to prevent any PII, it's no chat.

>> Izzy Neis: It's scripted, right.

>> Amy Pritchard: It's scripted chat.

>> Izzy Neis: And that's when your numbers go, "Whoo!"

>> Parry Aftab: Yeah. That's okay with a 6-year-old, but it won't work with anybody else.

>> Amy Pritchard: And you know where our kids are gonna go? Our kids are gonna go to World of Warcraft. They're going to --

>> Parry Aftab: And Blizzard was here, and we like them.

>> Izzy Neis: They're gonna open up AIM.

>> Amy Pritchard: Exactly. My husband said this is why they created skate parks -- got the kids off the streets. [Laughter]

>> Phyllis H. Marcus: I'd like to move now -- I mean, you guys have given us a lot to think about, and I really will encourage people in this room, and tell your friends, you know, that we need -- we need to hear more on this point, please, 'cause I'm still, you know, hearing a vacillation between a potential safe-harbor system or the iron-clad rule right now. But, you know, what Mamie and I are pretty much telling people if they're calling now is, "Stay tuned, but," you know? Right now we've got this strict rule, and that's it, and unless you can guarantee 100% stripping -- 100% -- we don't have leeway within this rule. I would like to move to black-listing of a child's online contact information, because we get a lot of questions from operators about that and where that falls within one of the exceptions. And we've heard that a strict interpretation of the rule wouldn't permit operators to retain a child's online contact information for the purpose of preventing that child from reregistering on a site -- for example, when she's underage. Is this right, or would exception 5 -- I'm gonna move back to exception 5, which is a safety -- or is it exception 4 or exception 5? Exception 5, which permits the retention of child's name and online contact information to protect the security or integrity of a website or online service. Would keeping a child's online information fall within exception 5 if you're trying to keep them off the site and keep your site secure from underage participation?

>> Izzy Neis: Depends on the information collected. I mean, a lot of the kids' sites these days are going straight to "e-mail plus," which is kind of the parents' -- assumed, right? We have to look at it that, you know, for the most part, people hold it the way it should be. So, if you're collecting a parent's information and the child that's attached to that information is breaking the rules and they've been "parent-verified" through the click-through, you have to be able to protect your overall audience, right? For me, this becomes more of a larger billing question, too. It goes into the whole area of if you have a paying member, you have to collect that information that should be the parents' information, right? So, there's a lot of variables in that one.

>> Parry Aftab: And -- I'm sorry. I think what it comes down to, what's personal information, so that I.P. question -- if I.P. information becomes personally identifiable information for the purposes of this, we're in a lot of trouble, because the sites are collecting I.P. for security purposes, but they're not keeping e-mail addresses and names to protect the site unless you've got a known hacker, a kid who's trying to hurt somebody else.

>> Phyllis H. Marcus: But, theoretically, if we read exception 5 this way, they could keep a child's online contact information. Yes, no?

>> Female Speaker: That doesn't do you a lot of good, because you can't add data to it, and so you can't age out of it. I mean, isn't the issue that I say I'm 11, here's my e-mail address, submit, we have to do the drop the cookie, all that, and what some of us are saying is, "Gee, it would be really nice if the kid comes back tomorrow and gives us that same e-mail. We can say, 'Sorry, you've already -- you need to now prove yourself as an adult versus being able to change your age.'" But we can't keep the date of birth against the e-mail under that exception.

>> Phyllis H. Marcus: Well, sure. What's good for the goose is good for the gander, so, you know, if we're reading these narrowly, we have to read all of them narrowly. Is anyone using exception 5?

>> Parry Aftab: Yes. We use exception 5 when you're dealing with kids who are trying to take down the site, so kids who are gaming the site, security risks to the site, kids who are trying to

collect passwords from other people. And that's where you're seeing it used, really to protect the integrity of the site, and, as we know, our best hackers are sort of 8. And so -- But, you know, they're out there, and they're doing that, so you're seeing that there. 4, you're seeing when you're dealing with kids who have indicated suicide or molestation issues, and then the question is, do you have to notify the parents? That's where we're seeing a lot of confusion. So, if a kid -- and they do it at the age of 6, 7, 8, 10 -- tell you that Daddy's hurting them or they're gonna kill themselves or something, especially when you put them on hold for 30 minutes, now what do you do to protect the safety of that child? Because you require that you're using it only a certain way, and you have to have reasonable efforts to notify the parent.

>> Phyllis H. Marcus: Right.

>> Parry Aftab: That's very confusing when you're dealing with those high-risk situations, but they're using 5 a lot.

>> Phyllis H. Marcus: Some of these exceptions, I will say, you know, you can get mired in them. And we scratch our heads and say, "Gosh, why did we collectively say that?" And here's, you know, kind of a gimme. Exception 3 provides for a parent to be notified by postal mail. When we read this again -- I will say I was not involved in drafting the rule, and I said, "What?! Postal mail?" You know, now you've collected a parent's or a child's home address on this. Do operators use the postal address in order to do the opt-out?

>> Izzy Neis: None of you ever noticed that?

>> Phyllis H. Marcus: Yeah, well, I mean, we can't hide from it anymore. That's what I'll say. This is the grand outing. It includes methods to notify parents. Well, right.

>> Female Speaker: But the question is, is it time to clean that up? Or is there some reason that that was in there that we --

>> Phyllis H. Marcus: Dona, what do you think? Time to go?

>> Dona Fraser: It's time to go, time to go. I think that if the initial contact happens online, it should remain online. I think the problem is that there's this -- You know, from the point that you decide to put something in the mail and by the time it gets there, the parent has forgotten. You're gonna think it's spam. You're gonna throw it out. I think once you're online, I think that's the way to remain online. Whatever the initial contact was, that's how it should remain.

>> Parry Aftab: It came from the olden days where kids might have access at school and parents may not have access at home, especially lower income and disenfranchised people. But those things are -- I'm not saying that they're fully over, but I think everybody has connection to something electronic now.

>> Phyllis H. Marcus: I mean, it seemed curious to us, because we started this entire conversation by saying that there -- that online contact information was seen as carrying less of a privacy risk. And then if you're adding on to that a child's home address, that's a great expansion of your information collection. I think, unfortunately, we've got to wrap up now. Thank you, guys. I mean, this is a good audience for the end of the day, and we really, really thank you for coming. I - - Should we do a little closing remarks? Okay. We're not gonna do the traditional closing remarks, where we say, "In Panel One, we heard this, and in Panel Two, we heard this," because all of you guys have been here all day. I think we've gotten a tremendous amount out of this. The story isn't written yet. We have until June 30th to collect your feedback and then to start seriously processing it, so thank you. Enjoy the rest of your week, and good night. [Applause]