

1 UNITED STATES FEDERAL TRADE COMMISSION

2

3

4

5 COPPA RULE REVIEW ROUNDTABLES

6

7

8

9 FEDERAL TRADE COMMISSION

10 CONFERENCE CENTER

11 601 NEW JERSEY AVENUE, N.W.

12 WASHINGTON, D.C.

13

14

15

16 WEDNESDAY, JUNE 2, 2010

17 8:45 A.M. TO 5:15 P.M.

18

19

20

21

22

23

24

25 Reported by: Susanne Bergling, RMR-CRR-CLR

CONTENTS

1		
2		
3	OPENING REMARKS:	7
4	David C. Vladeck	
5		
6	PANEL ONE:	11
7	Mary K. Engle, Moderator	
8	Phyllis H. Marcus, Moderator	
9	Michael F. Altschul	
10	Angela Campbell	
11	Edward Felten	
12	Jeff J. McIntyre	
13	John B. Morris, Jr.	
14	Michael Warnecke	
15		
16	PANEL TWO:	74
17	Richard Quaresima, Moderator	
18	Mamie Kresses, Moderator	
19	J. Beckwith ("Becky") Burr	
20	Jeffrey Greenbaum	
21	Christine N. Jones	
22	Gwenn Schurgin O'Keefe	
23	Guilherme C. Roschke	
24	Phyllis B. Spaeth	
25	Phil Terzian	

1	PANEL THREE:	138
2	Jessica Rich, Moderator	
3	Michelle Rosenthal, Moderator	
4	Maureen Cooney	
5	Matt Galligan	
6	Sheila A. Millar	
7	Kathryn C. Montgomery	
8	Paul Ohm	
9	Jules Polonetsky	
10	Heidi C. Salow	
11		
12		
13	PANEL FOUR:	208
14	Mamie Kresses, Moderator	
15	Phyllis H. Marcus, Moderator	
16	Jules Cohen	
17	Rebecca Newton	
18	Martine Niejadlik	
19	Alan Simpson	
20	Denise Tayloe	
21	Ron Zayas	
22		
23		
24		
25		

1	PANEL FIVE:	271
2	Phyllis H. Marcus, Moderator	
3	Mamie Kresses, Moderator	
4	Parry Aftab	
5	Dona Fraser	
6	Roslyn J. Kitchen	
7	Susan Linn	
8	Peter Maude	
9	Izzy Neis	
10	John Smedley	
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		

1 P R O C E E D I N G S

2 - - - - -

3 MS. KRESSES: Good morning. If everybody will
4 take a seat, we are going to try to get started. We
5 have a lot to do. Thank you.

6 We are delighted to have you here to discuss the
7 review of COPPA. We have five panels today that touch
8 some of the issues that we think are exciting and
9 challenging. There are many, many more issues in our
10 Federal Register notice, and we invite everybody to
11 please think carefully about them and do submit comments
12 on them.

13 The format we would like to have today, if
14 possible, is a very informal one. We would like the
15 audience to feel free to participate in the discussions.
16 So, if there are comments or questions that are
17 pertinent to the point being raised up here at the
18 table, feel free to raise your hand and ask for a
19 microphone. We are going to try that and hope that it
20 creates a free flow of dialogue. If it gets too
21 complicated or too disruptive, then we will go back to
22 just questions and comments at the end of each panel,
23 but let's give that a try.

24 In a moment, I'll introduce our bureau director,
25 but I have to make this required statement before we do.

1 This is our security briefing.

2 So, you should know that anybody who goes
3 outside the building without an FTC badge will be
4 required to go back through security and the x-ray
5 machine prior to re-entry into the conference center.
6 If there is a fire or another reason for evacuation, we
7 will all leave the building, and we will go outside,
8 across the street, and stand in front of Georgetown
9 University. One of us will put up a hand and let you
10 know where the conference attendee section is. So, if
11 that happens, everybody just pay attention.

12 In the event that there is any sort of emergency
13 and it's deemed to be safer to stay inside, then we will
14 tell you where to go.

15 And finally, if you suspect any suspicious
16 activity, please report it to one of the conference
17 planners, and we will have it looked into. I believe
18 that's it.

19 Oh, yes. And for those of you who haven't been
20 to this building before, when you exit the conference
21 center, to your right, right behind the elevators, are
22 the bathrooms, men's and women's bathrooms.

23 We will also have several breaks, brief breaks,
24 during the day between sessions, and we are going to try
25 to keep to those as best as we can. We will have a few

1 slides with the language of the Rule, the pertinent
2 parts being discussed, and also let you know when the
3 breaks are coming.

4 So, finally, I would like to introduce our
5 Director of the Bureau of Consumer Protection, David
6 Vladeck. I think most of you know him, so I am not
7 going to say anything more.

8 And we really, really look forward to a
9 productive, open day. Thank you.

10 (Applause.)

11 MR. VLADECK: Good morning, everyone. We are a
12 federal agency on the move. We are actually starting a
13 panel before 9:00 a.m. I'm delighted to welcome you
14 here today for the 2010 COPPA roundtable. We have
15 picked an auspicious month to do this. Twelve years ago
16 this month, in what now seems to be the dark ages of
17 technology, the Federal Trade Commission issued a report
18 to Congress on privacy online.

19 Our June 1998 report, which I know many of you
20 in this room had a hand in drafting, recommended that
21 Congress "develop legislation placing parents in control
22 of the online collection and personal use of information
23 from their children." The notion was supported by
24 industry and the advocacy community, and just four short
25 months later, the Children Online Privacy Protective

1 Act, or COPPA, was born.

2 At the time, approximately 14 percent of
3 American children were online. I know this well,
4 because at the time my sons were 10 and 12 years old.
5 Using the Internet for homework -- but not much --
6 informal learning, browsing, games, and, according to
7 our report, "corresponding with electronic pen pals by
8 email, placing messages on electronic bulletin boards,
9 and participating in chat rooms."

10 Their growing presence online was seen as
11 creating enormous opportunities for marketers. It also
12 presented safety concerns, as children were able to come
13 into contact with strangers without any parental
14 involvement and awareness.

15 And let me just, as an aside, say that the
16 problem that parents face today is a problem they still
17 face, which is by the time their kids are 10 or 12, they
18 are so much more technologically proficient than the
19 parent is that the idea of direct parental controls is a
20 difficult one to understand.

21 Now, let's fast forward 12 years to where we
22 stand today. According to a 2010 Kaiser Family
23 Foundation study, 84 percent of youth ages 8 to 18 have
24 Internet access at their homes, and in a typical day, 70
25 percent of 8- to 18-year-olds, in fact, go online. The

1 Kaiser study showed that the average young American
2 today spends practically every waking moment, except for
3 the time in school, using a smart phone, a computer, a
4 television, or another electronic device.

5 So, what do they do when they're online?
6 Activities only computer scientists or science fiction
7 writers among us could have conceived of in 1998. They
8 visit social networking sites, they download music, they
9 post and watch online videos, they watch TV online, they
10 create their own avatars, and move through online
11 virtual worlds.

12 And the concept of the computer, boy, that has
13 changed, too. Forget the clunky PC with the
14 freestanding tower. Now, a computer is something that
15 you hold in the palm of your hand and tuck into your
16 pocket. It gives you instant access to the Internet and
17 a host of online services barely imaginable just five
18 years ago.

19 Really, had we ever heard the term "app" before
20 the iPhone? Did we really know that the word "friend"
21 could be a verb? In just a few years, birds have gone
22 from the only things that tweeted to some sort of
23 anachronism.

24 Today, two-thirds of all 8- to 18-year-olds own
25 their own cell phones. It's just stunning. The

1 statistics are even more astounding when you consider
2 that 31 percent of 8- to 10-year-olds have a cell phone
3 and that 69 percent of 11- to 14-year-olds also own cell
4 phones. So, these devices are now ubiquitous.

5 Our rule review, including today's roundtable,
6 is all about how well this statute, this 12-year-old
7 statute, has stood the test of time in light of all
8 these head-spinning technological changes. We're taking
9 a look at the statute, even though we did just five
10 years ago, because things have changed that much.

11 Today, we're going to ask some fundamental
12 questions about COPPA. Is the basic requirement of
13 prior parental consent still sound? Does the COPPA
14 statute's coverage of websites located on the Internet
15 and online services reach the kinds of electronic media
16 children engage in today? How do we deal with the
17 statute's requirement that general audience websites
18 have "actual knowledge" that they are collecting
19 personal information from a child when we have no real
20 means of verifying age-identifying children? Should the
21 item of individually identifiable information currently
22 set out in the COPPA Rule be expanded to take account of
23 things such as mobile geolocation data or information
24 collected in connection with online behavioral
25 advertising? Are the methods for verifying parental

1 consent, such as using a print-and-send form, obsolete?
2 And are the limited exceptions set out by Congress for
3 the collection of children's online contact information
4 without parental consent being adhered to properly?

5 We've got a lot to cover today and in the months
6 to come as we consider possible changes to the
7 Commission's Rule. So, without further adieu, I look
8 forward to a great discussion and to your assistance as
9 we move forward.

10 I'd like to thank our unbelievably talented
11 staff for putting this together. Mamie Kresses, Phyllis
12 Marcus have taken the lead. I know we're going to have
13 a productive day. Thank you very much.

14 (Applause.)

15 MS. MARCUS: I'd like to call up the speakers
16 for Panel One.

17 (Pause in the proceedings.)

18 MS. ENGLE: Good morning, everybody. My name is
19 Mary Engle. I'm the Associate Director For Advertising
20 Practices here at the FTC, and I'll be moderating the
21 first panel this morning, along with Phyllis Marcus, who
22 is a Senior Attorney in the Division of Advertising
23 Practices and I'm sure is well known to everyone in this
24 room as the head of our COPPA program.

25 The first panel this morning is going to

1 hopefully set the stage for some of the later
2 discussions, because it's going to look at some very
3 basic issues, which are the definitions and scope of
4 coverage of terms like "websites located on the
5 Internet" and "online services," which, as you know,
6 COPPA applies to the collection of personal information
7 from children through those.

8 So, what are the definitions of those terms?
9 What is their scope and extent of coverage? How have
10 they held up over the 12 years? And do they need to be
11 modified or how do they cover current activities and
12 things that are going on?

13 So, with us this morning, I'm very pleased, we
14 have a terrific panel to help us explore these issues.
15 Starting to your left, my right, we have Mike Altschul,
16 who's Senior Vice President and General Counsel of CTIA,
17 the wireless association.

18 Angela Campbell, who is a Professor at the
19 Institute of Public Representation at the Georgetown
20 University Law Center, right across the street, where we
21 convene in the event of an emergency.

22 Ed Felten, who is the Director and Professor of
23 Computer Science and Public Affairs at the Center for
24 Information Technology Policy at Princeton.

25 Of course, here is Phyllis.

1 Jeff McIntyre, who's Director of National Policy
2 at Children Now.

3 John Morris, who's General Counsel and Director
4 at the Center for Democracy & Technology.

5 And Michael Warnecke, who is counsel at the
6 Entertainment Software Association.

7 So, starting off, as Mamie mentioned, we are
8 going to have slides just of some of the terms and
9 definitions that we will have under discussion today.
10 So, COPPA covers operators of websites located on the
11 Internet and online services but only defines the
12 "Internet." It doesn't define "website." It doesn't
13 define "online services."

14 So, starting with the statute's definition of
15 "Internet," we are wondering whether this remains a
16 valid description of what we consider the Internet
17 today, and I'd like to start off asking Ed to address
18 that issue.

19 MR. FELTEN: Sure. Well, so, the definition of
20 Internet here is technology-based, right? It's based on
21 the TCP/IP suite of protocols, which are the basic
22 communication protocols used on the Internet. That was
23 true in 1998, and it's true today as well. And so I
24 think this was and still is a spot-on definition of what
25 "Internet" means, worldwide interconnection and the use

1 of TCP or IP or any of that suite of protocols.

2 MS. ENGLE: So, how extensive would you say the
3 definition of "Internet" is or what does it encompass?

4 MR. FELTEN: Sure.

5 MS. ENGLE: I mean, what about, you know, mobile
6 browsers and things like that that we didn't really have
7 back in 1998?

8 MR. FELTEN: Sure. Well, if you are using
9 your laptop or desktop computer to access anything that
10 you think of as the Internet, that would be covered. If
11 you're using your mobile phone to browse a website, send
12 email, or something, most of the things you would do on
13 a mobile phone, including, say, watching a YouTube
14 video, would be within the scope of the Internet as
15 defined here.

16 So, it's not focused so much on which device
17 you're using to access the website or online service as
18 it is focusing on the basic network technology. And
19 because the Internet is worldwide and is used by such a
20 wide range of services, this is actually quite broad
21 coverage, independent of the access device.

22 MS. ENGLE: Do any of our other panelists have
23 any other comments or different views on this scope of
24 the definition and its currency?

25 (No response.)

1 MS. ENGLE: Okay, good. So, we got that much
2 right, I guess -- pretty good -- back in 1998.

3 Well, what about -- you know, it's kind of a --
4 to me, it sort of seems like a curious language,
5 "website located on the Internet," that the COPPA
6 statute uses. Does that definition limit the scope of
7 the application in any way, "website located on the
8 Internet," or how does that -- what does that mean?

9 MR. FELTEN: Well, I think "website located on
10 the Internet," roughly speaking, would cover anything
11 that you can access through your browser on your
12 ordinary computer or mobile phone. So, if you can
13 access it in Internet Explorer or Mozilla Firefox or the
14 browser that's on your mobile phone, for example, then
15 it is a website located on the Internet.

16 MS. ENGLE: Are there websites that are not
17 located on the Internet?

18 MR. FELTEN: I think that the distinction here
19 would be with something like a corporate intranet, where
20 a company has a website that's set up just for internal
21 use by their employees, and that's not located on the
22 Internet. But if it's generally available, accessible
23 to the public, then a website would be on the Internet.

24 MS. ENGLE: Okay. What about the definition of
25 "online service?" Now, we didn't -- that term was not

1 defined in the statute or the Rule, and somehow we seem
2 like we have an intuitive understanding of it, but the
3 way it was used back in 1998 may have been different
4 from the way we think about it today.

5 Does Ed or others want to comment on -- John?

6 MR. MORRIS: Sure. I mean, I'll jump in on
7 that. My guess is that, you know, if we really put all
8 the members of Congress up on the lie detector back in
9 '98, you know, they thought that online service meant
10 AOL or Prodigy, because those were big online services.
11 But, you know, there's I don't think a reason to try to,
12 you know, narrow that term. I think the term is fairly
13 broad, and I think there is a fairly kind of broad
14 understanding of, you know, websites and nonweb-based
15 services that are available over the Internet. So, I
16 mean, I think the term "online service" can fairly be
17 read to be quite broad.

18 MS. ENGLE: So, "online" is sort of a synonym
19 for "over the Internet," a service that is available
20 over the Internet or connects to the Internet?

21 MR. MORRIS: I think that's fair enough, yeah.

22 MS. ENGLE: Angie?

23 MS. CAMPBELL: Thank you.

24 I was counsel to the Center for Media Education
25 when we negotiated the bill, and I think I agree

1 absolutely with Ed that the "Internet" was intended to
2 be a very broad definition, and "online services" was
3 intended to be a broad or sort of a catch-all term that
4 would cover any service that was made available through
5 a computer or similar device connected to a network.

6 And I actually went and looked in some
7 dictionaries from that time period to confirm my
8 understanding, and the Webster's New World Pocket
9 Internet Dictionary from 1997 defines online as
10 "connected to a network or available from a network" and
11 defines online service -- online information service as
12 "a for-profit firm that makes current news, stock
13 quotes, or other information available to subscribers
14 over standard telephone lines."

15 And the Newton Telecom Dictionary from 1999
16 defines online as "available through the computer.
17 Online may refer to information on hard disks, such as
18 online documentation or online help or connection
19 through a modem to another computer." And then it
20 defines "online services" as "a commercial service that
21 gives computer users, i.e., its customers, access to a
22 variety of online offerings, such as shopping, games,
23 and chat rooms, as well as access to the Internet.
24 America Online and Microsoft Network are examples of
25 online services."

1 So, it was intended to be very broad, obviously
2 included everything on the Internet, but wasn't
3 necessarily limited to the Internet.

4 MS. ENGLE: Mike, did you want to --

5 MR. WARNECKE: Well, I mean, I think that the
6 online service today should be viewed in conjunction
7 with the Internet. If we were to take the view that
8 "online service" applies to any computer network that's
9 not covered by the definition of "Internet," it would
10 greatly expand I think the reach of COPPA in a way that
11 I don't think was intended.

12 MR. MCINTYRE: Okay, here we go. Yeah,
13 absolutely, it's got to be broad. Even in the
14 definition of the "Internet" that we have here, it
15 doesn't just refer to the technological base, but it
16 refers to the possible technological base, which it says
17 are any predecessor or successor protocols to such
18 protocols, such as TCP/IP.

19 For us, there's a great concern as well when we
20 see the growth of the wireless devices, for instance,
21 that the Internet isn't just something that we -- the
22 concerns about COPPA aren't just simply about Web-based
23 access but about communication, and that's the heart of
24 this, is communication. And it's communication in that
25 is information being exchanged? Is it going back and

1 forth? Where does the information end up at? You don't
2 need a Web site for that. You can use that through text
3 messaging.

4 Now, there are some tricky issues once we get
5 into texting, for instance, but absolutely, that sort of
6 communication, that sort of communication over an
7 Internet where information can be gathered and collected
8 through this purpose, absolutely, should be open to
9 interpretation here.

10 MR. FELTEN: So, I generally agree that a broad
11 reading of "online service" makes sense and that it's
12 not necessarily limited to just the Internet, although I
13 do think it would be limited to some kind of wide area
14 network. Congress wrote the statute with the two sort
15 of branches. One branch is "website located on the
16 Internet," and the other is "online service," which I
17 read as being broader. So, it's not necessarily any
18 network, but at least a service that's provided across
19 some kind of wide area network.

20 MS. ENGLE: Mike?

21 MR. ALTSCHUL: In the parallel universe of the
22 FCC just across the mall in Southwest, let's slice this
23 bologna a little thinner, so that depending on the
24 network address as opposed to the content, some messages
25 are categorized as communications -- if they use a phone

1 number, for example, as frequently happens in SMS
2 messaging -- but if the same content is transmitted by
3 the same user over the same wireless device that uses an
4 Internet address, domain name system address,
5 soandso@domain.com, then it's recognized really to be an
6 information or Internet access service.

7 While that may strain some of the applications,
8 in fact, federal courts now have relied on the FCC's
9 distinction in the context of enforcing the TCPA, which
10 applies to telephone calls against certain kinds of
11 commercial marketing activities. So, we just need to be
12 conscious of that distinction.

13 They both use IP formats, but one uses something
14 called SMTP, simple mail transfer protocol, and the
15 other is SMPP, which is the short message peer to peer,
16 typically what kids and teen-agers are using to send
17 messages within a wireless network.

18 MS. MARCUS: So, Mike, how would that map onto
19 the COPPA statute?

20 MR. ALTSCHUL: Well, clearly, if the address
21 used by the user or to reach the user is identifiable as
22 an Internet address, the common domain name system, it
23 is going to easily fall within COPPA. If a phone
24 number, as is often used in a text message, is used as
25 the address, there is certainly -- as I said, there is a

1 parallel universe of law that suggests it's a telephone
2 call and not an Internet service.

3 MR. MCINTYRE: I think there are debates that
4 are beginning to blossom, though, that are questioning
5 that. I mean, even in the recent --

6 MR. ALTSCHUL: There were debates and questions
7 at the beginning.

8 MR. MCINTYRE: Good. Let's continue those,
9 because I think that there's a real concern here that if
10 you have, for instance, the example of two teen-agers
11 that are using texting back and forth as going over a
12 telephone service, which may not be a problem under the
13 COPPA interpretation, but if those two teen-agers then
14 walk into a GameStop, for instance, where they are
15 texting and that information is being gathered by that
16 GameStop of the technology that they're using or how
17 they're using it or even the content of what they're
18 using it in, then at that point you have established a
19 commercial purpose, and I think it is and can be open to
20 COPPA interpretations.

21 MR. ALTSCHUL: Well, again, so far, at least in
22 federal court decisions I've seen, they have gone after
23 conduct like that under TCPA.

24 MR. MORRIS: And, I mean, you know, to the
25 extent that some of Mike's wireless carrier members are

1 providing text messaging services, you know, I think
2 it's actually very unlikely that that would go through
3 anything that the GameStop store could see. If the
4 GameStop store is offering a WiFi-based service, that
5 could well be connected to the Internet. There could
6 well be COPPA implications in that context. But if --
7 so, you know, it's a little unclear, you know, what the
8 GameStop example -- how that actually gets implemented.

9 MS. ENGLE: Anybody? Angie?

10 MS. CAMPBELL: Well, I just wanted to make sure
11 that everyone understood that whether or not something
12 is an online service or a website on the Internet is not
13 the only determination of whether it's going to be
14 covered by COPPA. So many things you might be concerned
15 about, you know, wouldn't be.

16 But just to give a real world example, what Jeff
17 was talking about, there's a service called Foursquare,
18 which is currently offering a promotion with Starbucks,
19 where a user can go into the Starbucks, and then they --
20 it's sort of like a game, where you check in using your
21 cell phone, that you're there, and if you check in a
22 certain number of times, then you get a barista badge,
23 and you can compete with your friends to become mayor of
24 the Starbucks, and if you're a mayor of the Starbucks,
25 which I think means you have been there the most number

1 of times, then you can actually get a dollar off a
2 frappuccino. So, there are commercial applications.

3 Foursquare is actually making the data. They
4 get, through this service to Starbucks or to other
5 retailers that sign up for this service, so that they
6 can get very detailed information about who's checked
7 in, what their gender is, what time of day, what they
8 like, what they don't like, a whole lot of different
9 information for commercial purposes.

10 MS. ENGLE: Well, I think that might be a good
11 segue to the next topic we wanted to talk about, which
12 is mobile communication.

13 Oh, okay. All right, I'll go there. Does
14 anybody in the audience have questions about that before
15 we get to mobile? Yes. Here's the microphone.

16 UNIDENTIFIED SPEAKER: What about
17 noncommercial -- thought I know that the COPPA
18 specifically says "commercial," there's the problem with
19 noncommercial services, such as BitTorrent. How do we
20 deal with those?

21 MS. ENGLE: Well, you know, I think -- I mean,
22 the question in terms of whether BitTorrent is an online
23 service, we had a little bit of a discussion about that,
24 but, you know, the FTC, the scope of our jurisdiction
25 and authority extends to commercial services. I think

1 BitTorrent is -- I mean, obviously, companies that use
2 BitTorrent are in commerce. So, if they are otherwise
3 covered in some way, then we're there, but I don't think
4 that, you know, that protocol raises a particular issue.

5 MR. MCINTYRE: I'll say one small thing to kind
6 of support what Mary is saying, that when you look at
7 BitTorrent or you look at other sort of technological --
8 I hate to call them platforms, but when you look at the
9 sort of processes, one of the things that's really easy
10 to do for regulators and consumers and politicians is
11 very quickly you're kind of glassy-eyed when you start
12 talking about all the platforms that are available, and
13 suddenly we can shift the conversation away from where
14 it's supposed to be in this, which is about children,
15 and suddenly get much more caught up in kind of the TCPS
16 versus the IPs versus the iPads, iPhones, iPods, et
17 cetera, et cetera. It becomes very technologically-
18 based.

19 The heart of COPPA is about protecting children,
20 and so each time that we have these sort of discussions
21 and the questions about a different sort of platform or
22 a different sort of technological basis for the
23 advocates in this arena, what each time we're going to
24 try to do is bring it back to the simple question of is
25 it good for kids? Does it protect kids? Does it put

1 kids at risk?

2 If it does, based on where the current research
3 shows it to or where the public health community
4 believes that it does, then at that point we are going
5 to start asking much more basic questions, other than
6 about kind of the technological platform and however
7 that may empower or disempower that risk.

8 MR. MORRIS: I mean, let me just respond. I'm
9 all for a broad reading of the applicability of COPPA,
10 you know, I think we all do want to protect kids.

11 Now, on the other hand, if it's good to protect
12 kids but it's outside the statute, then it's outside the
13 statute, and, you know, it may be a good idea to protect
14 kids, but -- and, you know -- I mean, no, you know, in a
15 particular way, but if it's outside the statute, then
16 it's outside the statute. So, I mean --

17 MS. ENGLE: So, for example, if Children Now had
18 a children's area on its website, you know, you are not
19 in commerce. You are not a commercial network that
20 would be subject to the FTC's jurisdiction, so
21 technically -- you know, it's that sort of thing. There
22 are limits on our jurisdiction, and -- in terms of who
23 we could actually pursue, yeah.

24 MR. MCINTYRE: And I think that's a valuable
25 question as well, then, because that also opens up other

1 nonprofit companies, if you will, or nonprofit
2 organizations and whether they should have more
3 oversight.

4 Does National Geographic? Does
5 Discovery/Hasbro? Does, you know, these other sort
6 of -- does Common Sense Media? Do these other groups
7 that have that, should there be some sort of privacy
8 consideration as they move forward?

9 MS. ENGLE: Question down here.

10 MR. ALTSCHUL: I just want to --

11 MS. MARCUS: Oh, hold on, Mike. One second.

12 Oh, go ahead, Mike.

13 MR. ALTSCHUL: I wanted to endorse John's
14 statement that we can't read "commercial" out of the
15 statute, and it's very easy to imagine an elementary
16 school setting up some kind of site that allows its
17 students to communicate and to share information with
18 one another over the Internet, and certainly personal
19 identifying information and other information otherwise
20 included under COPPA would be potentially available and
21 be available for use by third parties if the site wasn't
22 properly access-controlled, but, again, that would not
23 meet the commercial definition that's a part of the
24 statute.

25 MS. ENGLE: And it's not just that commercial

1 definition, but also elsewhere in the statute --

2 MR. ALTSCHUL: The purpose.

3 MS. ENGLE: -- it refers to the extent of the
4 FTC's jurisdiction is the extent of the jurisdiction we
5 have under the Federal Trade Commission Act, which is
6 limited to actual practices in commerce.

7 We have one question down here.

8 MS. TAYLOE: Good morning. Denise Tayloe with
9 Privo.

10 My question to the panel is specific. American
11 Idol says to text in a vote. I send it in with my cell
12 phone. They collect my cell phone number. It's now in
13 their database. Is that under COPPA?

14 MS. MARCUS: Mike, do you want to handle that?

15 MR. ALTSCHUL: Well, I think that there's a
16 larger body of law -- that I admit I'm not an expert in
17 -- as to what kind of information the promoters of
18 American Idol have as to their audience and what are the
19 purposes that they're doing their outreach, and perhaps
20 some later panel will be better suited than at least I
21 am to answer that question.

22 MS. MARCUS: Anyone else on the panel?

23 Ed?

24 MR. FELTEN: Well, I think texting in votes is
25 certainly something that occurs online. I think you can

1 make a good argument that, depending on the details of
2 how this works, that it could be an "online service"
3 within the scope of COPPA. As to whether there is
4 information gathered that is personal information within
5 the scope of the statute, that I don't know.

6 MS. CAMPBELL: I would also add, I think it is
7 an online service, but not only do you have to also then
8 show that it's personal information, that it meets the
9 definition of that, but also that they know it's from a
10 child, and, you know, that's a factual question they may
11 or may not know. So, it could be and it may not -- it
12 may be covered by COPPA; it may not be.

13 MS. ENGLE: And later panels will explore those
14 issues.

15 Susan?

16 SUSAN LINN: Yes. I'd like to go back to the
17 question of what is commercial and what is not
18 commercial and your example of a school website. What
19 if there's advertising on the website, on the school's
20 website, or what if the website is funded by a
21 commercial company? Then what?

22 MR. ALTSCHUL: I think those are two different
23 questions. Certainly, there's a model in the area of
24 both schools and not-for-profit organizations where some
25 kind of sponsorship does not change the legal status of

1 the activity, but certainly when something is actually
2 sponsored by a commercial firm for a school, let's say,
3 but as part of that commercial agreement, the commercial
4 entity is entitled to information, I think that under
5 that circumstance, it would fall under the commercial
6 purpose.

7 The kind of ads that the -- you know, in the
8 back of high school yearbooks and so on may enable it
9 but I don't think would change the purpose of the
10 bulletin board or website.

11 MS. ENGLE: Okay. Going back to -- we've
12 touched on actually mobile communications, and, you
13 know, we have been very clear that when a child can
14 access the Web or a WAP site through a mobile device and
15 can provide or disclose personal information through
16 that, that that is covered by COPPA, that COPPA applies,
17 and I just wondered whether there's any disagreement
18 among the panel about that.

19 MR. ALTSCHUL: Well, you know, we had a pre-
20 call, and I think that all of us agreed that any kind of
21 Internet site that you can access over a desktop can
22 also be accessed today over a mobile device. And I
23 should say, that's true using commercially licensed
24 spectrum as well as the kind of WiFi access that's
25 available in this room and, you know, increasingly in

1 all other rooms. But the devices are increasingly
2 agnostic as to what kind of spectrum they interconnect
3 with to access content on the Internet.

4 MS. ENGLE: So, let's talk a little bit more
5 about the types of online services that can be accessed
6 via mobile devices. We heard about Foursquare, for
7 example, that's at a location, Angela mentioned, and
8 others. I probably should have -- if my 12-year-old
9 were here, she could probably tell me more about what
10 she does on her smart phone and the types of apps and
11 services than I personally use.

12 So, anybody want to volunteer to talk about what
13 kinds of online services or services that, you know, we
14 would agree are covered that you can access through
15 mobile devices?

16 Angela?

17 MS. CAMPBELL: Well, I went on my iPhone and
18 looked at the apps, and there is actually quite a large
19 number of apps that are specifically designed or appear
20 to be specifically designed for children to teach
21 letters and numbers and things like that. So, I think,
22 again, you can't just say all apps are online services
23 or all apps are not online services. Some of them will
24 be; some of them won't be.

25 If apps do allow children to receive targeted

1 advertisements or to purchase goods and services, to
2 play games that are connected to a network, to obtain
3 information, to get access to the Internet, those would
4 be examples of online services that could be subject to
5 COPPA. If you're just, you know, downloading a game and
6 you're just playing the game on your phone and there's
7 no network connection, then that would not be an online
8 application.

9 MR. FELTEN: So, the way this part of the
10 statute is structured, it matters not so much what is
11 happening on the end device, whether you're in a browser
12 or in a, say, mobile phone app. What really matters is
13 the nature of the service and how it's provided across
14 the network. If it is either a website provided across
15 the Internet or if it is an online service under the
16 broad understanding that we generally seem to share
17 here, then regardless of whether it's accessed on a
18 mobile device or a stationary machine, regardless of
19 whether it's accessed via a website or via an app, it
20 would still be within the scope of COPPA. Again, it's
21 the nature of the service.

22 MR. MORRIS: I mean, I would suggest that we be
23 precise to figure out who might be covered. I
24 absolutely agree that if there is an app on my Android
25 phone -- I don't have an iPhone -- but if there's an app

1 on my Android phone that accesses an online service that
2 goes out and retrieves information or, you know, allows
3 me to post information, there's clearly an online
4 service involved. There's clearly COPPA applicability.

5 But I would suggest that the software designer
6 of the app may not be an operator of an online service.
7 He or she may just have written a piece of software and
8 made it available and then had no further connection to
9 the communication, no later involvement.

10 And so for that kind of individual, I would say
11 that the designer of the actual software is probably not
12 an operator of an online service, but to the extent that
13 software connects to an online service, then absolutely,
14 the operator of the online service is COPPA-covered.

15 So, I mean, you know, I think that one just needs to be
16 precise when we're talking about apps as to who might be
17 covered.

18 MR. FELTEN: Just if I could expand a little on
19 what John said, and I agree with that. If you look at
20 an example like Foursquare, which is a service for
21 recording your location over time and publishing that
22 information, Foursquare is an online service, and you
23 might access it via the Web, you might access it via,
24 say, an iPhone app that came from the Foursquare
25 company, or, in principle, you might access a service

1 like that via an app that was written by some third
2 party.

3 And as John points out, in a case like that,
4 where you're using an app that was provided by a third
5 party, which does nothing more than connect to
6 Foursquare's servers and provide information to
7 Foursquare servers, it seems to me that Foursquare, the
8 company, is providing the online service, and the app
9 developer is not necessarily an operator of an online
10 service, as the statute would have it.

11 Also, by the way, the operator of, say, the
12 wireless network that is used to transmit those bits up
13 to Foursquare in that scenario also is not the operator
14 of the online service.

15 MR. ALTSCHUL: That's the part of this panel I
16 like the best.

17 MR. MCINTYRE: I would indicate a great amount
18 of comfort with this, because it definitely begins to
19 draw some lines into some areas that can be gray and can
20 be an area where some kind of a tricky definition can
21 come up on this.

22 I think what's important with this is that as
23 it's been -- it's -- well, it is. It's cliché to talk
24 about the technology moving so fast right now, and so I
25 think the trick with the regulators in this instance is

1 being able to write language for a proposed regulation
2 in this area that is broad enough to be able to still
3 apply to that dynamic of collecting information on
4 technologies that we may only really kind of grasp that
5 are out there, kind of get an idea of protecting that
6 dynamic of information collection around children.

7 I don't know if the trick to that is being able
8 to be specific, like you're saying, to protect the
9 software developer, and instead going to Foursquare than
10 the online developer that may actually be collecting
11 that information. But, you know, we look back now at
12 1997 and 1998, you know, technologically as kind of the
13 quaint good ole' days, but, oh, God, how did I survive
14 with dial-up?

15 We want to be able to make sure that we allow
16 the language here to not just pull out the specific
17 instances and then give hard regulation about what we
18 know that exists, but also to be broad enough to be able
19 to apply itself so we don't find ourselves and the
20 Federal Trade Commission isn't outdated within 18
21 months.

22 MR. WARNECKE: If I could add something on that,
23 I mean, I think it's important when we're looking at
24 these scope issues to also consider the fact that not
25 all instantaneous communications are necessarily going

1 to fall within the scope of COPPA. I mean, you could
2 have a situation where the communication is not
3 utilizing the Internet, where it's not utilizing a
4 worldwide network of networks, but that personal
5 information is being communicated.

6 So, for example, let's say that six people in
7 the audience here had generic tablet computers and those
8 tablets had a dual connection mode that would allow the
9 users to connect to each other either through the
10 Internet or in a limited geographic region through
11 another technology that doesn't follow a wireless access
12 point or any cables.

13 Now, in the first instance, yes, the definition
14 of "Internet" would apply, but in the second sentence,
15 that instantaneous communication through a local, very
16 defined geographic area, that I would argue would not.
17 So, we need to be careful when we're looking at how
18 broadly it applies to new communications to keep that in
19 mind, and I think that would even be consistent with
20 what Ed was saying earlier about even online service
21 would have some limits in terms of how broadly it would
22 be defined.

23 MS. MARCUS: So, in your case, the tablet
24 communications would be neither a website located on the
25 Internet nor an online service?

1 MR. WARNECKE: That's my position.

2 MR. ALTSCHUL: And there are some -- I think the
3 software writers have locked down the vulnerabilities,
4 but there are certain kinds of access ports to wireless
5 devices, infrared and Bluetooth, that there were
6 commercial applications being designed to sort of
7 capture the information about that device, the phone
8 number and other aspects of the device, for people who
9 were just walking by an airport concourse or whatever
10 that was enabled to read and capture that kind of
11 information. That's not going over the Internet, but
12 that certainly would qualify as PII under, you know,
13 many contexts.

14 MS. MARCUS: We have a question from the
15 audience.

16 MR. GALLIGAN: Matt Galligan from SimpleGeo.
17 I'm on a panel a bit later.

18 But you've talked about computers, mobile
19 devices, but there are many other connected devices that
20 can access the Internet or wireless protocols. Great
21 examples would be video game devices, so Xbox, and
22 specifically speaking to your point, the Nintendo DS
23 comes prepackaged with a bit of software called
24 PictoChat, and PictoChat can create a local network
25 where anybody that is on that local network can

1 communicate with other people. That completely
2 circumvents the Internet, but anybody that is actually
3 connecting to that local network can communicate with
4 each other.

5 And so it could be, you know, the 10 DS users
6 around or it could be the 10 DS users around and the
7 11th that's sitting outside of the building that could
8 be communicating with those 10 people, and so that
9 software itself is providing communication, but there
10 are potential dangers there with the communication that
11 is going on, because it is circumventing the Internet
12 completely, but it's meaning that there are other people
13 that are being connected locally through a similar
14 service that you would find on the Internet.

15 MS. MARCUS: Matt, that's an excellent question,
16 and I'm going to ask the panelists to hold the answer,
17 because we are about to get to interactive gaming, but
18 thank you for raising that.

19 MS. ENGLE: Okay. So, we have been -- oh, one
20 more question from the audience.

21 MR. SAMET: Shai Samet with kidSAFE Seal.

22 You know, I just want to go back to a comment
23 that was made earlier about a question that was asked by
24 Denise regarding the American Idol text submission. I'd
25 like to understand. It seemed like there were some

1 contradictory remarks as to whether that would be
2 covered or would not be covered. I'd like to understand
3 what is it about this definition that would cover the
4 submission of a text message back to American Idol in
5 that example.

6 MS. MARCUS: John, do you want to --

7 MR. MORRIS: I'm not sure I do, but, you know, I
8 think Mike was suggesting that, you know, if it's a pure
9 telephone call not using an Internet-based address, that
10 possibly it is not covered by COPPA. You know, my
11 impression is that the wireless companies are pretty
12 sensitive, you know, on COPPA issues in general, and so
13 I'm not sure it actually makes a difference in terms of
14 their behavior as to whether it's kind of online or
15 offline, but I think one could argue that if it is just
16 something that happens on the telephone network, that
17 it's not covered by COPPA.

18 MR. FELTEN: I would disagree with that to the
19 extent that I don't think that something being provided
20 across, let's say, text messaging as a medium would
21 necessarily put it outside the scope of what is covered.
22 A service provided via text messaging, for example,
23 might be an "online service." It would not be a
24 "website provided on the Internet," but the Internet
25 limitation applies only to the website side of the fork,

1 if you will.

2 Now, in the case of American Idol, it does seem
3 to me that there's a reasonable argument that collecting
4 votes could be seen as an "online service," but whether
5 this meets the other requirements of the statute,
6 collection of personal information and knowledge that
7 there's a child and so on, that I don't know.

8 MR. ALTSCHUL: And we had discussed that factor,
9 the knowledge of the child, which is really a fact-based
10 inquiry. Television producers spend a lot of time
11 targeting and knowing the demographics of their viewers
12 and targeting advertisement -- selling advertisements
13 based on the demographics of their viewership. So, you
14 would have to determine -- I'm weak in popular culture,
15 so I can't tell you who advertises on American Idol, but
16 whether it's products that are designed to be purchased
17 by people who are older than 13 or under 13 would be
18 part of the fact-based inquiry.

19 MS. ENGLE: Well, that is a separate issue, and
20 I think -- so, I gather we really don't have agreement
21 at the table about whether text messages like that, that
22 kind of voting at American Idol, are covered right now.

23 MR. MORRIS: You know, I was not kind of trying
24 to urge disagreement. You know, I think one could make
25 an argument that if it is wholly on the telephone

1 system, it might not be reached here. I'm actually
2 personally quite comfortable with Ed's push-back to say
3 that this could easily be an "online service." You
4 know, again, it's correct to say it's not clear in most
5 texting contexts whether there's any direct knowledge,
6 and I have no more cultural knowledge than Mike does,
7 but I don't think that American Idol is aimed at the 12
8 and under set. I think it's more aimed -- but I may be
9 wrong.

10 MS. MARCUS: We have, I'm sure, some
11 disagreement on that in the room.

12 MS. ENGLE: That's a separate issue, I think.

13 MS. MARCUS: Right.

14 MS. ENGLE: But I think this is an area where we
15 will definitely want written comments, so it's something
16 to keep in mind as you're preparing written comments,
17 that particular issue. Is that something that is clear
18 or something where we would need clarification? And
19 that's going to apply throughout a number of other
20 issues.

21 You know, as you know, we have more flexibility
22 in the changes we make to the rule. If there needs to
23 be a change in the statute, that's something that
24 Congress will need to do. So, any views on this issue
25 would be very helpful to us.

1 MR. MCINTYRE: I might offer this, that I don't
2 think this reflects a disagreement as much as it
3 reflects kind of a threshold or a burden by which then
4 other panels may explore today, that if this is a
5 text-based service, if they determine the information is
6 being collected, if it is determined that a child is
7 submitting that information, then at that point, I think
8 the burden shifts, and we can kind of reframe the
9 conversation then about whether this particular instance
10 of the American Idol issue becomes then an online
11 service.

12 If those other things are held up as verified,
13 if they are children and they are submitting information
14 and it is collected, then that, I think, reframes this
15 conversation.

16 MR. ALTSCHUL: It may not be the best example,
17 because as I recall, 800-number voting is the alternate
18 mechanism for voting on American Idol, which is just a
19 traditional telephone network activity, and the
20 particular architecture used for this kind of short
21 message service is a virtual private network
22 architecture. Nothing is being translated or flowing
23 over the traditional network to network.

24 MS. ENGLE: So --

25 MS. MARCUS: Well, hold on, Denise. Let's keep

1 moving through our questions.

2 MS. ENGLE: So, kind of related to the question
3 of what information, you know, in the case of American
4 Idol, the texting and votes is just voting for somebody,
5 but in other situations, information may be being
6 collected, personal information, from the person or the
7 child, and I'd like to have a little bit of a discussion
8 about that.

9 What types of personal information are collected
10 through apps and how does that vary and is it more
11 active versus passive collection of information?

12 Mike?

13 MR. ALTSCHUL: Well, one piece of information
14 that typically will be collected will be the telephone
15 number associated with the wireless device, and the
16 COPPA statute does identify telephone numbers as
17 personal information. Interestingly, the
18 Telecommunications Act and Section 222, which deals with
19 similar kinds of issues, thanks to the lobbying
20 activities of directory publishers, does not include
21 telephone numbers and names and addresses as personal
22 identifying information.

23 So, we end up back on the horn of the dilemma.
24 Is a message sent using a phone number going to fall
25 under the Communications Act rules for telephone call

1 messages or will a message sent using an IP protocol
2 fall within COPPA and have the telephone number be
3 treated as personal information?

4 Another increasingly frequent source of
5 information is location information, and location
6 information is not provided without notice and consent
7 to the customer and subscriber, oftentimes the user.
8 The child may not actually be the subscriber to the
9 service; it would be the parents on a family plan. And,
10 you know, depending on the application when it's
11 downloaded, for example, if you download Google Maps to
12 your wireless device, there will be a long, you know,
13 terms of use license agreement which provides notice,
14 and presumably customers give consent to then provide
15 that location information in using any location-based
16 services enabled by their software.

17 So, those are the two fundamental pieces. the
18 telephone numbers provided by the network and
19 location-based information today -- and it's changed
20 just in the last two years or so -- increasingly is
21 provided by the wireless device without the involvement
22 of the wireless carrier.

23 MR. MORRIS: I am just going to toss out that
24 you should be aware that there is a huge diversity of
25 information that technology designers are designing the

1 platforms to allow to be transmitted from the devices.
2 I'm very involved in an ongoing standards discussion at
3 the Worldwide Web Consortium where we're discussing the
4 privacy implications of this kind of device's ability to
5 be able to transmit to a website the ambient temperature
6 in the room, the ambient noise level, the light level,
7 you know, a whole range of environmental facts, some of
8 which could have, you know, privacy implications.

9 I mean, you know, one could actually determine,
10 you know, where someone is not; you know, you can rule
11 out locations by knowing, as they're thinking about
12 doing, the barometric pressure kind of. There are
13 devices that are being designed that will, you know, be
14 able to convey the barometric pressure. And you can
15 say, well, you know, I know that that person cannot be
16 in this location if the baro -- you know, so there
17 are -- there's a huge diversity of information.

18 So, I mean, you shouldn't focus on just what's
19 available now. You should, you know, recognize that
20 there are things coming down the pike, applications and
21 devices that we really haven't kind of seen in the
22 market yet.

23 MS. ENGLE: And that's going to -- you know,
24 later on, we'll have a discussion of what constitutes
25 personal information, and as you know, that one of the

1 elements is that it allows you to contact a child online
2 or offline. So, perhaps that type of information will
3 be relevant to that, you know, if they are standing
4 inside or they are outside the building, for example.
5 Okay.

6 MS. MARCUS: In helping us think through the
7 information that's collected through mobile apps, does
8 it help for us to divide them between information that's
9 actively provided by users and information that's
10 passively collected from a user on the device, or
11 perhaps between applications that a user must pay for
12 versus those that are free? I'll throw this out to the
13 panel. Anyone?

14 MR. MCINTYRE: Can you define "active" and
15 "passive"?

16 MR. FELTEN: Well, I think what's intended here
17 is to draw a distinction between information that's
18 actively entered by the user versus information that's
19 just gathered. So, something like the barometric
20 pressure, if the device can measure that, leaving aside
21 whether it's personal information, that's information
22 that is collected by the device of its own accord. A
23 physical location also might be collected by the device,
24 as opposed to information like the user's name, which is
25 inherently going to be entered by a person.

1 So, it might be useful, just in thinking these
2 things through, to think about those cases -- to divide
3 those cases, although the language of the statute would
4 cover them both. It just talks about information being
5 collected.

6 MR. MORRIS: But, I mean, I -- I agree, but you
7 also might even need to have a third category or at
8 least recognize that in the passive category, you know,
9 when you install an app on this device, at the time of
10 installation, it will tell you the seven different data
11 points that this app uses and it transmits to the
12 network, and you have to agree to it.

13 So, you know, I suppose you might view, then,
14 that as passive after you've done the agreement, but
15 I -- so that there is passive data collection that
16 there's been no consent, no notice for at all. There is
17 somewhat passive data collection where you agreed when
18 you installed the app that this could be transmitted.
19 And then there's what you're actually typing in.

20 MR. FELTEN: So, the consent issues are likely
21 to be different in these cases, at least the way you
22 think about it, it is likely to be different in a case
23 where a user actually actively typed something in versus
24 one where it's gathered maybe with some kind of consent
25 in advance; maybe not.

1 MR. ALTSCHUL: To complicate it even further,
2 there's the concept of implied consent, which is neither
3 active nor passive but somewhere in the middle. The
4 granddaddy of this kind of consent is for 911 calls or,
5 more recently, for concierge-type services where you
6 want driving directions.

7 So, in dialing 911, the Justice Department has
8 opined that the caller wishes to disclose their location
9 so they can be rescued or assisted by the dispatcher
10 without ever expressly consenting to provide their
11 location information. In using a location-based app to
12 find the nearest gas station, you can extend that to
13 say, well, if I'm looking -- if I've asked the app to
14 provide the nearest gas station, I'm consenting to
15 provide my location so that the app can figure out where
16 I am to find the nearest gas station.

17 MR. MCINTYRE: I'd like to make just a quick
18 shot at getting some unanimity on this just to make sure
19 no one on the panel is talking about getting informed
20 consent from a child. That is, we talk about loading
21 these applications and loading these apps, that the idea
22 of getting informed consent from a child underneath the
23 age of 13, much less in a younger age, is something that
24 does not exist.

25 Children developmentally cannot make that

1 decision for themselves, should not make that decision
2 for themselves, and don't have the developmental
3 capacity to be able to do that, and any commercial
4 application that relies on that in any capacity then
5 absolutely falls under this.

6 When we're talking about consent then at that
7 point, what we're talking about is parental consent for
8 the application used by a child, and that's a very
9 different thing. If we're talking about location
10 devices, that's a little different. That begins to get
11 into a gray area, at which point then we begin to argue
12 about the definition of commercial intent. You know,
13 GPS locators, no problem; OnStar, no problem; that sort
14 of stuff, no issues in the public health community for
15 that sort of stuff. In fact, you'll probably find a
16 great amount of advocacy for that sort of stuff.

17 But once that turns into a locator device to let
18 you know, as Angela's example was earlier on, that when
19 you're pinged that you're in Starbucks and you are able
20 to get points for that based on your location, then the
21 question changes.

22 MS. MARCUS: All right. And what you've pointed
23 out is COPPA's regime. I mean, it was not consent from
24 the user itself, but consent from a parent that was
25 anticipated.

1 MR. FELTEN: There's one more piece of your
2 initial question which we haven't addressed yet, and
3 that is whether an app is free or costs money, and I
4 don't think that matters in itself. The statute
5 requires that the website or online service be operated
6 for commercial purposes, but often a website or service
7 that's operated for commercial services provides an app
8 for free to the user, which is their interaction with,
9 and if that's the case, it would still be covered.

10 MS. ENGLE: So, turning now to interactive
11 gaming, which somebody earlier asked a question about
12 and wanted to address more specifically. So, would a
13 company that offers interactivity on a gaming device,
14 whether a handheld or a console, be an operator under
15 COPPA?

16 Mike, did you want to address that?

17 MR. WARNECKE: Sure. Perhaps, but I think you
18 need a little bit more information to answer that
19 question. I don't think mere interactivity alone is
20 determinative of the answer. You would have to figure
21 out what the device maker is doing with the information
22 that it's receiving, and if it's merely passing it
23 through as a conduit, then no, I don't think that
24 interactivity would make them an operator.

25 If, however, it's collecting and maintaining

1 that information and if it's doing so in a way that it's
2 aware that it's directed to children or that it has
3 actual knowledge that kids under 13 are involved, then
4 you would maybe be an operator. You would have to look
5 at the FTC factors for being an operator. But I think
6 the main point here is that mere interactivity alone is
7 not determinative.

8 MS. MARCUS: Can you refine that distinction?
9 What would be the type of interactive gaming activity
10 that would be a conduit only?

11 MR. WARNECKE: You could have a situation, for
12 instance, where there is a Web browser capability in the
13 device but that the operator isn't collecting any -- the
14 game device operator -- or, I'm sorry, the game device
15 maker isn't collecting any information, but just
16 enabling the user to access the Internet.

17 MS. MARCUS: Does anyone have refinements on
18 that?

19 Angela?

20 MS. CAMPBELL: Well, it's clear that COPPA
21 covers chat rooms, and it seems to me that you could
22 have a situation where kids are communicating with each
23 other on their DS, for example, and it really is the
24 equivalent of a chat room, even if the information is
25 not being necessarily collected and used. So, I think

1 in that situation, again, parental consent would be
2 required.

3 MS. ENGLE: We had some earlier, I think,
4 opinions that if it's just a local network, so a few
5 kids in a room chatting with each other, I think we
6 heard an opinion earlier that that would not be covered
7 if it's not going over the Internet. Was there a
8 difference of opinion on that?

9 MS. CAMPBELL: I don't think it has to do with
10 geographic location necessarily. I mean, I think it has
11 to do with whether it's really a chat room where kids
12 are disclosing information, where parents don't have any
13 control over who is actually getting that information.
14 I think parents have to consent to that if they want
15 their kids to be able to do that under COPPA.

16 MR. WARNECKE: Well, I mean, a couple of
17 responses to that. First of all, I mean, I think that
18 goes to the basic question that we were addressing
19 earlier, though, that there are limits on the scope of
20 COPPA. It does apply only to certain networks and not
21 to every, you know, local communication that may occur.

22 But secondly, I think a larger point to make is
23 this, that the consoles have built within them parental
24 control functions that allow parents to limit this
25 information at the git-go, and so I think when we're

1 considering these issues, we need to be aware of that
2 backdrop of the parental controls that specifically
3 allow parents to address those issues.

4 MR. MORRIS: And, I mean, I would push back a
5 little bit, you know, for a DS that allows, you know,
6 essentially peer-to-peer communication within the room,
7 within the distance of a WiFi signal, you know, every
8 single computer laptop available can do that, and so my
9 question is since my child could take this laptop, could
10 create an ad hoc wireless network, and could communicate
11 with another child in the same room on an ad hoc
12 wireless network, there is nobody else involved in doing
13 that, does Apple in this case have a COPPA obligation to
14 get the parents' consent for that communication?

15 I would say that's not really workable. I'm a
16 little, you know, kind of anxious about the idea that
17 the maker of a device that has WiFi capability has a
18 COPPA obligation without more, without being somehow
19 involved in providing an online service that allows
20 communication. So, I'm a little -- I'm worried that
21 we're going too far here.

22 MS. ENGLE: So, who is the operator? Angela,
23 who would you consider then who had the obligation to
24 get parental consent in that situation? Nintendo who
25 makes the DS or who?

1 MS. CAMPBELL: Well, I mean, there's a lot of
2 questions, and I think there are probably some gray
3 areas here, but I think you have to go back to what the
4 purpose of COPPA is, to protect children and to provide
5 a way for parents to know when they're interacting with
6 complete strangers or where other people may be
7 collecting information about them. And so, you know, I
8 think we have to talk about specific situations.

9 MR. MCINTYRE: If I may offer on this, I mean,
10 if we can get guarantees that these sort of
11 communications are happening in a closed network, then I
12 have got no problem with that. I mean, we're
13 essentially talking, to use a 1970s reference, to
14 nothing more than kind of like CB radios. If they are
15 talking to each other through whatever technological
16 platform and it's staying reframed within that space, I
17 don't think there's going to be an issue.

18 The problem here is that the way the technology
19 is formed here is it allows for loopholes in that, and
20 that's where we're concerned. We don't want to
21 overburden the technology or kind of point fingers where
22 they don't need to be pointed, but if I'm convinced that
23 it's six 12-year-olds that are talking, not an issue,
24 but if it's six 12-year-olds and a marketer from
25 McDonald's is suddenly thrown into the mix who can

1 collect information, which will come up in later panels,
2 then at that point, it's an issue. It's the collection
3 of information and it's distributed. It's just a matter
4 of kind of how we pinpoint where -- operator and which
5 is the most appropriate definition for being able to --

6 MR. ALTSCHUL: Doesn't that read back into the
7 statute, though, a commercial purpose, which, you know,
8 we can't read out, and there are different models for
9 chat rooms. Some may be sponsored for free to attract,
10 you know, information -- you know, for a commercial
11 purpose. You can find out who is interested in your
12 products. Other kinds of commercial chat rooms may be
13 offered on a subscription basis. That would also be a
14 commercial purpose.

15 MR. MCINTYRE: Yes, absolutely. We see that the
16 trend in gaming, especially these days, is towards a
17 much more individualized sort of experience. I don't
18 think there's anybody among us that wants to be able to
19 inhibit that sort of technological growth or that sort
20 of individualized experience for the gamer these days as
21 well.

22 The trick comes in in making sure that this
23 isn't an interpretation based on exception but it's
24 based on rule instead and still is able to meet -- take
25 care of the spirit of COPPA while still adhering to the

1 ultimate missions.

2 MS. MARCUS: I'd like a follow-up question,
3 then, to ask a follow-up question of Michael. Most
4 gaming systems, I would say all three of the big three,
5 offer parental controls as options, but in your opinion,
6 is that done as a best practice or because the
7 manufacturers have determined that COPPA applies to
8 those interactive gaming capabilities?

9 MR. WARNECKE: Well, I can't opine on the
10 specific motivations of any one company, but what I can
11 say is this, is that there are interests here that go
12 beyond merely protecting children for purposes of COPPA
13 compliance. There are brand protection issues. There's
14 issues of enabling parents and developing a good rapport
15 with parents to make sure that they have a comfort level
16 with the technology, that they feel comfortable with
17 kids using them and that they have some level of control
18 over what they're engaging in.

19 So, I think the desire to help families provide
20 a safe entertainment experience for their children is
21 the key motivating factor there, and, you know, this is
22 something that was, you know, in place and was done
23 apart from the COPPA compliance, but it's an example of
24 how the marketplace already has some features in place
25 to address these issues, not necessarily just for legal

1 compliance reasons, but because of a desire to enable
2 families to enjoy games in a safe manner.

3 MR. FELTEN: Well, in thinking about this issue
4 of when a game console company might be an operator, it
5 seems to me there are three sort of basic cases that are
6 worth thinking about. One of them is the one that
7 Michael pointed to at first where the game console
8 provides, say, a web browser or a way to access
9 something that occurs elsewhere. Let's say you can use
10 your game console to access Facebook. In that case,
11 there probably is an "online service" or "website on the
12 Internet" involved, but the game console maker is
13 presumably not the operator of it, and so it would be
14 Facebook or whoever else who would have any obligations
15 under COPPA.

16 A second case which we have talked about is the
17 case of communication within a room, let's say, between
18 devices, three kids who have Nintendo DS devices and
19 they're chattering with each other while they play, but
20 they're not connecting to a wide area network for this
21 purpose, and to me, that's not an "online service,"
22 because it's not online or it's not using the Internet.

23 And the third case is, let's say, a chat room
24 which is accessible via the device and which is really
25 available to everyone in the world on which to chat, and

1 there again, you have an "online service" or you have a
2 website and you have to ask who's the operator of it.
3 If it's the game console company also, then yes, they
4 might have some obligation.

5 MR. MORRIS: Just to kind of add onto that, I
6 mean, I think this discussion highlights a critical need
7 for the Commission to, you know, not only ask about and
8 imagine what is possible, but look at what is actually
9 plausible and likely, because, I mean, certainly I could
10 envision a world where McDonald's sends people out into
11 the neighborhood with their DS-Lites and they create a
12 network, and they hope that kids in the neighborhood get
13 online, and then they can market to them without
14 touching an online service, and so maybe they're not
15 COPPA-compliant, but that seems pretty unlikely to me,
16 at least today.

17 I mean, it seems to me that, you know, most of
18 the motion in the technology development is toward
19 greater interactivity, greater connectivity to online
20 resources. I think that it is very likely that most
21 services that we're going to see are going to have an
22 online component, an "online service" component, and
23 even if we can imagine marketing to kids technologically
24 being done in a way that circumvents COPPA, you know, I
25 would suggest that until we actually see that kind of

1 behavior happening, it's not something we need to expand
2 the reach of COPPA to envision a technical possibility
3 when it's, in fact, not a practical or a market or a
4 likely possibility.

5 MR. MCINTYRE: The exceptions always make for
6 bad rules on this, just as we have seen in terms of --

7 MS. MARCUS: But good conversation.

8 MR. MCINTYRE: -- text messaging and closed chat
9 rooms within gaming sites and whatnot as well, and I
10 would argue that I think Google does this already a
11 little bit. I am able to pull up a photo of my front
12 yard, my front door, my truck, and the gear that I have
13 on Google right now, and I can zone in. I was looking
14 for a friend that had bought a house recently in a
15 nearby neighborhood, and I was able to pull up almost
16 every information, including I could zone in and see
17 something that he had placed in his front window based
18 on the Google website. And this is from Google driving
19 around, you know, with their camera on the top.

20 So, I don't think in this particular example,
21 which may not be the greatest example, I don't think
22 it's as much of a reach to be able to say that we may be
23 able to begin to see location-based networks grow up
24 that marketers and advertisers are able to use for their
25 own purposes in gathering information.

1 MS. ENGLE: Okay. We just have a few minutes
2 left and there is a couple more topics that we would
3 like to cover, so we will move on now to interactive TV.
4 Actually -- no, we're good. It's 10:30. I was thinking
5 10:15.

6 So, interactive TV is a broad term that can
7 cover anything from using a wireless remote to purchase
8 product advertised in a commercial or changing the
9 actual viewing of a show that you're watching, and so
10 we're wondering, when would a provider of an interactive
11 TV service be considered an operator under COPPA? And,
12 you know, I am sure everybody knows, we're getting
13 closer and closer to interactive TV being something that
14 people are actually doing and using way more now than
15 just a few years ago when it was announced.

16 So, John or Jeff, did you want to take a stab at
17 that?

18 MR. MCINTYRE: Not really.

19 MR. MORRIS: Well, being a cultural Luddite, and
20 as far as I know, I've probably never used interactive
21 TV, I'm not sure I'm the best source, but, I mean, you
22 know, again, I actually would come back to what I just
23 said a moment ago. You know, I think that, you know,
24 whatever interactive TV was five or eight years ago, you
25 know, may have been being done, you know, using

1 proprietary signals between the cable network head end
2 and the home box, and thus, conceivably might skirt, you
3 know, the TCP/IP-ness that COPPA suggests for the
4 Internet definition.

5 But my impression is that, again, you know, more
6 and more things that are interactive are, in fact, tied
7 in to things on the Web, things -- I mean, you know,
8 we're not moving to a world, you know, where interactive
9 TV is going to be siloed off by itself. It's all going
10 to be, you know, I think a single rich experience, and
11 my guess is that that experience is most often going to
12 involve something that is pretty clearly an online
13 service.

14 And so, you know, I'm not sure that all
15 interactive TV, whatever that was five years ago, would
16 necessarily be an online service, but my guess is that
17 the interactive TV of today and the interactive TV of
18 tomorrow will likely involve an online service, and
19 thus, likely would be covered by COPPA.

20 MS. MARCUS: Angela?

21 MS. CAMPBELL: Yeah, I would agree. I mean,
22 again, I think the statute covers it. I think that we
23 knew back in '98 that digital television was already
24 being talked about. We envisioned it as being able to
25 connect to websites or website-like services, and, in

1 fact, the way it is developing is a way that you can get
2 more information about products; you can purchase things
3 online. So, it's clearly covered as an online service.

4 I just wanted to also mention that the FCC has
5 had a tentative conclusion since 2004 that any
6 interactive advertising targeted to children would not
7 be in the public interest and is not allowed. The
8 Chairman of the FCC said last summer that they were
9 planning to finalize that decision soon. So, I do think
10 that it would be covered by COPPA.

11 MR. FELTEN: I tend to agree. I agree
12 especially I think with John's point, that it's not
13 clear that interactive TV will pose difficult questions
14 beyond the difficult questions we already have in this
15 area; that is, that it's likely to look like perhaps an
16 online service that involves some video as opposed to
17 some entirely different kind of thing.

18 And so whether it qualifies as an "online
19 service" or meets the other requirements to be an
20 operator under COPPA I think will be a similar question
21 to what we would face with other kinds of services.

22 MR. MCINTYRE: I just want to make a brief,
23 quick mention that I think this is really cool, because
24 as recent as 2008, we were being told in the child
25 advocacy community and the public health community that

1 this was really a nascent technology and was something
2 that was probably not going to be -- you know, 10, 15
3 years off or so, that we just really didn't see that
4 these issues were going to arise.

5 And so to be able to have esteemed federal
6 representatives talking about the issues that this is
7 going to represent, especially on the heels of the
8 introduction of Google TV and what we see as the growth,
9 you know, with the interaction of DVRs and those sort of
10 technologies, this is something that's very real.

11 I don't know that it necessarily poses any new
12 issues that are any more tough than what we already
13 have, to mimic what Edward has said as well, but I think
14 when we also look at the arena, kind of what's been
15 happening in terms of online and in terms of the gaming
16 world, when you look at multiuser gaming instances,
17 where they go online, if there are commercial instances
18 and if there's an awareness of children that are playing
19 that, we already have this sort of larger on-screen that
20 can be interactive.

21 I think that's just kind of going to serve as a
22 good, perhaps, metaphorical model for how we are able to
23 view interactive television down the road. It's not
24 going to necessarily be, "Hey, it's cool, I can order a
25 pizza on my TV," but it's going to be much more about

1 the collection of information, that I think we're
2 comfortable with where we're at now.

3 MS. MARCUS: Michael, what are you thinking?

4 MR. WARNECKE: Well, I think that the issues
5 that we're seeing play out in the gaming devices and
6 interactive TV just illustrate the point that when we're
7 looking at "operator," we have to be really careful to
8 look at the specific facts and what's going on with the
9 technology and how the information is being used. It's
10 a little bit hard to address these issues in the
11 abstract.

12 MS. MARCUS: We have a question from the
13 audience.

14 MS. MONTGOMERY: Hi. I'm Kathryn Montgomery at
15 American University, and along with Angela, I was
16 involved in actually leading the campaign that resulted
17 in COPPA. So, it's heartening for me to hear that the
18 statute we all negotiated was written broadly enough and
19 inclusive enough and hopefully with some foresight, even
20 though we didn't know how it would all evolve, that
21 these new forms of marketing to children are covered.

22 I just want to sort of make a comment that we
23 could talk more about how these various platforms are
24 being used for marketing purposes. We've discussed
25 gaming a little bit, but the fact that in-game

1 marketing, in-game advertising is a growth area in all
2 of these platforms, mobile, huge growth areas for
3 marketing and marketing directed at children as well as
4 teens and adults.

5 And I think there are going to be a lot of other
6 questions that we will be addressing this afternoon that
7 will touch on what this is about, but I hope we get to
8 some of these issues.

9 So, for example, with mobile, I think we have to
10 look at how mobile works, how parents are involved in
11 mobile, how one does agree. I think that the questions
12 that Jeff raised are very important, what constitutes
13 opting- in and is it really meaningful, because the
14 purpose of this law was really to protect children from
15 manipulative marketing in the digital media.

16 And so I want to just keep the focus on that and
17 just underscore that I'm glad to see all these platforms
18 are included as we talk more about it.

19 MS. MARCUS: Sure, and just by virtue of design,
20 we had to kind of break up topics so that we can really
21 delve deeply into each one, and as you know, you are
22 going to be participating in a panel a little bit later,
23 and I hope you delve into that, and then we will be
24 talking about parental verification mechanisms in the
25 panel following yours.

1 You know, just to kind of close the loop on
2 interactive television, I think it was John who said
3 that we're going to move toward more television and
4 video -- I think it was said down here, too -- looking
5 like "online services" than others. So, just to note
6 our carve-out or to ask a general question, if it's a
7 broadcast network company that's soliciting interactive
8 participation from a child during the course of
9 programming, for the lawyers among us, would the FTC
10 have jurisdiction under that situation?

11 Mike?

12 MR. ALTSCHUL: I don't know.

13 MS. MARCUS: And, you know, that may --

14 MS. CAMPBELL: Well, why wouldn't they? I mean,
15 we have jurisdiction over broadcast advertisers. I --
16 you know, who do advertising. If they're collecting
17 information that's being used for commercial purposes --
18 absolutely.

19 MR. MORRIS: Although, let me push back -- and,
20 again, if we're talking about COPPA, you know, obviously
21 there are other statutes and things that the FTC
22 appropriately can regulate.

23 Now, if I go onto the street and every
24 tourist -- every young -- you know, every 12-year-old
25 who walks by, I say to them, "Go on Disney.com and have

1 fun," I'm a little skeptical that COPPA would apply to
2 me, to me as just someone who, in a completely offline
3 way, is promoting an online service.

4 And so if a broadcast -- to come back to the
5 hypothetical, if a broadcast network simply airs a plain
6 old commercial that says, "Go online to Disney.com,"
7 well, clearly, Disney.com is an online service that's
8 covered by COPPA, but I'm a little unclear how you get
9 COPPA applying to the broadcaster of that commercial.

10 MR. MCINTYRE: What is this broadcast TV you
11 speak of? It reminds me of the VCRs and the
12 long-playing records we used to use.

13 I'm not sure that there is much -- in terms of a
14 regulatory definition, this is an important conversation
15 to be able to have, because it's going to draw a
16 distinction between where the FTC powers are and where
17 the Federal Communications Commission powers are, and
18 the FCC is still kind of playing that out a little bit,
19 although we have seen indications from their tentative
20 conclusion on interactive advertising that they are
21 going to come out with some protective language there as
22 well, or they will at least reaffirm the protective
23 language there as well.

24 But to kind of play off something that Michael
25 mentioned earlier on is that, you know, all this stuff

1 is going to be integrated, and so the idea that a
2 broadcaster is going to exist as kind of solely in its
3 own individual little bubble out there I think is a
4 broadcaster that's pretty doomed to begin with, and I
5 can't think of many instances -- I mean, you know, there
6 may be legal definitions for how the name is used, but,
7 you know, I think of ABC Disney; I think of NBC/Comcast,
8 if I can say that; I think of, you know, Viacom/CBS; I
9 think of all these services already beginning to merge
10 together.

11 And if a broadcaster is collecting information,
12 then we are going to see it, and we're able to, at the
13 Federal Communications, begin to get some foundations
14 laid out to be able to protect kids in that way, that,
15 yeah, if they just have -- you know, say Nick.com shows
16 up on the screen, then they can't -- you know, that may
17 not fall under COPPA regulations, but at the same point,
18 if that Nick.com flashes on the screen, then there are
19 certain things that can not happen on the website at the
20 same time, such as wholesaling requirements that point
21 to the importance of protecting kids in the online
22 environment in this instance.

23 And so I just don't see -- you know, the
24 broadcaster -- God bless his little airway-based
25 heart -- just may be, you know, as we imagine it with

1 the long-playing record album, an endangered species in
2 this regard and not something I would like to see the
3 Federal Trade Commission really spend a lot of
4 regulatory effort on.

5 MS. MARCUS: Okay. Now, to turn to another
6 controversial topic, we have a question about ad
7 networks and whether an ad network that is serving
8 targeted ads to kids or tweens should be considered an
9 online service.

10 Angela?

11 MS. CAMPBELL: Yes. Actually, in adopting the
12 COPPA rule, the FTC said that if companies collect
13 personal information directly from children who click on
14 ads placed on websites that are online services directed
15 at children or if companies collect personal information
16 from visitors who click on their ads on a general
17 audience site and the information reveals that the
18 visitor is a child, then they will be subject to the
19 Act. So, I think the Commission already has answered
20 this question.

21 But I guess I would add that, you know, an ad
22 network is targeting -- if they're targeting kids, you
23 know, that it's really the functional equivalent to
24 targeting computer users on the Internet and websites,
25 and so, you know, I think there is just no question that

1 it would be covered. You know, that doesn't necessarily
2 mean the website itself is. I mean, you could have a
3 part of a website that is subject to COPPA and another
4 part that's not. But the part that is being used to
5 target ads to kids and to collect information from kids
6 would be covered by COPPA.

7 MR. MORRIS: So, we might have our first
8 concrete disagreement here. You know, absolutely, if
9 there is a website that has ads, that utilizes an ad
10 network, and either the ads or the website is targeted
11 at kids, the website is clearly covered by COPPA, has
12 full COPPA obligations.

13 To suggest that a piece of the website has
14 independent COPPA obligations, what that would lead to,
15 I would think, would be a requirement that two companies
16 gather the full information about the parents when, in
17 fact, the one company that is the operator of the
18 website -- I mean, to me, you know, an ad placed on a
19 website is not an independent website. It is one
20 graphic on a larger website. Clearly, the website
21 operator has to get full, verifiable parental consent.

22 But to suggest that the display of a particular
23 ad, I mean, that would I think suggest then that any
24 piece of the website that, you know, gets displayed to
25 kids might then have to go collect, you know, the

1 information about the parents and all. I mean, it seems
2 to me that when there is clear COPPA culpability for the
3 website, it is unclear to me either whether the statute
4 covers an element on the page, but it's also unclear to
5 me, as a policy matter, whether we want to enforce and
6 create two COPPA interactions as opposed to one.

7 Now, having said that, I mean, if the ad
8 network, you know, crosses different sites, then any
9 website that uses the ad network has to get full COPPA,
10 you know, consent from the parent to do that website --
11 you know, to do the cross-site connection. And, I mean,
12 there has to be full disclosure to the parent about
13 exactly what is happening.

14 So, you know, there shouldn't be an end-run
15 around COPPA, but the website ought to be the
16 responsible party.

17 MS. CAMPBELL: Going back to the legislative
18 history, there is a section-by-section analysis that was
19 put into the Congressional Record by the sponsor of
20 COPPA, Senator Bryan, and he says that the term
21 "operator" is defined as the person or entity who both
22 operates a website or online service and collects
23 information on-site either directly or through a
24 subcontractor. The definition is intended to hold
25 responsible the entity that collects the information, as

1 well as the entity on whose behalf the information is
2 collected. It doesn't apply to the extent that it is
3 just used to -- that it doesn't collect information.

4 So, clearly, we understood from the beginning
5 that you could have more than one entity covered by
6 COPPA, and then there's also FTC cases that have been
7 brought against, for example, Bigmailbox, which operated
8 a chat room that resided on children's websites, and
9 they said that because they collected personal
10 information, that embedded component was itself subject
11 to COPPA.

12 So, I mean, they may be able to work out some
13 sort of agreements that they can share the parental
14 consent, but there clearly is the opportunity for both
15 to be covered.

16 MS. MARCUS: Thank you.

17 I'd like to at this point open the mics up for
18 questions from the audience, either about things that
19 we've just been talking about or things that we
20 mentioned earlier in the session, and for the next five
21 minutes we'll hear from people in the audience.

22 Anyone? We have a question over there.

23 UNIDENTIFIED SPEAKER: Based off of that example
24 that you just gave where you've got two business
25 entities serving up information, if there's parental

1 consent on the website with the operator, how is that ad
2 then covered by that parental consent, or are they now
3 not covered?

4 When a parent gives parental consent to a
5 website and collecting of PII and then you have got
6 another ad operator on the site, how is the parental
7 consent then given for that or how is that covered?

8 MS. CAMPBELL: Well, I think that's really the
9 topic of another panel, but I would say -- I mean, I
10 think it kind of goes to the adequacy of consent. I
11 mean, parents may be consenting for one thing and then
12 the information is being used for something entirely
13 different than what they thought they had consented for
14 their child to use. That would not be adequate consent.

15 MR. MORRIS: I would completely agree, I mean,
16 that any parental consent needs to provide full notice
17 and consent from the parent for any use and any, you
18 know, information. So, I mean, a website would need to
19 make clear, you know, your child will both be able to
20 play a game where he or she can tell their name to, you
21 know, to another game player and they will be served
22 targeted ads based on, you know, information collected.
23 And the parent needs to be able to understand both
24 elements and consent or not to both elements.

25 MR. WARNECKE: I'd like to address this

1 multiple-operator question in a slightly different
2 context, apart from the online advertising, and it's a
3 context that we generally seeing occurring quite
4 frequently in the game industry, and that is where you
5 have consent at the platform level that a parent gives
6 for certain communications to take place, and then a
7 couple of months later, the child acquires a game that
8 they play, and then the publisher's software comes up
9 and says, "Hey, we need parental consent for in-game
10 chat."

11 And this causes a big confusion with a parent
12 who doesn't understand, well, I previously gave consent
13 before, why am I being asked again for this same
14 consent? So, I think what would be very helpful in that
15 situation -- and I appreciate it's a little bit
16 different from the online advertising circumstance, but
17 it raises a similar issue -- is that if there was some
18 streamlined way where you could have one operator obtain
19 consent for multiple parties, subject, of course, to
20 appropriate disclosures and making sure that the parent
21 is fully informed. But if there was some flexibility to
22 do that, I think that would be very useful.

23 MR. MCINTYRE: I would add one last kind of
24 issue that is important, I think, for us to consider.
25 We talked a lot about, as we were talking about American

1 Idol and determining whether the user is a child, when
2 you're dealing with consent, I think it's also important
3 to make sure that you can consider whether the person
4 giving consent is, indeed, in fact, the parent or the
5 guardian.

6 I think there are a lot of instances that are
7 where the child is marking off on consent without ever
8 reading the consent notice, and I'm not sure how that's
9 resolved, but I think it's definitely an issue that
10 exists that who we think are the parents online may,
11 indeed, not be.

12 MS. ENGLE: Well, that's definitely a topic for
13 later in the day, an oldie but a goodie question for us.

14 MS. MARCUS: I think at this point we need to
15 wrap up. I thank all of our panelists and everyone in
16 the audience for being so interactive, and we hope that
17 this continues throughout the day.

18 (Applause.)

19 (Recess.)

20 MR. QUARESIMA: I'm Rick Quaresima. I'm an
21 Assistant Director in the Division of Advertising
22 Practices. With me as co-moderator is Mamie Kresses,
23 who, along with Phyllis Marcus, is the co-head of our
24 COPPA program.

25 The second panel today is going to talk about

1 discussing the legal and policy implications of COPPA's
2 inclusion of an actual knowledge to general audience
3 operators. So, I would first like to introduce our
4 panelists.

5 Starting down here on my far right, we have
6 Becky Burr, who is a partner with WilmerHale.

7 Next to Becky, we have Dr. Gwenn O'Keefe, M.D.,
8 and she is the CEO and editor-in-chief of Pediatrics
9 Now.

10 Then we have Phil Terzian, Senior Director of
11 Government Affairs of Activision Blizzard.

12 Coming down to the left of Mamie is Phyllis
13 Spaeth, Associate Director of the Children's Advertising
14 Review Unit, Council of Better Business Bureaus.

15 Then we have Guilherme Roschke, a graduate
16 fellow from the Institute for Public Representation,
17 Georgetown University Law Center.

18 And then Jeffrey Greenbaum, a partner at
19 Frankfurt Kurnit law firm.

20 And then Christine Jones, who's the General
21 Counsel of The Go Daddy Group.

22 So, right now, I think we are going to go down a
23 little bit deeper into the specific type of operator
24 covered by COPPA. We have talked about that COPPA
25 covered websites and online services, but there are two

1 different websites and online services that come within
2 that; those that are services that are directed to
3 children or operators that have actual knowledge that
4 they are collecting personal information from a child.
5 And this panel will deal with that actual knowledge
6 standard.

7 So, I'd like to open it by just sort of getting
8 back to the original purpose and the original passage of
9 COPPA and try to maybe get a little feel for how
10 Congress settled upon the actual knowledge standard for
11 general audience operators, as opposed to any other
12 standard.

13 So, I think I would like to begin a little bit
14 with Becky on that.

15 MS. BURR: Thanks.

16 We've been talking about gray areas, and I think
17 we all, sitting around the table in 1997 and 1998
18 talking about this, knew that there would be gray areas,
19 and specifically, that there were sites that would be
20 interesting to adults and interesting to children as
21 well. And the question is, you know, what are you going
22 to do with those sites?

23 The actual knowledge standard was adopted --
24 replaced the original draft language, which was
25 "knowingly," in Senator Bryan's original draft, the

1 language was "knowingly," and it was replaced with the
2 actual knowledge standard in committee, in the Senate
3 committee, as a result of the hearings. The two
4 standards are very different.

5 Legally, the knowingly standard will allow you
6 to consider information, inferences, inferences,
7 information that you should have known, whereas actual
8 knowledge is a direct and clear knowledge of a fact, as
9 distinguished from constructive knowledge.

10 So, it was a very deliberate move on the part of
11 Congress to distinguish the standard.

12 MR. QUARESIMA: Guilherme, do you have anything
13 that you would like to add to that?

14 MR. ROSCHKE: Yeah. I will just add that as
15 originally introduced, the bill only had a directed ad
16 section, was limited to that. Consumer groups then
17 proposed language to cover websites that know or should
18 reasonably know they are collecting information from
19 children. And then in the negotiations, the industry
20 retorted with, you know, the actual knowledge standard.
21 And so that's how we got to the actual knowledge.

22 MR. QUARESIMA: Okay. How has the requirement
23 of actual knowledge, as opposed to a constructive
24 knowledge, affected the development of various business
25 models? And I'd like to sort of make this a kind of

1 very broad-based question and get a lot of input from
2 the panelists.

3 I think I'll begin, perhaps, with Jeffrey, and
4 then we can, you know, sort of work our way through.

5 MR. GREENBAUM: You know, obviously, I think
6 there are certain times, you know, when advertisers,
7 marketers, they want uncertainty. They want
8 flexibility. They want the ability to look at all the
9 facts and circumstances. And there are other times when
10 you need certainty, that it's just virtually impossible
11 to build a business, to, you know, plan what you're
12 going to do without a level of certainty that you know
13 that you can comply with. And I think that the actual
14 knowledge standard does that.

15 The way that we've got a standard right now that
16 is very clear, advertisers or operators know what they
17 need to do. They know when they have actual knowledge,
18 and they know when they don't, and it has allowed
19 businesses to develop, and I think as the discussion
20 will show, that, you know, many of the websites
21 available today, if we had a broader standard, if we had
22 a "knew or should have known" standard or had some sort
23 of constructive knowledge standard, I think what we
24 would find is that it just really wouldn't be workable,
25 that regardless of whether you have some kind of age

1 screening or not, I mean, the whole notion of that, you
2 know, you're responsible for the content of everything
3 that's on your site, you know, and knowing what the
4 possible information that could be on there, is just
5 simply not workable and wouldn't work for the kinds of
6 websites that we have today.

7 MR. QUARESIMA: Anybody else?

8 Becky, do you want to --

9 MS. BURR: I just want to say that Congress made
10 a decision in passing Section 230 to ensure that
11 operators of websites would not necessarily be
12 responsible for everything that was on their site. That
13 was designed to promote innovation and uptake of
14 ecommerce, and the actual knowledge standard supports
15 that.

16 MS. JONES: And could I just say, as the evil
17 website operator on the panel, we're so glad they did?

18 MR. QUARESIMA: Why is that?

19 MS. JONES: Let me say at the outset, before I
20 got up here, I checked in with Foursquare, and I noticed
21 that at least four others in the room had done the same.
22 I sent out a geolocated tweet to tell people that I'm in
23 the room, and I also didn't mention the fact that I'm
24 over 13. So, we'll see if anybody has actual knowledge
25 when we leave here of what we're doing, information

1 we've collected, and whether or not there are children
2 in the room. That's just for you, Professor. We'll
3 sign you up with a Foursquare account before we leave, I
4 promise.

5 The reason we're happy about the fact that the
6 actual knowledge standard is actual knowledge and not
7 constructive knowledge, "knew or should have known," or
8 some lesser standard is because, let's face it,
9 businesses are in business to make money, and they want
10 to push the envelope.

11 Now, we're very careful at Go Daddy about what
12 information we collect and how we use it, but we have 41
13 million customers who maybe aren't quite so careful, and
14 we hear every time they do something wrong, and if there
15 weren't, as Becky pointed out, such a specific intent to
16 make the standard as high as it is, we would have a lot
17 more violations.

18 And so I say a little bit tongue in cheek that
19 businesses are happy about the standard, but really,
20 honestly, it has been a watermark, a benchmark, that
21 people can use to say either I knew or I didn't know and
22 don't ascribe knowledge to me if I didn't have the
23 actual knowledge. So, it's been something that people
24 have really backed up against to form business models to
25 make more money.

1 MR. TERZIAN: I'd like to, you know, reiterate
2 the certainty aspect and how the predictability of that
3 is very helpful for site operators. I mean, the actual
4 knowledge standard does provide the certainty. It
5 allows you, you know, at a point in time, such as when
6 the user is registered, to make a quick, easy decision
7 as to whether or not that person is under 13 or not.

8 A "should know" standard, more murky or
9 uncertain, would have to be -- you know, it would be
10 hard to follow. I think there would be, you know, a
11 huge amount of businesses that would have to then adhere
12 to that.

13 MR. QUARESIMA: Gwenn, do you have any thoughts
14 on that?

15 DR. O'KEEFFE: You know, I think when you look
16 at actual knowledge in children, it's a sticky point,
17 because they're -- it's a strict definition right now of
18 actual knowledge, but we know children are on these
19 sites. So, I'm very uncomfortable with using just
20 actual knowledge from a -- and we will get to this more
21 in a little bit, but, you know, I think that, you know,
22 when you look at the Go Daddy and the -- you know, the
23 Foursquare, the Foursquare example that you just gave,
24 I'm not comfortable, you know, because I think it's --
25 when you look at businesses and what they have to do,

1 it's, I think, incompatible with what you have to do to
2 keep children safe online and protect their privacy.

3 MR. QUARESIMA: Phyllis, let me turn this over
4 to you for a minute, and I think in some ways, I hear a
5 lot about certainty, but I'm not hearing a lot of
6 specifics about how some of the business models actually
7 have developed and what is the specific business model.
8 So, I would like to kind of talk about that. So, maybe
9 even in relation to figuring out what some of the models
10 were beforehand that you saw at CARU versus ones we know
11 of now.

12 MS. SPAETH: By the way, I'm not wearing my
13 bullet-proof vest, and I feel like, except for Gwenn,
14 I'm not in the real majority here. So, let me just
15 start by saying that I'm from the Children's Advertising
16 Review Unit, which is the self-regulatory arm of the
17 children's advertising industry, and I think we were
18 even a little ahead of the game when it came to online
19 media, because back in 1996, before I was even born,
20 CARU came up with self-regulatory guidelines on
21 interactive electronic media, which at the time had the
22 intent of covering websites directly, you know, intended
23 for children or targeted at children.

24 I came to CARU in 2000, and it was very clear,
25 even at the beginning, that there were lots of websites

1 that children were going to be going to, and I'm not
2 talking necessarily about general audience websites.
3 I'm talking about websites that were made for teens.
4 And what was interesting is even before then, there were
5 websites that had within their names "preteen chat,"
6 "kids this," "preteen that," so, like, somebody knew
7 somewhere that they were having children below the age
8 of 13 there.

9 And somewhere I believe in 2001, we changed our
10 guidelines to come up with what we call our "reasonable
11 expectation" standard, and what this says is our
12 guidelines cover websites that are directed to children
13 under 13 and those where there's a reasonable
14 expectation that a significant number of children will
15 be visiting. And in using this, we've decided that if
16 there is a site that has "teens" in its name -- or let
17 me step back a second.

18 What I think any child psychologist or parent
19 can tell you is that children model up. Every
20 10-year-old, especially girls, wants to be able to do
21 what the 15-year-old girls are doing, and if there is a
22 rock star, you know, any kind of pop icon that
23 15-year-olds are interested in, mark my words,
24 8-year-olds are, also.

25 So, we decided we can't just let all these teen

1 websites you know, out there and, you know, just doing
2 this little "don't ask, don't tell" thing, so that
3 everybody is free and clear. So, instead, with the
4 "reasonable expectation" standard, we were able to look
5 at sites and say, "Okay, what do you have to do now?"

6 If there is a reasonable expectation, it's not
7 that hard. Just do one neutral age screening so that
8 you ask people that want to register for their age in a
9 way that doesn't tip them off as to what age they should
10 be, so that you can ask for a date of birth, you can
11 have a drop-down menu from which you can pick a month,
12 date, and year of birth, but you can't say right next to
13 it, "You have to be 13 or over to register."

14 Neither can you then, when a child says that
15 they are 10 years old, can you have a screen that comes
16 up that says, "Oops, you're too young, go back and
17 reregister," or just, "Oops, you're too young," and the
18 kid just presses the back button, and there she is. She
19 changes her age, and she's in. So, the third part of
20 this is that you have to have some kind of a tracking
21 mechanism to stop a child from going back and changing
22 their age.

23 MR. QUARESIMA: Jeff, you had something?

24 MR. GREENBAUM: Yeah, a couple things. First, I
25 don't think you need to worry, Phyllis. I don't think

1 you need a bullet-proof vest. It doesn't matter where
2 you sit. I think that people are concerned about
3 children and are concerned about protecting children,
4 but it's about choices, and everything we do is about
5 choices. I think of my son in the playground and
6 deciding which thing is he allowed to go on. You know,
7 do I let him go on the small slide or the big slide?
8 Can he climb up the ladder by himself or not? We are
9 constantly making choices, and some of them are
10 difficult to make, and these are just more difficult to
11 make.

12 But I think that, you know, the reasonable
13 expectation that you're talking about is an interesting
14 one. I just don't think it relates to the actual
15 knowledge standard. I think it relates to the
16 "directed-to-children" standard, and I think that it may
17 be that in today's environment, we have to look at what
18 does it mean to be a site directed to children, and that
19 is something that may require some further exploration,
20 because it may be that "directed to children" meant
21 something very different.

22 And certainly in other contexts, you think
23 about, you know, when we've had concerns about a child
24 audience, there's a big difference between "directed to
25 children" and the percentage of the audience that is

1 children, and it's one of those difficult issues that
2 we've struggled with in other contexts. But I think
3 that it may be that, you know, it's not about actual
4 knowledge, because I think actual knowledge at least
5 gives someone an ability to plan their conduct.

6 I think that, on the other hand, if you relook
7 at perhaps "directed to children," you could make
8 decisions about the size of the audience, things like
9 that, things that, you know, give operators a certainty,
10 you know, certainty in the way that they proceed.

11 You know, finally, on the neutral age screening
12 thing, I think that you can't ignore, one, the cost
13 associated with that. I mean, it does require operators
14 to do additional things that have a cost, but also, that
15 doesn't change anything. Whether you are directed to a
16 general interest website -- whether you're directed to a
17 general interest audience and you don't age-screen or
18 whether you do neutral age-screen, you still have a
19 website where people are still, you know, giving you
20 information which still raises the same question. So, I
21 don't think that solves the problem when we're talking
22 about how do we address the actual knowledge issue.

23 MS. SPAETH: Well, hold on one second. There
24 are several things I have to answer there.

25 MR. QUARESIMA: Okay, quickly, because we need

1 to give other people an opportunity.

2 MS. SPAETH: Okay, I'll be very quick.

3 Okay, number one, I don't think we should get
4 into semantics here. I'm talking about the actualities
5 of the way we work, so that I don't care what you call
6 it, like which rubric it fits under. We do need to take
7 care of children.

8 And I also think we need to go back to the
9 purpose, as David Vladeck started off with. The purpose
10 of COPPA was twofold: One had to do with marketing to
11 children, gathering information from them. The second
12 part of it was a safety interest.

13 And I will tell that you when I first came to
14 CARU, most of the websites that we looked at -- I mean,
15 not only am I a Luddite, but I am really old-fashioned,
16 and I couldn't believe the sex that was going on in chat
17 rooms. So, all I'm saying is, there's a real interest.
18 You know, we're looking here to protect children.

19 And that's it. Everybody else go on.

20 MR. QUARESIMA: Okay.

21 MS. BURR: So, I think all of us want to protect
22 children, although I have to say that the congressional
23 purpose of COPPA was to prevent the use of manipulative
24 ads and unfair and deceptive practices. It wasn't a
25 child safety law.

1 But having said that, my problem with the -- why
2 I think the actual knowledge standard is useful is
3 because I think verifiable parental consent is too
4 expensive to get, not putting up the age screen, that's
5 pretty easy. I don't think it costs that much to put up
6 the age screen, but what it does is it teaches kids to
7 lie. So, you don't change the number of kids who are on
8 the site. It's still a lot of kids under 13. They're
9 there, and they've lied to get there. And that's the
10 message we're sending, which I think is not a healthy
11 message.

12 MR. QUARESIMA: Let me just sort of follow up,
13 but if that's the message, do you have any proposal
14 to -- I mean, would a different standard at all solve --
15 try to address that problem?

16 MS. BURR: Well, I think that there are very
17 good reasons to think about different levels of parental
18 consent, maybe turning to a notice provision only if a
19 website is engaging in, you know, activities within a
20 certain parameter, so that there's a safe harbor not for
21 compliance with COPPA, but there's a safe harbor that
22 gets you out of the verifiable parental consent and
23 sends you into a no-penalty notification provision,
24 something like that.

25 I think those are the changes that would make

1 the most difference, that would encourage children to be
2 honest and encourage communication between parents and
3 children through notice, as opposed to not being able to
4 get on the site at that moment when the kid wants to.

5 MS. KRESSES: And I would go back to Jeff, who
6 had said earlier that a broader standard would not be
7 workable for all sorts of websites today, and I think
8 that it's just too easy to say, and so we need to look
9 at how would it not be workable and how would you work
10 around it if a reasonable expectation or a more
11 constructive knowledge standard were dropped on you from
12 the sky?

13 MR. GREENBAUM: Well, you know, again, I think
14 that there's -- I still think, you know, we're talking
15 about two different things. I think that the notion of,
16 you know, what an online service website or online
17 service directed to children, I think, you know, the FTC
18 could develop guidance that says, "What does it mean to
19 be directed to children?"

20 You know, it's one thing to have a site that is
21 obviously directed to kids, you know, the Dora website,
22 whatever it is. You know that that's directed to kids.
23 You know little kids are going on. You know, I think
24 you could also give guidance that says, you know, look
25 at your audience. Look at the number of kids that are

1 coming to your -- and look at the -- do demographic --
2 do research. If you have a concern that there is a
3 substantial number of kids, you know, that may be
4 something that you could explore, but at least it would
5 give -- you know, it would give you certainty.

6 The issue that -- and I think we're going to
7 talk about this in a little more, is, you know, what
8 we're talking about here is not children generally. I
9 mean, the actual knowledge standard is not about actual
10 knowledge that you are collecting information from
11 "children." It is actual knowledge that you are
12 collecting personal information from "a child."

13 And I think that we have to go back to the
14 statute here, and what the statute is is either a
15 website that is directed to a child audience generally,
16 and I think we can explore that and develop that in a
17 way that perhaps is productive, but I think that in
18 terms of collecting personal information from "a child,"
19 it's temporal. It's about at a moment in time, you're
20 collecting personal information from a specific child.

21 And so that is a very, very high standard to
22 reach, to meet, and I think that it would be an
23 extremely difficult one to say that at any moment that a
24 child is entering into information on your website, you
25 have this obligation to, you know, have 11,000 people

1 standing by and reviewing the website and making sure
2 every key stroke goes in, and the minute the word "I'm
3 10" goes in, you go, "Got to delete that," because, you
4 know, you now have actual knowledge that you're
5 collecting information from a child.

6 So, obviously, you know, we have to be more --
7 we have to be rational. We have to say, "Well, look, we
8 know kids are going to lie. We realize we have set up a
9 system that leads kids to lie, and we know that there's
10 a tremendous amount of Web content." You look at the
11 amount of content that is posted every day on any major
12 social networking site, and you realize it's just simply
13 not possible to go and screen that or monitor that in
14 any kind of a productive way.

15 And I think the other problem -- and I think we
16 can talk more about this, too -- is you don't want to
17 create reverse incentives either. I mean, you do want
18 website operators to have the ability to engage in
19 conduct which helps protect the safety of people online,
20 that tries to protect the privacy of people online, and
21 to do that, you have to enable them to go and look at
22 things that they believe would be helpful.

23 But the minute that you start to go down that
24 road, you start to get into the question of, well, you
25 know, you were looking -- you started to look at that

1 site. You have that person there. You could have done
2 this, this and this. You should have known that those
3 kids were -- that there were kids there, if you had
4 looked a little bit deeper, looked deeper into the
5 comments. You start to get yourself into a murky world
6 which I think would be extremely unworkable.

7 MR. QUARESIMA: Actually, you had noticed
8 something that I -- you talked about something I did
9 want to explore, and that was the idea that operators of
10 websites directed to children and those that have actual
11 knowledge, that is, collecting personal information from
12 a child, and I did want to explore that and give some of
13 the other panelists an opportunity to speak on that.

14 Guilherme, did you have any thoughts on that?

15 MR. ROSCHKE: Well, I think that the --

16 MR. QUARESIMA: Would you agree with Jeff's
17 characterization on that?

18 MR. ROSCHKE: Not exactly. I think it would be
19 kind of wrong and it would protect children less to read
20 too much meaning into this. You know, let's take the
21 example of, like, behavioral targeting, where you're not
22 targeting -- you're probabilistically targeting
23 children. You know, I think that that would fit
24 probably under the directed-at-children standard, but
25 then there's a certain point, which depending on how

1 your behavioral targeting analytics are done, where you
2 know that pretty much all of these are children, and at
3 a certain point where we can talk about you having
4 actual knowledge that you're collecting information from
5 a child.

6 MR. QUARESIMA: Gwenn, did you have anything to
7 add?

8 DR. O'KEEFFE: Yeah. I think -- well, there's a
9 lot of ways of looking at this. The first is, you know,
10 getting back to something Jeff said, we cannot, on any
11 level, be okay with a system that encourages children to
12 lie, and I think that, you know, from a developmental
13 point of view, to have a system that tells kids you can
14 lie about your age, we are teaching kids the wrong
15 lesson and putting them in just so many precarious
16 situations for their health, their well-being, their
17 safety, and their development. I mean, we're not even
18 talking about privacy yet. We are just putting them in
19 arm's length of danger.

20 Now, from a privacy point of view, we're putting
21 them at risk there, too. So, we are just teaching them,
22 "Hey, guys, go ahead and lie. We're cool with that."
23 We can't be cool with that. We can't be cool with that
24 as educators, we can't be cool with that as
25 professionals, we can't be cool with that as parents,

1 and we can't tell parents to be cool with that.

2 So, if we are going to have some good come out
3 of today, we have to look at the statute and what we're
4 here to do on this panel and recognize that actual
5 knowledge doesn't work.

6 Now, constructive knowledge, that does work,
7 because we know that if a child posts information about
8 their life, that implies that they're 10, a website can
9 do something about that. Posting works. Posting
10 behavior works. Websites use behavioral targeting all
11 the time to do ads, to do all sorts of information
12 collecting. We know about a child and we can target who
13 they are by what they post about every single day. If
14 we change what type of knowledge we use to capture a
15 child, we can better serve their needs. Actual
16 knowledge isn't it.

17 MR. QUARESIMA: I'd like to go to the audience
18 now, if anybody has -- does anybody have a question in
19 the audience?

20 MS. LEVIN: Good morning. My name is Toby
21 Levin. I'm recently retired from federal service. I
22 was at the Federal Trade Commission when the agency was
23 working on legislation and the regulation and was the
24 first COPPA program manager.

25 So, if I can just bring a little historical

1 perspective on this and recognize that I think the FTC
2 staff did an amazing job in 1999 of coming up with a
3 regulation that works incredibly well, but recognizing
4 that it does create some compliance challenges and
5 obviously some challenges for industry as well.

6 I'd like to think of when we dealt with the
7 actual knowledge, we were not strictly identifying the
8 age registration as the only way to determine actual
9 knowledge. We were dealing with what was a common
10 practice at the time. We know that even for
11 nonchildren, date of birth is greatly desired by
12 websites. They want to know their audience very
13 specifically. So, they weren't doing age registration
14 just for COPPA. They were doing age registration
15 because it was valuable information.

16 So, the agency piggy-backed on what was a
17 convention at the time and then tried to use that in a
18 way to at least get kids to input ages and prevent them
19 from going back and changing them by requiring, as
20 Phyllis noted, that there be a mechanism in place to
21 prevent them from going back and changing their date of
22 birth.

23 But the rule itself doesn't limit actual
24 knowledge to age registration. It specifically gave
25 some other illustrations, some examples. It talked

1 about information that comes from a concerned parent,
2 asking age-identifying questions, and we were just
3 recollecting examples of what we were aware of then. I
4 think since then, there are probably a lot of other
5 means by which actual knowledge can be determined.

6 We did note in the preamble the fact that
7 experiential evidence, actually data regarding -- you
8 know, empirical evidence regarding who, you know, who is
9 going to websites would be useful in identifying
10 websites directed to children, but I think if you look
11 at ads on a spectrum of where you have websites directed
12 to children all the way to actual knowledge, that
13 somewhere in between -- and maybe it's addressed by the
14 concept of constructive knowledge -- there's indicia
15 that children are going to -- and younger children --
16 are going to some of these websites.

17 MR. QUARESIMA: Let me -- actually, I can take
18 the opportunity, because I was going to go there anyway,
19 to sort of throw open to our panelists, I mean, what are
20 some of those other ways, you know, currently in the
21 online environment that a business might actually --
22 that might acquire this actual knowledge?

23 And I think we can start with our business
24 representatives. Christine, let me start with you on
25 that.

1 MS. JONES: There are many, and one of the
2 things that we see a lot coming from customers whose
3 websites we host is complaints where mom calls and says,
4 "Daughter just was served up an advertisement for a
5 company that makes products for children, and why are
6 you serving my daughter with an ad that targets kids?"
7 So, we know somehow that ad network has knowledge that
8 probably the person looking at the screen at that
9 particular time is a kid.

10 So, this gets back to kind of what Gwenn was
11 saying. They're getting the information somehow, right?
12 They're looking at where the kid came from. So, did
13 they come from a child's website or a website designed
14 to solicit children? Did they have a web-browsing
15 history that they're collecting in their vast array of
16 data that goes into their algorithm to determine what ad
17 to pop up? Did they buy information from a website that
18 said specifically this person at this IP address is this
19 age?

20 There are a multitude of ways, and we see all of
21 them every day, because believe me, when you pick up the
22 phone 24 hours a day and the operators of websites that
23 you host don't, you get the phone calls. You get the
24 people saying, "Hey, Go Daddy, what's going on and why
25 are you targeting my kid?" And we say, "Well, actually,

1 sir, I'm sorry, I'm not targeting your kid, but let me
2 go talk to my customer who is."

3 So, there are a multitude of ways that people do
4 it. It's very clever. I'm not going to stand up here
5 and say I patently agree with Gwenn, that actual
6 knowledge is the wrong standard, but it's fascinating to
7 hear from you, from your perspective, because it's
8 completely different than ours. We're much more
9 responsive to the complaints, whereas you're sort of
10 suggesting a solution maybe that's different. So, I'd
11 love to hear more about what you think the standard
12 should be.

13 MR. QUARESIMA: Phil?

14 MR. TERZIAN: I just want to finish up on the
15 question real quick. I mean, it was just brought up,
16 you know, one excellent example is the one that the FTC
17 provided, which is if parents, a concerned parent, such
18 as myself as a parent, if I were to call and say that
19 "Hey, there's an issue," the companies have to then have
20 the knowledge. You know, we, of course, would have a
21 mechanic in place for parents to do that, as would I
22 assume most websites out there. So, that would be one
23 great example of where someone might have actual
24 knowledge.

25 MR. GREENBAUM: Also, just to finish up on the

1 point, I mean, I think the actual knowledge standard is
2 working in the sense that it has led to companies
3 complying with the Children's Online Privacy Protection
4 Act, and to the extent that operators obtain actual
5 knowledge, they're addressing it.

6 Now, I think that we may wish that Congress made
7 a different choice, and I think that that's something
8 that we could look at, but I think that, you know, in
9 terms of does the standard itself work and is it
10 workable, I think it is.

11 I think there's another thing that is important
12 to remember here, is there's no magic to age 13. I
13 mean, there's nothing that happens -- you know, there's
14 nothing that happens, unless you're having a Bar or Bat
15 Mitzvah, when you turn 13 that suddenly turns you into a
16 man or woman.

17 So, there is a spectrum, and we have picked a
18 moment in time that allows us to try to sort of gauge
19 where the behavior is, but I think that where you would
20 probably look, if you did the research, is that, you
21 know, kids that are really young on the spectrum are not
22 lying and are not getting their personal information
23 online, and as you get older, as you're more ready to be
24 able to deal with all of the things that the Internet
25 has to offer, you get better able to deal with it.

1 And I think that that's certainly an area where
2 we could do research on, but I also think that we have
3 to realize that there is no standard, there is no age
4 that is going to, you know, create a situation where no
5 kid can, you know, disclose personal information.

6 MR. QUARESIMA: Okay. I'll let you -- Gwen,
7 and then I know we had another question in the audience.

8 DR. O'KEEFFE: Just a quick comment about age.
9 If you actually look at kids and their online behavior,
10 the younger kids just do not developmentally handle
11 online issues well, and it's not a matter of lying.
12 They don't have the developmental skills. So, they will
13 go online and get into a boatload of trouble because
14 they don't understand the wording, they don't understand
15 how to negotiate, they don't understand how to interact
16 properly. Teen-agers, in fact, you could argue 13 is
17 too young. So, we could have an entire panel about
18 that.

19 MS. AFTAB: Hi. My name is Parry Aftab, and I
20 was there in the days when Toby and Kathryn were. They
21 actually had done research on the ability of kids at
22 various ages to understand things, and that's where the
23 13-year-old age came from. They said that 13 was the
24 magic age, that kids understood it.

25 My real concern, though, is with the CDA and how

1 it's going to interact with this actual knowledge. If
2 we go into constructive knowledge, are we now going to
3 say that the websites and service providers that are
4 exempt from what their users are doing on their site and
5 don't have to monitor are now going to be required to
6 monitor because it's a general audience site that's
7 really popular with kids at the time?

8 And I think we have to be very cautious. I
9 mean, I run Wired Safety. I'm the one who's out there
10 trying to protect kids, but we have to be very careful
11 when we look at actual knowledge. If we move it to
12 constructive -- Gwenn, you know I love you -- if you
13 move it to constructive, what are you moving it to? So,
14 that means everyone now is going to have to monitor it.

15 The last issue is, kids lie. We know they lie
16 about their age. More importantly, they lie about the
17 age of their friends. So, if somebody is on Facebook,
18 legitimately 14 years old, and they don't like somebody
19 else in their class, they will report them as underage.
20 They will pretend to be their parents. They will do all
21 kinds of things to get somebody else out.

22 It's a form of cyberbullying, cyberbullying by
23 proxy. So, when we look at this, when you look at
24 actual knowledge and who's telling you what, we need to
25 realize that kids lie on both sides. "I'm 97. And oh,

1 by the way, my friend is 12."

2 MS. KRESSES: Okay.

3 MS. BURR: I just want to not leave this issue
4 of advertising targeted to children untouched, because I
5 would say that if you are a website and you are
6 promoting your website as, you know, a demographics of
7 8- to 10-year-olds or 8- to 12-year-olds, that is
8 something that would certainly be part of the
9 consideration for directed to children from my
10 perspective. So, I don't think that we have to move
11 into this constructive versus actual knowledge world
12 because of behavioral targeting.

13 MS. KRESSES: And the Rule itself, the Statement
14 of Basis and Purpose does discuss that that is one
15 factor that we can look to, is both demographic
16 information and, you know, what advertising is doing,
17 but I think the question gets a lot harder when we're
18 talking about ads targeted to particular people, as
19 opposed to ads just sitting on the website.

20 Does anybody have any further thoughts on that
21 question of how we use that indicia? Okay.

22 MS. BURR: Well, I mean, if there's an ad
23 targeted to a specific person at age 9, I mean, I think
24 we have to at least think about whether in that case
25 we're talking about, you know, targeting a child.

1 MS. KRESSES: And then, Kathryn, go ahead.

2 MS. MONTGOMERY: Yeah. I'm glad that we brought
3 up -- first of all, I want to thank Toby for reminding
4 us of the ways in which we all dealt with this difficult
5 question. I mean, I had said to Angela when the panel
6 started, "Oh, I hate this, because it's complicated."
7 It was complicated then, it's complicated now, and no
8 solution is perfect. But I appreciate Toby reminding us
9 that there were a number of different indicators that we
10 included in the definition.

11 The market, as everybody knows, has changed
12 tremendously, and I think it would be a mistake if the
13 Commission did not closely look at behavioral targeting
14 and profiling and analytics and that those kinds of data
15 collection practices, that are state of the art now in
16 the digital marketplace, as a source of information for
17 clarifying how this part of the rule works. Again, it
18 could be, you know, controversial and a knotty question
19 to address, but I think it's important.

20 The other thing that I would like to respond to
21 is what Phyllis was discussing, because I do think that
22 teen websites are a particular category that we may want
23 to look at more closely. It is true that kids watch up,
24 they want to go on the sites for teens, and developing
25 some more effective mechanisms that are industrywide

1 would be a really good idea.

2 And then finally, I hope somebody will talk a
3 little bit more about social networks, because there's a
4 lot of knowledge that goes on there about -- there's a
5 lot of data money that goes on there as well, and they
6 shouldn't be overlooked.

7 MS. KRESSES: Okay. And in that vein of teen
8 marketing, of teen websites, Guilherme, do you think
9 that there is leeway within the actual knowledge
10 standard itself to deal with sites that target kind of
11 above and below that line?

12 MR. ROSCHKE: Well, I think that when you're
13 looking for -- you know, actual knowledge is a factual
14 determination, and one of the facts that would weigh
15 into that fact is that your website is attractive to
16 children, and so that would be part of the information
17 that you have when you're coming up with the knowledge
18 of the age of somebody on your website.

19 You know, other information would be things
20 like, for example, if somebody's visiting your website
21 with a kid-oriented browser, you know, that is
22 information that's available to you that you can use to
23 determine their age as well, and it could be part of
24 your actual knowledge determination.

25 MR. QUARESIMA: I'm sorry. Phyllis, you had

1 something?

2 MS. SPAETH: Yeah. I'm sorry, I don't want to
3 just toot CARU's horn, but I will say that since we
4 started looking at websites -- and I'm telling you, we
5 haven't really gone to adult-oriented websites, we've
6 done what I've said, which is look at teen-oriented
7 websites or things that we know that kids are interested
8 in.

9 We've done over 200 cases, and I would tell you
10 in the last year and a half, we have, I think, 25
11 reasonable knowledge cases, and everybody that we've
12 contacted, 95 percent or over, have agreed to make the
13 changes. And anybody can argue, yes, kids lie, and
14 that's a whole other thing that we have to deal with.
15 I'm the first one to say that, because I believe most
16 self-respecting 8-year-olds, you know, that want to get
17 on the Internet know to say they're 13.

18 But right now, we can only do what we can do,
19 and I do think that the reasonable expectation standard
20 works.

21 MR. QUARESIMA: You know, I think I want to
22 expand upon that. I wasn't going to go here quite yet,
23 but let's -- since we're here, and we've heard a lot
24 about the concern about -- that kids lie. So, if one of
25 the big concerns we're dealing with is kids lying, is

1 some sort of constructive knowledge standard actually
2 more protective of their privacy or less protective?

3 I mean, is it really in their interest to have
4 website operators going around trying to root out this
5 information? And, you know, I think I'd like to sort of
6 have a general discussion on that. Maybe we'll start
7 here with Phil and then have people pipe in.

8 MR. TERZIAN: So, just to reiterate, is it more
9 protective to have the site operators trying to weed out
10 potential children who might have said they are either
11 over the age of 12 or maybe they weren't screened at
12 all?

13 I would first say that I don't think it just
14 applies to children, because if you're trying to figure
15 out how old somebody is and you don't know how old they
16 really are, you're suddenly trying to figure out how old
17 everybody is, potentially, on your site. I mean, I'm
18 sure most of you have used Facebook and have seen
19 people's profile pictures some used when they were
20 younger, some use their kids, you know, I don't know how
21 you deal with something like that.

22 I think it's a burden you might not want to put
23 on the site operators, but it might also, I would say,
24 reduce your expectations of privacy as a user knowing
25 that every site operator out there is trying to figure

1 out who you are.

2 MR. GREENBAUM: Well, I think also we have to --
3 you know, obviously raise this raises significant
4 constitutional issues as well. I mean, you know, people
5 do -- you know, adults, teen-agers, you know, they do
6 have the right or there is certainly many socially
7 beneficial reasons why people would go online
8 anonymously and look for certain kinds of information or
9 do certain kinds of thing online.

10 And I think we have to be sensitive to the
11 notion that, you know, operating in a digital world,
12 operating in virtual words, this is part of what it
13 means to grow up today, and we have to figure out ways
14 that are going to allow kids to do that and allow kids
15 to practice for some of that, you know, building certain
16 types of relationships online as well. And those are
17 important things that could be lost if we took a
18 standard that was overprotective.

19 Of course, the standard is not constructive
20 knowledge, it's actual knowledge, and so it would
21 require, I think -- you know, I don't think that that's
22 something that can happen at the Commission, you know, I
23 think --

24 MR. QUARESIMA: I think that's right, yeah.

25 MR. GREENBAUM: -- but I do think -- I still get

1 back to I think that we keep getting the two issues a
2 little bit intertwined, and I think that they are very,
3 very different. I think actual knowledge is specific.
4 I think that directed to children as a website -- I
5 mean, I think that what -- you know, Phil's point, which
6 is I think a very nice one, is that when you look at
7 directed to children in a rational way, you know, it may
8 just not mean -- it may mean many more things than some
9 people have understood it to mean.

10 And I think that CARU's very important work in
11 looking at teen-directed sites that are also very
12 attractive to young kids doesn't require any, you know,
13 rejiggering of the statute here or rejiggering of the
14 rule. It simply means for us to rethink or think a
15 little bit more deeply about what does it mean to be a
16 website directed to children without having to work with
17 the actual knowledge standard.

18 MR. QUARESIMA: Gwenn?

19 DR. O'KEEFFE: Well, you know, it may be that
20 instead of going -- you know, "constructive knowledge"
21 may not be the right phrase. It may be that we actually
22 have actual knowledge about kids by the way they post.
23 We just may need a better reporting system, because I do
24 agree with Parry that kids lie all the time, but younger
25 kids typically don't lie about things that they love to

1 tell stories about.

2 So, if a kid is really excited about a fifth
3 grade field trip and they're sharing that wall to wall,
4 they're going to be factual about that, and if somebody
5 wants to report that, they may need a way to do that,
6 and then we could argue maybe that that is actual
7 knowledge. And right now, that can't be used.

8 So, maybe we just need to be more realistic
9 about today's sites and what sites kids are on and how
10 they're using information about themselves and what
11 information can be used for people to report, "Hey, I
12 know this kid is on that site." And we haven't even
13 gotten into the reporting of who was on these sites.
14 That's a whole different issue that we should probably
15 address, too.

16 But kids do often give away who they are. You
17 know, sometimes they fudge, and sometimes they, you
18 know, love to tell big whoppers, but, you know, a kid
19 will often, you know, give enough clues of who they are,
20 because that's who they tend to be. They tend to wear
21 their hearts on their sleeves that way when they're
22 talking to each other and they're really getting into,
23 you know, a nice little trail of -- a nice little peer
24 group, especially the younger kids, because the younger
25 kids stick together on Facebook and the social

1 networking sites.

2 MS. BURR: It's not a requirement that if
3 somebody reports it, why couldn't you use that
4 information?

5 MS. KRESSES: That is in the statement of basis
6 and purpose, that that is one method, and certainly it's
7 there, but I guess that leads to, you know, a sort of
8 finite question of what sense do any of the panelists
9 have of how easy it is for parents to report children
10 being on a site where they don't want them to be and how
11 responsive are the online services?

12 DR. O'KEEFFE: Well, it's easy to find the link
13 to report. I went on yesterday to both MySpace and
14 Facebook. MySpace's reporting links are right there on
15 the site. Facebook, you have to go to the help center
16 and then dig a little bit, it's a little harder, but if
17 you find the link, up comes a nice little form you can
18 fill out and there it is.

19 But I hear consistently from parents that
20 getting -- and actually, MySpace actually will take
21 you -- walk you right through, how do I delete my kid's
22 profile? Facebook, though, basically says if you want
23 to delete your kid's profile, talk to your kid, and then
24 if you need to reach a live person, parents will tell
25 you it's impossible, you know, and that's the issue,

1 that if you want to get response back, you can't find a
2 person. There's no 800 number, in other words.

3 MS. KRESSES: And, Phyllis, from your
4 perspective, going beyond Facebook and MySpace, do you
5 have any sense of how difficult or easy it is for
6 parents?

7 MS. SPAETH: Absolutely not. Nobody has ever
8 complained to us about that, and I think that's very
9 interesting.

10 MR. QUARESIMA: Christine, I think you had
11 something you wanted to add?

12 MS. JONES: Well, this is where the people who
13 answer their phone 24 hours a day come in, because it is
14 absolutely impossible to get a live body at Facebook.
15 It just is. You just cannot get a person on the phone,
16 which is why, when you answer your phone 24/7, you end
17 up with all the lunatics calling you making complaints.
18 No offense, parents.

19 But I don't think -- we cannot lose sight of
20 your really, really, really good point on the CDA,
21 because if you start ascribing that responsibility to me
22 just because I pick up the phone -- and it's all
23 user-generated content. I didn't put that content out
24 there, folks. Some 8-year-old did, and, parent, why
25 don't you go figure out what your 8-year-old is doing?

1 I'm sorry to be so blunt about it, but come on.
2 We know kids lie, we know they're under 13, and we know
3 you're -- they're giving the website actual knowledge.
4 So, why don't you figure out what your kid is doing
5 online instead of calling me and telling me it's my
6 fault.

7 I'm sorry, I didn't mean to get all emotional,
8 but wow.

9 MR. QUARESIMA: Interesting point, but I -- you
10 know, here's a question.

11 MS. JONES: And she brought up the CDA, so it's
12 her fault.

13 MR. QUARESIMA: But it raises an interesting
14 point. In this online environment where you have tens
15 of millions of users of a service, all right, you know,
16 and somebody has reported in some way, all right, a
17 parent, that my child, all right, has put this
18 information out there, all right, and does that trigger
19 actual knowledge on the part of somebody who is
20 collecting the information? In this case, collecting
21 can also mean providing a forum for disclosure.

22 So, I think, Jeffrey, you had some points.

23 MR. GREENBAUM: Well, I think there are also
24 important lessons to be learned from the DMCA as well,
25 and, you know, I think the DMCA was enacted right around

1 the same time as COPPA, and the DMCA made very, very
2 different choices. I mean, the DMCA has both an actual
3 knowledge standard as well as essentially a constructive
4 knowledge standard. The constructive knowledge standard
5 of the DMCA doesn't really work, doesn't really provide
6 any useful guidance. It's a very, very difficult thing
7 to apply, and I think that, you know, I think the lesson
8 of that is in the context of this very, very big online
9 world, you know, the constructive knowledge standard
10 doesn't or the red flag standard doesn't really work.

11 On the other hand, the actual knowledge
12 standard, combined with a procedure that enables someone
13 to send a take-down notice, enables someone to contact a
14 website and say, "There is infringing content online,
15 and it's mine and you should take it down." It's
16 something that operators have been able to implement.

17 Look, it's not without its challenges, it's not
18 without its gray areas, it's not without its
19 difficulties. I mean, when you're talking about a very,
20 very big website, a very, very big social network that
21 has huge amounts of content, there's enormous costs
22 associated with it, but it is a way that we have been
23 able to make a certain choice, that's been able to
24 address an issue in a certain way, and I think that
25 there is no reason that -- there is no reason to believe

1 that, you know, websites couldn't do something similar
2 in a privacy setting where they were given -- where
3 there was certainty and there was a procedure in place
4 that both allows the internet to continue to develop and
5 allows these sites to continue to develop, but gives
6 parents the ability to get information and to make
7 certain choices for their kids.

8 MS. JONES: Could I touch on that real briefly?

9 MR. QUARESIMA: Okay, okay, quickly.

10 MS. JONES: Just quickly. About ten years ago,
11 we wrote -- I/we wrote a mirror policy for trademark
12 infringement exactly mirroring the DMCA. Today I look
13 at other people's websites, I see it everywhere. It
14 works really well. So, I think Jeff's point is great.
15 Let's all go write a similar thing for parents to make a
16 report, we will go take them down like the DMCA, but
17 we've gotta have a hook, right? I have to have
18 something that makes it illegal in order for me to do
19 that. So, let's do that. Totally outside of this
20 panel, but let's do that, too.

21 MR. QUARESIMA: Well, it may not be outside of
22 this panel. I mean, in examining the statute, it might
23 require a statutory change. It also could be possible
24 to do that by the regulation, but let me turn to
25 Guilherme, because I think he had something to say.

1 MR. ROSCHKE: I think we should look back to --
2 you know, one of the goals here is to put parents in
3 charge and put parents in control, and so there's this
4 notice system, and we're all concerned about how can we
5 make the notice work better. But I think the FTC should
6 seek comments on the ways for parents to more easily
7 communicate this actual knowledge standard, the actual
8 knowledge that's required.

9 So, for example, you know, what if I could give
10 a device to my child and then program the device such
11 that the device would automatically communicate to an
12 operator of a website the actual knowledge that they
13 would need to comply with COPPA, and, you know, that my
14 child can lie, but then the operator can just trust the
15 signal from the device as opposed to, you know, whatever
16 my child lies about?

17 You know, I think there are pluses and minuses
18 here, and I'm not 100 percent behind it, but I think
19 taking comment on this would be really instructive about
20 a way to put parents in charge.

21 MS. KRESSES: That's a good idea for a panel
22 forward when we talk about parental consent as well, so
23 if we don't get to that sort of point, somebody remind
24 me.

25 MR. QUARESIMA: Becky, you had a point, too.

1 MS. BURR: I just wanted to remind people about
2 Parry's point about, you know, being put on notice does
3 not necessarily mean that you actually have a child. I
4 am sure it's true that there are friends who are
5 reporting each other in that case.

6 I think, though, as I -- in thinking about this,
7 if a site says, "Here's a place to report an underage
8 person," then under the FTC Act, forget the COPPA, they
9 have -- they're making a representation that they are
10 going to investigate that and make a determination about
11 whether they have actual knowledge on that basis.

12 I don't think you could assume that just having
13 a report provides actual knowledge, and I don't want to
14 lose sight of the CDA point, but where a site says,
15 "This is how you report and we will take action," I
16 don't think you need to change the law to take care of
17 that problem.

18 MS. KRESSES: That seems like a good opportunity
19 to ask the audience if you have -- if anybody would like
20 to make a comment on these points being raised.

21 MR. NICHOLSON: John Nicholson. I'm with
22 Pillsbury -- the law firm, not the dough boy.

23 And we're going to cover this later on today,
24 but my real concern about the knowledge standard comes
25 through the definition of what is personal information

1 and the way that we're moving to aggregations of
2 individually nonidentifiable pieces of information
3 creating a statistically significant profile that
4 individually identifies a person.

5 And if you move from actual knowledge to
6 constructive knowledge and you have all those individual
7 pieces of information and some researcher does an
8 analysis that says, "Oh, well, if you have hair color
9 and car and family income and these individual pieces,
10 you can actually individually identify this person, you
11 can pick them out in their zip code, and you can do --
12 create a zip-plus-four and you know exactly who it is."

13 And then, when you get to that, does that
14 suddenly become constructive knowledge? And if you've
15 collected all of those things, do you have to then go
16 back and say, "Oh, well, gee, we collect all that
17 information. Somebody's just proven that identifies
18 people. Do I have to go back and look at all my
19 information to figure out whether or not I've got any
20 under 13s?"

21 MR. QUARESIMA: Okay, I think I do want -- we
22 are going to actually address something like that very
23 soon.

24 Yeah.

25 MS. TAYLOE: Hi. My big issue is that we all

1 know that kids have gmail accounts, AIM accounts,
2 Facebook accounts, MySpace accounts. I mean, we
3 could -- you know, I'm just topping those off because we
4 all recognize the names. And so when is industry going
5 to get out of the way and actually let kids tell the
6 truth? Because industry is the one who's forcing kids
7 to lie, because if kids could tell the truth, I have to
8 believe some percentage of 11- and 12-year-olds would
9 not lie, would engage the parent, and would ask for
10 consent, and maybe we'd start getting out of the "there
11 is no methods for consent," because there would be a
12 reason to process consent.

13 MS. KRESSES: So, are you saying, Denise, that
14 if companies offered more opportunities for consent, it
15 would lessen the amount of lying and that --

16 MS. TAYLOE: Yeah. I mean, to get an iTunes
17 account, you have to be 13. So, if you're an app
18 developer and you build a game, you rely on the fact
19 that, well, the only way you can access my game is with
20 the app that you had to be 13, so I don't have any
21 actual knowledge, you must be 13; or lots of companies
22 that I'm dealing with that have contests and they want
23 the kids to upload a YouTube video, and they are
24 directing the kid to go to their YouTube site and upload
25 their video, but they can't have a YouTube account or

1 gmail account to do so.

2 So, I know there are people who advocate kids
3 shouldn't be on social networks, but there are lots of
4 parents who want their kids to have a Facebook account
5 to talk to their cousin or talk to their father who's in
6 the military or whoever it might be, and the companies
7 themselves are making no attempt to actually allow a
8 child to tell the truth and then get parental consent
9 under some method that becomes reasonable and scalable.

10 MS. KRESSES: Becky, did you want to comment on
11 that?

12 MS. BURR: Yeah, that comes back to my point
13 earlier, and I want to say, I think that this is a
14 function of the difficulty associated with getting
15 verifiable parental consent, and if you had a world in
16 which there was a broader scope of safe behavior that
17 permitted a website operator to rely on notice to the
18 parent only, you know, an email notice, and that it was
19 the parent's responsibility to then come back to the
20 website or the child and say no, that's something that
21 could be automated; that would foster communication.

22 I think there are -- is some percentage of 11-
23 and 12-year-olds who would provide their parents' email
24 address for that purpose. So, I mean, my only -- I
25 guess my point is that it's not -- from a practical

1 standpoint, the cost of getting verifiable parental
2 consent is still expensive in this environment.

3 MS. KRESSES: And Gwenn had one thing to say,
4 then we are going to move on to another question.

5 DR. O'KEEFFE: Just very quickly. The other
6 issue is that while I don't disagree with you that a lot
7 of kids would be truthful, it's not so much a matter of
8 truthfulness. It's a matter of there's still a digital
9 divide and participation gap. So, even if we didn't
10 have the age issue and even if we didn't have the
11 verifiable parental consent and we weren't dealing with
12 COPPA, getting younger kids online with their parents
13 knowing how to have them be online safely for the 8- to
14 12-year-olds is very challenging right now, because
15 parents don't understand the technologies as well as
16 we'd like them to understand them, especially for social
17 networking and even for things like AIM, and I don't --
18 you know, texting and all of those things.

19 I don't disagree that there are probably some
20 kids who could handle social networking, but certainly
21 not Facebook and certainly not for under 13. I would
22 even argue 13 can be too young because of the social
23 skills that it takes to negotiate that site right now.
24 But there are some new sites coming out for that age
25 group that would be a wonderful social networking site,

1 and I think that we have to respect the ages of kids
2 online and help parents be online more safely and that
3 13 is still a reasonable cut-off for kids outside of the
4 scope of COPPA.

5 MR. QUARESIMA: We have a couple of questions
6 from the audience. Let's see, I'm trying to balance
7 this.

8 Let me -- I am going to give some -- give at
9 least another five minutes, if not more, at the very end
10 for audience questions, but I do want to try to reach
11 two other topic areas, and one of them was essentially
12 to address this other question that we had over here, is
13 that if, you know, as part of the process, the
14 Commission expanded the definition of personal
15 information to include other things, I mean, how does
16 that -- how does that impact the actual knowledge? Will
17 it be easier to show actual knowledge if the definition
18 of personal information were broader?

19 So, let me, you know, start with -- I think let
20 me start with Christine maybe, if you had any thoughts
21 on that, and then we will go to Guilherme.

22 MS. JONES: I'm not sure if I know the color of
23 your car or -- what was the other thing you said?

24 UNIDENTIFIED SPEAKER: Hair color.

25 MS. JONES: -- hair color, that I have actual

1 knowledge of whether or not you're 13, but there's
2 definitely some combination of factors that I could tie
3 together that would make me believe that you're a
4 certain demographic.

5 I would be really careful about going too far
6 down that path, just because suddenly am I going to have
7 actual knowledge because some Google algorithm served up
8 an ad to somebody who's on my website because they -- I
9 don't know. There's just a ridiculous number of things
10 that are going through my head right now in terms of the
11 actual knowledge that could be ascribed to me because of
12 some algorithm that I'm relying on from a third-party
13 provider.

14 So, I would caution against making that too
15 broad and having too many factors that are going into
16 that actual knowledge, the definition of what includes
17 actual knowledge.

18 MR. QUARESIMA: Guilherme, go ahead.

19 MR. ROSCHKE: I think if -- once we start
20 broadening the definition of PII, which would start to
21 capture more behavioral advertising, it would certainly
22 impact the sorts of -- the actual knowledge and also the
23 directed-at-children determinations that are made. So,
24 the third party -- I think a third-party ad network that
25 promised to, like, deliver ads to someone under 13 is

1 likely saying that they have actual knowledge that these
2 people are under 13, and they arguably also fit under
3 the directed-at-children standard.

4 You know, actual knowledge can also be derived
5 from other age-related information, such as the grade
6 that people are in in school, you know, if you've got
7 them participating in a social group, such as the Cub
8 Scouts, you know, so an ad network collecting -- using
9 or targeting this information would qualify under actual
10 knowledge.

11 And, you know, lastly, you know, I think we
12 don't really have a directed-at-children panel, but, you
13 know, they would also be considered directed at children
14 under the traditional standards of the content, like the
15 creative content that they are using as a directed at
16 children or, you know, are the interest categories that
17 they're using directed at children, much like you have a
18 Barbie website be directed at children, the same with,
19 you know, an interest category of Barbie fans would be
20 directed at children.

21 MR. QUARESIMA: Okay.

22 MR. GREENBAUM: You know, what I would just say
23 there is that there is a big difference between actual
24 knowledge that personal information is being collected
25 from a child versus that you have the ability to

1 determine whether information is being collected from a
2 child. I think that those are two, you know, extremely
3 difficult things, and I don't think that the statute,
4 you know, would -- the second would fall under the
5 statute, but also, again, I don't think it would be
6 workable.

7 And the standard I would, apply which I think is
8 probably the standard we should judge all of this by, is
9 the phone number when you call Phyllis and Mamie and ask
10 them a question of, "Well, what do we do here?" And I
11 think it's important -- and if someone hasn't mentioned
12 already, I wanted to mention, which is I think that this
13 is such a model of really great government, which is
14 this -- the service that they have provided and the
15 ability -- and what they have given in terms of, you
16 know, being able to call up, have these conversations
17 with someone, you know, not the sort of notion of there
18 is no one at the other end of the line, but someone who
19 is really actually helping you comply, I think it works
20 so well. And I just want to commend them, because I
21 think it's an incredible thing.

22 But I look at some of these things and I would
23 say -- you know, I would call them up, and they would
24 go, "Yeah, I don't see how we would apply that." So, I
25 think we have to have a Phyllis and Mamie panel which

1 is, you know, we'll ask them these questions and see if
2 they could actually give us an answer, and then we will
3 know.

4 MS. KRESSES: Well, that actually -- you know,
5 it's people like Jeff and Becky and lots of people I see
6 out in the room that, you know, have, you know, in some
7 way contributed to the process that we're in now,
8 because we are, you know, reaching questions that are
9 not simple, and they apply to a lot of people. And so,
10 you know, we thought this is a way to get at that.

11 But I want to turn the discussion a little bit
12 around and ask the question, assuming that an operator
13 really does want to use its best efforts to identify
14 kids on its service who are lying about their ages, does
15 the actual knowledge standard deter the best efforts of
16 these companies because they don't want to acquire
17 actual knowledge? And I was wondering if anyone would
18 speak to that.

19 Phil.

20 MR. TERZIAN: I'll take that one. No, I
21 don't -- I would say no. You know, we're part of a safe
22 harbor program, and no one's really talked much about
23 that yet, but it's also something that's commendable
24 that the FTC provides and that there's four great
25 providers in the room here as well, and it's part of our

1 program, and we focus on screening and registration for
2 both compliance, you know, we don't do it in a tricky
3 way to try to, you know, check if you're under 13 here
4 or over 13. We do it very neutrally, in line with what
5 the FTC has given guidance on.

6 I think that's consistent with the intent of the
7 law and the practical realities of trying to screen out
8 the children, assuming, as we all agree, that, you know,
9 not every child is going to tell the truth, but I think
10 that's the best you can do with it, is leave it the way
11 it is.

12 The other thing is, what can you do post
13 registration? You know, it's one thing to talk about
14 trying to determine how old someone is at a set point in
15 time, predictable, consistent, versus trying to figure
16 out -- there's been a lot of talk on it already, so I
17 won't go into it -- trying to figure out what someone is
18 saying later on that might give rise to something else.
19 You know, in the vast world of user-generated content,
20 it's a very daunting task to even touch upon on that.

21 MS. KRESSES: Becky, do you have any thoughts on
22 that?

23 MS. BURR: I guess if you ask -- I mean, if you
24 age-gate, then you -- let me step back.

25 I don't -- I'm not sure it's the actual

1 knowledge standard that is a problem here. I think we
2 just have to be realistic about what a website can
3 actually do in an automated fashion that doesn't
4 require, you know, thousands of people standing up and
5 looking at the information afterwards.

6 My sense is that there are a lot of sites out
7 there that are responsible and do want to identify
8 underage children and are using various tools to do
9 that. They're not fool-proof. But to the extent that
10 tools still require a human being at the end of the line
11 to look at them, that is difficult and expensive and not
12 particularly consistent with the economics of most of
13 the websites.

14 MS. KRESSES: And would it help if there were
15 some sort of safe harbor for taking an effort, that you
16 would not be, you know, punished for that effort? Do
17 you think that would be something that businesses would
18 be interested in?

19 Christine?

20 MS. JONES: Well, we always like a good safe
21 harbor provision, and we use them to great effect every
22 day. The DMCA is a great example. But I think the
23 answer to your original question here is no, absolutely
24 not. If we go out and tell website operators to collect
25 more information about kids so we can figure out if

1 they're kids, that is counter-productive, guys. That
2 specifically does not protect their privacy, right?
3 We're collecting more information when we should be
4 collecting less information. So, the answer to that
5 question is no.

6 What website operators can do if they really
7 care about protecting kids is look at the collective
8 data that you have. If you think it might be a kid,
9 don't serve up porn spam, okay? If you think it's a
10 kid, then don't give them stuff that kids shouldn't see.
11 I mean, really, if we're really trying to protect
12 children here and really trying to protect kids'
13 privacy, don't collect more data about them, and don't
14 show them stuff that they shouldn't see.

15 I mean, honestly, it's not that hard if you're a
16 good website operator. Most of the ones that we've
17 talked about here today, the big ones, are, right? This
18 is about the smaller, maybe less upstanding corporate
19 citizens that we're trying to talk about, right?

20 MS. KRESSES: That's your words.

21 MR. GREENBAUM: This was not a statute that was
22 designed to create incentives for websites to monitor
23 the websites. I mean, it's not like the CDA, which, you
24 know, certainly provided the ability of websites to
25 monitor and take action when it felt it was necessary,

1 and, you know, certainly I think that many companies
2 will be very, very responsive to -- if there were ways
3 that -- you know, that the FTC or Congress, if
4 necessary, provided the incentives or the ability of
5 companies to do more that they wanted to do, I think
6 many, many companies want to do that, and I think that
7 there are many people that feel constrained.

8 I also think we have to recognize that there is
9 a limit to what we can do in a rule or a statute. At
10 some level, I think there's lots companies can do, but,
11 you know, there's people -- the people at the other end
12 of the line, the parents are going to have to do it,
13 too, and I think that we all have to recognize as
14 parents that, you know, a lot of this and a lot of the
15 great work that's been done is about the education, and
16 certainly COPPA served that role, too, but really, it's
17 going to require some in-person monitoring, too, and we
18 are going to have to continue to balance the interests
19 here to make sure that, you know, we get the good parts
20 out of both.

21 MS. BURR: Mamie, I would be really, really
22 careful about a safe harbor here, only because I think
23 that, you know, applying a standard across a huge
24 variety of websites is very, very hard to do, and you
25 may end up with a sort of de facto minimum --

1 MS. KRESSES: Floor.

2 MS. BURR: -- that comes back to bite you when
3 what you've selected as the safe harbor isn't possible
4 given the site arrangement.

5 MS. KRESSES: Okay.

6 MR. QUARESIMA: I want to --

7 DR. O'KEEFFE: One quick point. I just want to
8 echo what Jeff said. I mean, education is ultimately
9 the bottom line, and I think parental empowerment -- you
10 know, no rule is going to be fool-proof, but I think we
11 can all agree that we can empower parents to be more
12 involved with their kids and we can all help to educate.
13 And I don't think any of us do enough to do that, and I
14 think all businesses actually should take a more active
15 role in education.

16 And I think if everybody reinforced the same
17 messages about online protection and privacy of kids,
18 independent of this rule, kids would be safer online,
19 and help parents do a better job parenting online. If
20 everyone does that, frankly, a rule is not necessary.

21 MS. KRESSES: Okay.

22 MR. QUARESIMA: Phyllis, did you have something?

23 MS. SPAETH: Yeah. I just wanted to say that,
24 again, the Net Cetera guide is incredible. I'm thinking
25 about Ad Mongo -- which doesn't have to do with the

1 Internet, it has to do with advertising -- but that's
2 something that goes into schools. I think that a
3 program that started teaching in schools about the use
4 of the Internet, starting at a really young age, when
5 kids first go online, I think that would do more than
6 anything.

7 MS. KRESSES: Okay. So, we only have a couple
8 minutes left, so I would really like to -- we would love
9 to hear from people on the other side of the table, any
10 other thoughts about the actual knowledge standard or
11 questions.

12 UNIDENTIFIED SPEAKER: I have two comments, one
13 in regards to the constructive knowledge standard or the
14 directed-to-children standard. You know, I think the
15 flexibility in that standard that exists today is a good
16 thing for industry, and in particular, when you look at
17 the types of games on the Internet today, many of which
18 are not for kids, a lot of them are animated, have heavy
19 animation. I think the world is animated today. We're
20 living in an avatar world. So, I think the flexibility
21 there and the consideration of various factors is a good
22 thing, and that should certainly stick to the extent
23 that it can.

24 The second comment I have is really with regards
25 to actual knowledge, and I don't think that this was a

1 point that was addressed on this panel -- forgive me, I
2 walked out for a few minutes -- but that is the issue of
3 who has the duty -- now, COPPA doesn't have an explicit
4 requirement to screen for age in particular, but the
5 question is, who has the duty, when you've got these
6 devices which are Apple devices, okay, and you have got
7 the front-end platform, which is iTunes, and then you
8 have got the third-party developers, and then the same
9 thing is true -- so, if you have got the third-party
10 apps, the mobile apps.

11 The same thing is true in the Facebook world.
12 You have got the Facebook platform, as well as other the
13 social network platforms, and you have got the
14 third-party developer, games and whatnot, sitting on top
15 of that, and there is data being exchanged, right, and
16 there are assumptions being made as to the ages of the
17 user, and today, most of these third-party apps, whether
18 they're on the mobile devices or in the Internet world,
19 are really relying on the original entry point, whether
20 it's Facebook, MySpace, iTunes, to determine what the
21 age of the user is. Is that -- who has that duty?
22 Where do we see that going? And is there any guidance
23 that could come out of COPPA on that issue?

24 MS. KRESSES: Does anybody on the panel want to
25 touch that?

1 Guilherme.

2 MR. ROSCHKE: I think to the extent that each
3 one of them is an operator of an online service, each
4 one has to make their own determination of whether they
5 are directed at children or whether they have actual
6 knowledge. You know, the information that's flowing
7 back and forth between these services can add to the
8 actual knowledge determination.

9 If I have Facebook Connect on my website and I
10 use the information from Facebook Connect, then that's
11 part of the knowledge that I have about my users.
12 Likewise, if Facebook Connect is just -- you know,
13 without me -- you know, is sending the information to
14 me, I -- that's -- that's part of the information that I
15 have available to me that would go into my determination
16 of the age of my users.

17 MS. KRESSES: And does that -- you've both
18 raised a good point and something we actually wanted to
19 get to and just didn't have time, but, Guilherme, does
20 the services like the OpenID and Facebook Connect,
21 Google Buzz, does that -- if kids are aging up to set up
22 those accounts, does that complicate the actual
23 knowledge discussion?

24 MR. ROSCHKE: I mean, I think it complicates it
25 in the sense that it adds more information to the actual

1 knowledge determination. I don't think it complicates
2 it too much from the point of view of information is now
3 more hidden.

4 And then you also have the determination of, you
5 know, whether their operator -- you know, who is the
6 operator of the online service? I think it's -- you
7 know, we saw here in the earlier panel that there could
8 be more than one. So, it's -- I don't -- I think each
9 unit here is going to make its own determin -- have to
10 be determined separately.

11 MS. KRESSES: Okay. We have, like, one or two
12 minutes. Do we have any other questions? There's
13 someone right here.

14 UNIDENTIFIED SPEAKER: In terms of the actual
15 knowledge standard, there are a number of websites who
16 follow Phyllis' recommendation of trying to do more. I
17 would say that I'm aware of several companies who
18 institute neutral age screening, per CARU/FTC
19 recommendations, to try to prevent collecting personal
20 information from somebody who's a child.

21 Those sites typically report that 25 to 30
22 percent of their complaints from adults is that they're
23 age-screened out; they can't access the content; they
24 can't go to the shop. And it goes back to I think a
25 point several panelists made, that these are

1 interconnected issues, that the standard that you apply
2 in going beyond that standard imposes costs on a company
3 and imposes burdens on the consumer that you're actually
4 trying to target.

5 I'm curious if any of the other panel members
6 have experience or comments on that particular issue.

7 MS. KRESSES: Anybody have any comment? Okay.

8 And I think there was another question right
9 here.

10 UNIDENTIFIED SPEAKER: In a recent survey of
11 under-13s, where they were playing online, two of the
12 top games in the top five of under-13s were actually
13 games that were on the Facebook platform, so they
14 shouldn't be playing them. Is it fair that websites
15 that do ask for age and do accept under-13s cannot sit
16 on that platform? So, they are excluded from sitting on
17 the Facebook platform, where are the games are just
18 age-gates?

19 MS. KRESSES: Does anyone want to comment on
20 that?

21 MS. JONES: I'm not sure I understood the
22 question.

23 MS. KRESSES: So --

24 UNIDENTIFIED SPEAKER: So, the question is, on
25 Facebook platform, you're over 13, okay? So, the games

1 that are on there, a recent survey of under-13s, two of
2 the top games they were playing were on the Facebook
3 platform. Is it fair that games that do ask for the age
4 of the users and do allow under-13s are excluded from
5 that platform, which is a powerful platform?

6 MS. KRESSES: That's a great question. I don't
7 know that we have an answer, but --

8 MS. BURR: Actually, I think it is a really
9 great question, and it is a question where if you had
10 some differentiation, you could address that problem.
11 So, you have a platform that you're providing notice to
12 parents on about -- you know, an email notice about your
13 kid is doing this, and then there's some game or some
14 add-on or something else that requires a greater level
15 of sophistication or maturity, you can age-screen, and
16 you're not penalized down the line. So, I actually
17 think that there is a way to do it, but it involves
18 changing the dynamics about how hard it is to get
19 parental consent.

20 MS. KRESSES: And with that, we are going to
21 come back for Panel Four, which talks about parental --
22 Panel Three, sorry, and then later Panel Four. So,
23 let's break for lunch.

24 (Applause.)

25 (Whereupon, at 12:03 p.m., a lunch recess was

1 taken.)

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 AFTERNOON SESSION

2 (1:16 p.m.)

3 MS. RICH: So, welcome back after lunch. This
4 is Panel Three. My name is Jessica Rich. I'm Deputy
5 Director of the Bureau of Consumer Protection here at
6 the FTC. And this is Michelle Rosenthal from the FTC's
7 Division of Advertising Practices. We're going to
8 co-moderate.

9 So, this is the panel on personal information.
10 As you all know, the FTC issued its COPPA rule in 1999,
11 which is dated, as previously noted now, in what seems
12 like the dark ages in the online world. As part of this
13 Rule review, we're examining the rule's definition of
14 personal information. Does it still make sense?

15 Certainly the kinds of information that can be
16 used to contact an individual -- I'm having some trouble
17 with this mic -- okay, have changed over the last 11
18 years. Companies are collecting, retaining, combining,
19 using and sharing data in ways we never could have
20 anticipated a decade ago. The key question for us is,
21 what information permits the physical or online
22 contacting of a child under 13?

23 During this panel, we'll focus on the definition
24 of personal information, both in the rule and the COPPA
25 statute. As you may know, when promulgating the Rule,

1 we did not stray far from the definition in the statute,
2 and as shown on the screen -- and I think each of you
3 has a handout -- the COPPA Rule currently includes in
4 its definition the following pieces of data:

5 First and last name; home or other physical
6 address, including street name and name of a city or
7 town; email address or a screen name that reveals an
8 individual's email address; telephone number; Social
9 Security number; persistent identifier if it's
10 associated with individually identifiable information;
11 or a combination of last name or a photograph with other
12 information if the combination permits physical or
13 online contacting; or information concerning the child
14 or his parents that the website collects from the child
15 online and combines with one of the identifiers we've
16 already listed.

17 In addition, Part (f) of the statute gives the
18 FTC authority to include any other identifier that
19 permits the physical or online contacting of a specific
20 individual. So, the big question is, what does it mean
21 to contact a specific individual?

22 In the past couple of years, we've had some
23 experience with the evolving nature of data and data use
24 and personal information and what that means in other
25 contexts. In 2008, in 2009, we issued a report and a

1 set of principles to address online behavioral
2 advertising. In that context, which is the use of data
3 to target personalized advertising, we said that the
4 traditional dividing line between personally
5 identifiable information, PII, and non-PII has become
6 blurry and may not make sense anymore, staring at the
7 person who wrote that report sitting right across from
8 me.

9 That's because certain data, once thought to be
10 anonymous, may no longer be so due to technological
11 changes, and just as important -- and this came up in
12 some prior panels -- little bits of anonymous
13 information, if pieced together, may actually become
14 personally identifiable once those pieces are put
15 together.

16 And we also -- we held some recent roundtables
17 on commercial privacy writ large, not just about kids,
18 and there we discussed the need to look at geolocation
19 data and static IP addresses and consider how those --
20 you know, how identifiable those pieces of information
21 are and how they implicate consumer privacy.

22 And just a few months ago, we expressed some
23 concern to Netflix that the release of large amounts of
24 consumer data that everyone thought was anonymous may
25 actually be reidentifiable given the state of technology

1 and the large quantities of available data that's out
2 there.

3 So, I imagine with this great group of
4 panelists, these issues are going to come up today, and
5 we want them to, but we need to remember and keep in
6 mind that the particular context and focus here is
7 children's online privacy and the concerns and
8 objectives that led to passage of COPPA and the
9 promulgation of the COPPA rules. So, we want to keep
10 bringing it back to that.

11 So, let me briefly introduce our panelists.

12 To my right, we have Maureen Cooney of TRUSTe, a
13 COPPA safe harbor.

14 We have Paul Ohm from the University of Colorado
15 Law School.

16 We have Sheila Millar from Keller and Heckman.

17 Michelle over here.

18 Kathryn Montgomery from American University.

19 Matt Galligan from SimpleGeo Company.

20 Jules Polonetsky from the Future of Privacy
21 Forum.

22 And Heidi -- is it Salow?

23 MS. SALOW: "Salow."

24 MS. RICH: "Salow," sorry -- from DLA Piper.

25 And Kathryn and Sheila, among others -- me, too,

1 actually -- have been members of the COPPA family from
2 the very start, so they, along with Toby, who is still
3 here, and I'm sure many others of you can pipe -- oh,
4 Angela -- can pipe -- there she is, oh, yeah -- oh,
5 there you are -- can pipe up with a historical
6 perspective, when needed. So, let's get started.

7 So, we talked about the language of COPPA and --
8 of the Rule and the personal identifiers that are in
9 that now. So, speaking of historical contexts, maybe we
10 can talk about how we originally identified those list
11 of identifiers and what was the significance of those
12 identifiers. Some of them are obvious.

13 But, Kathryn, do you want to take that?

14 MS. MONTGOMERY: Sure. And it's really
15 heartening to see, you know, ten years later, how well
16 we've done implementing this law and how robust it is.
17 We were talking about words we weren't going to use
18 anymore, and we have had a very granular discussion
19 today, and as we all know in Washington, when we talk
20 about policy, the devil's in the details -- you didn't
21 have that on your list -- but, you know, it was a
22 challenge to do all of this.

23 I do want to remind people that -- and a couple
24 people have already mentioned it, maybe including me --
25 that we created COPPA and we advocates pushed for COPPA

1 because of concerns about digital marketing and about
2 the need to ensure that there were some safeguards in
3 the new digital marketing environment, which was in its
4 earliest stages at that point.

5 And even then, we could see that the business
6 model that was governing most all of digital marketing
7 at the time was called one-to-one. It was the idea of
8 personalized marketing messages targeted at individuals,
9 and children were one of the most powerful, most
10 lucrative markets at the time, and there was an enormous
11 amount of energy and innovation going into developing
12 commercial applications aimed at children.

13 So, what we wanted was to ensure that there were
14 some safeguards, based on long-done studies, studies
15 over a number of decades, that showed that children
16 simply didn't have the developmental capacities, the
17 cognitive capacities, to deal with all of this and to
18 respond to many of the personal appeals, with marketers
19 talking at the time about wanting to develop
20 personalized, ongoing relationships between product
21 spokes-characters and children.

22 That was the one comment in a trade conference,
23 trade association conference, that just kind of hit me,
24 and, you know, it was an epiphany, and I realized, okay,
25 we need to do something to ensure that there are

1 safeguards.

2 So, at the time, of course, children were being
3 mainly supplying information, and there weren't any
4 rules, it was like the wild west, so they were being
5 asked for all of this stuff. So, we wanted to specify
6 specifically what kinds of information would enable
7 marketers to communicate directly with them, but we were
8 also very aware at the time that the so-called passive
9 technological mechanisms for identifying children and
10 for collecting information from them -- at the time, I
11 remember one of the terms was mouse droppings, that one
12 seems to have gone by the way -- but it really was a
13 precursor -- I know, that's pretty disgusting -- but
14 that really was a precursor to what we have now with
15 cookies and other types of data collection and tracking
16 mechanisms.

17 So, what we see now -- also, the other thing I
18 just want to add here that nobody's really brought up is
19 that one of the goals of the law was to minimize data
20 collection from children, and often that gets missed and
21 people don't realize that that was one of the
22 intentions.

23 So, we're now at a time when the industry has
24 evolved, as everybody has been talking about, and I'm
25 pleased that the language in the law is flexible enough

1 to accommodate many of these new practices. So, it's
2 very good that we're having this conversation today.

3 MS. RICH: So, does anyone -- so, we have
4 these -- the list -- is this one on?

5 MS. ROSENTHAL: Yeah.

6 MS. RICH: Okay. I seem to have trouble with
7 the mic today.

8 MS. MONTGOMERY: I thought we were sharing. Do
9 you want mine?

10 MS. RICH: That's okay. I can share with her.

11 So, we have a list of identifiers. Maybe we
12 could -- without trying to get too abstract here, maybe
13 we could talk a little about why these identifiers are
14 on this list, what characterizes them, which might help
15 us to determine whether there's things left off the list
16 or things that shouldn't be on the list anymore.

17 Jules, do you want to talk a little about what
18 it means to permit the online contacting of a specific
19 individual and why these identifiers are on it? And
20 maybe we can start talking about what else might fit
21 those criteria.

22 MS. POLONETSKY: Well, having still been in, I
23 guess, city or state government at the time of COPPA,
24 it's been a great experience to spend time over the
25 years with Parry and to hear from Kathryn and some of

1 the others who were so instrumental and with all of you
2 at the Commission. So, the history of why and how one
3 picked these in those early days I'll leave to others,
4 other than they obviously are sort of the most obvious
5 subset of personal information.

6 But I think what has happened over the years
7 that has changed -- and I'm not sure this is something
8 that easily fits into the COPPA structure -- but what I
9 think has dramatically changed over the years, I think
10 in the time that these identifiers were selected, these
11 were the ways that, (a) you actually reached out and
12 touched somebody and visited them and, you know, called
13 them, visited their house, could contact them; and then
14 the second really interesting thing that comes along
15 with these sorts of things is they were the keys to all
16 the other data that's available about people.

17 And so by having a name or an address or a phone
18 number, the databases that are available for all the
19 other robust marketing purposes can be brought in and
20 queried. And if you didn't have any of those, it wasn't
21 really easy to bring in all the other data that's out
22 there online and offline.

23 I think what's happened on both those fronts --
24 the can I maintain a relationship with you and message
25 to you or can I correlate lots of other information out

1 there about you -- I think that's really dramatically
2 changed. It was always theoretically possible, but
3 today, it's par for the course for information to be
4 either deidentified or never actually identified, but
5 given that a user may show up and authenticate
6 somewhere, to correlate the other data that's available
7 about them, appending it throwing it over the wall,
8 leaving it on a cookie, and being able to maintain that
9 there's never been any identification, but yet, the
10 PII-connected data, all the other lifestyle stuff,
11 purchase activity, whatever it is, can end up being
12 available online, and, indeed, that's, you know, a
13 significant part. Technically, folks don't call it
14 behavioral. It's appending; it's adding data. It's not
15 necessarily your clickstream, but it's adding data.

16 So, to the extent that that was intended to be
17 the dividing line for PII or not, that's sort of long
18 been crossed. You know, around the world, folks argue,
19 "Well, therefore, it ought to be personal." I don't
20 think we've gone that far in the U.S., but clearly the
21 correlation of PII is no longer limited to PII.

22 Then I think the second thing that's happened
23 that has dramatically changed was you couldn't easily
24 maintain a relationship with somebody without them
25 identifying themselves in various places online or

1 offline and then correlating that, and today, whether
2 it's because of cookies, whether it's because of other
3 identifiers, I can maintain that relationship. That
4 wasn't that unique back then, but I think what's
5 happened today is I would have had to go to lots of
6 places and separately, you know, try to interact with
7 you. Today, because of ad exchanges and data exchanges,
8 I can maintain state with one user across websites,
9 across end networks, across sometimes even devices and
10 platforms.

11 I don't see how easily, you know, we broaden the
12 COPPA definition because it breaks down on a lot of
13 these other issues around actual knowledge, around, you
14 know, being able to get consent, but it certainly raises
15 a whole host of marketing issues that, you know, Kathryn
16 just kind of put out there as, well, we wanted to deal
17 with those. There is today a whole host of marketing
18 issues that can happen quite discretely, as well as
19 maintaining a relationship and messaging the same person
20 over lots of places because of the way the technology
21 and the data use has evolved.

22 MS. RICH: Okay. So, you have put forward two
23 basic things, which is maintain a relationship and
24 correlating other data so that you can end up
25 identifying somebody. Keeping those criteria in mind --

1 and people can add to that or dispute that -- I'd love
2 to hear ideas about other data. I have my own little
3 list that I'm planning to get to, but better for the
4 panelists to toss it out, other data that may fit that
5 criteria that aren't on this list.

6 MR. GALLIGAN: Sure. So, I see three categories
7 of data, of identifiers, and I break them down as
8 exclusive, derivative, and additive. So, an exclusive
9 identifier is something that on its own can identify an
10 individual. That would be something like first
11 name/last name, physical address, telephone number,
12 Social Security number. Those are exclusive
13 identifiers, because without any other information, I
14 can find out the individual.

15 An additive identifier would be something like
16 with any one of those individual exclusive identifiers
17 or with multiple additive identifiers, I can find out a
18 identity. So, I can take -- let's just take
19 geolocation, for example, which is something that is
20 proposed. On its own, a coordinate doesn't necessarily
21 speak to who somebody is. It might speak to where they
22 are at that given time, but it also doesn't mean home or
23 work. It could mean anything. It could mean the coffee
24 shop down the street that they frequent. It could mean
25 the park that they like to go to. But just a coordinate

1 doesn't necessarily identify a specific individual.

2 However, a coordinate attached to any one of
3 these other categories could better identify an
4 individual than even a physical address, because we're
5 going beyond an address to something far more specific
6 than an address. So, that's what I would consider an
7 additive identifier.

8 A derivative identifier is something we haven't
9 discussed, which is using a third party to identify a
10 person. So, Facebook Connect, for example. So, using
11 Facebook Connect, I can, let's just say, log in using my
12 Facebook identity, and it now generates an ID. If I was
13 a Web service using Facebook Connect to identify my
14 users, it generates an ID whenever I sign in. That ID
15 can be called using something called FQL, Facebook Query
16 Language, and by FQL, I can identify first name, last
17 name, gender, date of birth, address, anything that has
18 been allowed within FQL. And that's not necessarily
19 something that I own. I only own that ID, but by using
20 that ID, I can correlate that with any other information
21 that Facebook has on me.

22 And the same could be said for any API that has
23 personally identifiable information, be it Twitter, be
24 it Google's ID service, any of that. But that's I would
25 consider a derivative identifier.

1 MS. RICH: So, do all three classes of those fit
2 the COPPA statute definition, which is an identifier
3 that permits the physical or online contacting of a
4 specific individual, or a subset?

5 MR. GALLIGAN: I think it just depends upon what
6 each one of them is. I think exclusive personal
7 identifier means that without a doubt, it does allow for
8 the contact, because you can find out anything else on
9 that list. Additive would mean that you would have to
10 have multiple sources to be able to get to that point,
11 but you could potentially get to that point if you had
12 multiple sources. Actually, I think derivative probably
13 is almost up there with exclusive, because most likely,
14 that information exists and resides somewhere else and
15 you're able to correlate that with something else.

16 But the additional problem with derivative is
17 that you question whose responsibility is it at that
18 point? Who's falling under the COPPA rule? Is it the
19 person that is collecting that identity, or is it the
20 person that "owns" that identity, meaning the original
21 service provider that actually has that information
22 stored in their database?

23 MS. RICH: Okay. So, does anyone else have
24 comment on the way he's characterizing this?

25 Paul?

1 MR. OHM: This is actually a comment on the way
2 you're characterizing things. Whenever people talk
3 about the COPPA family, I feel like I'm not quite a made
4 man yet, because I'm coming to this with fresh eyes, but
5 I think it helps me play the role of a judge looking at
6 this statute without living and eating and sleeping it,
7 as a lot of you have.

8 What I see when I read this statute is I'm not
9 sure that the language in (f), which is what you keep
10 citing to, which permits the physical or online
11 contacting, necessarily is the be-all and end-all of
12 what the FTC is supposed to regulate. I mean, I
13 understand that (f) is our guiding light, but the thing
14 I would say is if you look at the rest of the list and
15 if you look at Social Security number, in particular, I
16 mean, I think there is a judicial argument that we can
17 get some interpretive use out of why Congress included
18 Social Security numbers in the list, right?

19 What is it about a Social Security number? I
20 mean, there's obviously a lot of misinformation about
21 how secure it is, how sensitive it is, what it can be
22 used for, but the key attribute of a Social Security
23 number is it's the key to linking lots of different
24 databases together, right?

25 And so Congress, in its infinite wisdom, said

1 when we're talking about permitting the physical or
2 online contacting, we want to include Social Security
3 numbers because they're in this list of types of
4 information that are so linkable that we're going to,
5 per se, just add them to the list. So, I think
6 linkability has to be part of the Commission's charge
7 here.

8 I think the Commission has to look at different
9 types of information, and the Commission has to ask
10 itself, how linkable is this particular type of
11 information given what we know about the state of data
12 in the world, who holds data, the amounts of which they
13 hold data?

14 And I know one of the reasons I was invited to
15 be here is because I have done a lot of recent research
16 in reidentification. I don't want to monopolize the
17 microphone at this point, but I'm happy to throw the
18 proposition out there that the computer scientists have
19 recently begun to kind of chip away at this entire
20 construct, this idea that some pieces of information are
21 really, really, really linkable and some pieces of
22 information are not terribly linkable and we could worry
23 a lot less about them.

24 And if you are really aggressive about it -- and
25 I have been accused of being aggressive in the past --

1 there are lots and lots and lots of pieces of
2 information that are much more linkable than we ever
3 realized and much more linkable than we realized in
4 1999, certainly. So, I have lots more to say about
5 that, but I will...

6 MS. SALOW: Jessica, this is Heidi. I will just
7 add one more thing. I liked the way you categorized
8 those three categories, and I think all three are
9 actually encompassed already in the definition. We
10 have -- I'm not sure if I am going to use the same
11 terminology, but the exclusive identifiers are the
12 obviously the individual data elements, right? We have
13 additive in (f) and in (g). And then I think we also
14 have -- what's the one, the reverse engineering?

15 MR. GALLIGAN: Derivative.

16 MS. SALOW: Derivative, we have that as well I
17 think in (f) and (g) built in.

18 And I also would agree with the linkage issue.
19 I would suggest that the way the definition is written
20 now actually leaves open lots of room for the FTC to
21 decide that there are other data elements out there that
22 can allow a company or a website operator to contact a
23 child without needing to even revisit. I think that
24 you've got the flexibility here to, you know, get in
25 line with technological developments, and I think that

1 was probably intentional.

2 MS. RICH: Okay, so -- oh, Sheila.

3 MS. MILLAR: I think that's right, and I also
4 think that it's important when we talk about any of
5 these issues that we keep in mind the greater construct
6 of the statute, because we need to talk about website
7 operators and online service providers and targeted to
8 kids, directed to kids, or actual knowledge about kids,
9 and the gray area, if you will, is in that
10 additive/derivative area where you don't know.

11 You might have an email address of an
12 individual. You have no idea that it's a child. But if
13 you've collected that at a kid-oriented website, then
14 you have kids' data, and you handle it appropriately.

15 I think to Kathryn's earlier point, one of the,
16 I think, important things to remember about COPPA is
17 that there was tremendous support by the business
18 community for COPPA, many of whom were active members of
19 CARU, as Phyllis mentioned, and who were living by many
20 of these rules -- not obviously in the same level of
21 detail or enforceability -- for a number of years before
22 COPPA was adopted.

23 And so for those kid sites, they've embraced
24 COPPA, they've lived by COPPA, they understand that
25 they're dealing with kids, and I think it gets harder

1 when you alter the definition, particularly if you're
2 going to expand the universe and expand the standard of
3 who knows what about you, you exponentially change the
4 burden, which is a very important issue, because a lot
5 of folks out there -- it's not that they don't care
6 about kids. Everybody cares about kids. Everybody
7 wants to protect kids. It's a matter of how do you do
8 it and what's a reasonable way to go about addressing
9 any issues to the extent there are issues?

10 MS. RICH: Okay, thanks.

11 Well, I wanted to get to sort of some concrete
12 examples, which I think people are dying to get to, and
13 the ones that we've certainly heard talked about today
14 and in comments, there's four different examples, and I
15 want to know if there's other classes of data we should
16 be talking about.

17 There's behavioral advertising, which has
18 already come up quite a bit today. There's geolocation
19 data, which Matt is dying to talk about. There's -- and
20 we are, too -- there's, of course, IP address, which is
21 constantly an issue that everyone wants to explore. And
22 there's aggregation of allegedly anonymous data, which
23 is a tall issue, as well as all of our concerns.

24 So, why don't we -- are there other obvious
25 categories of data that we should be debating today at

1 this panel?

2 MS. MONTGOMERY: Can I --

3 MS. RICH: Yes.

4 MS. MONTGOMERY: I don't know if we have talked
5 about in-game advertising and avatars, but to the extent
6 that avatars are individually identifiable, I mean, we
7 would have to look more closely, but they do permit the
8 kinds of relationships and interactions and targeted
9 personalized marketing that this law was intended to
10 address.

11 MS. RICH: Okay, that's a great addition.

12 So, why don't we take these one at a time and
13 see where we go with this. So, why don't we start with
14 IP address, since it's the most basic, understanding
15 that IP address is actually collected far more than -- I
16 mean, it's collected immediately. So, we have got a
17 real issue about IP address, and if somebody would like
18 to just give us the basics on the theory as to why IP
19 address should and shouldn't be considered personally
20 identifiable information.

21 Paul?

22 MR. OHM: I mean, I can. And by the way, I
23 classified my research as a -- I'm an import/export
24 specialist. I was a computer science undergrad and then
25 a systems administrator for a few years and in that job

1 spent a lot of time living in the APACHE log files and
2 trying to figure out who was visiting the website for
3 what purposes, and I promise you they were all noble.

4 But the point -- I think this is commonplace to
5 everyone in this room -- is that there once was this
6 belief that IP addresses were these evanescent little
7 fragile bubbles that disappeared every time you hit
8 reload on your browser, and, of course, many, many, many
9 technological and organizational decisions have
10 conspired to make that really no longer true and that we
11 all know this, right?

12 Your cable modem is always on. Your DSL is
13 always on. Your computer with its DHCP settings is not
14 getting a dynamic IP address that frequently, and I'm at
15 the point now where my home computer has the same IP
16 address probably for months on end, at least the last
17 time I looked at it, and at work, it's even more
18 ridiculous. I'm basically always attached to a single
19 IP address.

20 So, the idea now is there is this very
21 persistent piece of information about your computer --
22 that's an important caveat, not necessarily you, but
23 your computer -- that, as you say, is promiscuously
24 handed out to everybody. So, the idea is that once you
25 have this IP address, you now have this fulcrum upon

1 which reidentification can occur, and if we attach it to
2 a home address in this one instance and if we attach it
3 to a credit card in this instance and what you did on
4 Facebook last night in this instance, if you're a
5 savvy-enough data aggregator, you are going to be able
6 to use that one piece of information to correlate lots
7 of pieces of information.

8 So, what does this start to sound like? It
9 starts to sound like the modern Social Security number,
10 and what animated Congress to include Social Security
11 number in 1999, I'd submit, probably brings IP addresses
12 into a similar category, but let me have one important
13 caveat, and Sheila kind of made this point, which is we
14 can't break the Internet, right? And so you're right.

15 The APACHE log, for no pernicious reason, saves
16 IP addresses as soon as you install it. It seems like
17 it would be an unwise regulatory decision to then say
18 that anyone who collects IP addresses automatically has
19 to start worrying about COPPA, but my argument would be,
20 that's a matter for regulatory discretion and restraint
21 more than it is a hard question under the statute.

22 I would -- you know, I like to tell my students
23 when I see a legal battle which side would I rather
24 represent. Oh, yeah, I'll represent the side that
25 argues that IP addresses fit comfortably and squarely

1 within this list. So, then the question is, should we
2 really be putting this onerous burden on every website?
3 And I would say probably not.

4 MS. RICH: Well, let's get that answer. Should
5 we be putting this burden on every website?

6 MS. SALOW: I'm dying here, but I'll wait for
7 Jules.

8 MS. RICH: Kathryn first.

9 MS. MONTGOMERY: Age comes first.

10 Well, I think we need to always get back to the
11 goal of addressing marketing. So, if you look at how --
12 and you have to then look at contemporary business
13 models and the extent to which IP addresses -- and the
14 other things, and I think it's hard to talk about them
15 in isolation really, because that's not, in reality, how
16 they work.

17 It's a system of marketing that is designed to
18 identify individual consumers, and in the case of
19 children, then I think there is a burden, and I
20 understand as well that, you know, industry -- we did
21 negotiate with industry on a certain set of rules, but
22 there has been an understanding that the business
23 evolves, and those rules have to be updated -- in
24 response to your comment -- in ways that will really
25 meaningfully address what's going on.

1 So, for example, I've looked at some children's
2 websites -- and we are going to be submitting comments
3 -- through the Center for Digital Democracy and the
4 Coalition For Children and Consumer Groups, where we can
5 see that children under 13 are on the sites that are
6 designed for them, parents may give permission, and the
7 privacy policy says we only do this and this and this,
8 but there is other evidence that suggests there's a lot
9 more going on there that may be enabling marketers to
10 personally market to individual children. And I'm not
11 certain that all of that's being disclosed.

12 MS. RICH: Jules?

13 MS. POLONETSKY: So, I mean, I guess one point
14 before we touch the IP address, which relates to it, you
15 know, it would be really interesting if what was here
16 was, you know, an identifier that's widely and globally
17 used, because that would include a lot of interesting
18 things, frequent flyer numbers. Social Security number
19 kind of comes with the government-backed you can't get
20 rid of it, this, you know, special category, this is
21 your passport number, and so forth.

22 So, I'm not sure I would look to it -- you know,
23 to make Paul's point, I think, you know, (f) perhaps,
24 you know, faints in that direction, although again, it
25 ends up being linked back to that tied with, you know,

1 PII. So, I think the statute and rule kind of push a
2 little bit away from drawing the broad conclusion there.

3 And the second thing is, you know, Paul, in his
4 paper, does a great job of kind of looking at the scope
5 of research out there, and I think, you know, it's
6 certainly conventional wisdom in one part of the
7 community that just about anything when you've got a lot
8 of data or even not that much data can become
9 identifiable with enough rocket scientists or even maybe
10 with just enough smart people doing some work.

11 And if that's going to be the screen of, like,
12 whether something starts becoming verboten, we're
13 screwed, right, because the reality is that just about
14 covers, wow, everything that is out there. And to the
15 extent that we want to recognize that but yet give
16 people credit for not going ahead and trying to be
17 rocket scientists and come up with technologies -- and
18 obviously there are people doing it. There are people
19 fingerprinting browsers. There are actors around that
20 edge who are seeking to do so.

21 So, it's one thing, I think, to say, well, yeah,
22 if you're able to, if you're somehow managing to
23 accomplish this or you create a great likelihood or
24 you're going to publicly expose it, you know, in the
25 Netflix circumstance where there's, you know, reason to

1 say, well, wait a second, there is some risk or some
2 issue created, but if everyone falls under, you know,
3 the rule because of what is theoretically possible, I
4 think it really breaks the practical process.

5 So, bring that over to the IP address for a
6 second. Look, I mean, I think -- you can look at IP
7 address a number of ways. I don't know that anybody
8 would argue that if someone is using an IP address to
9 get your name and, you know, have it available next to
10 it, just using it as a substitute, you know, identifier
11 to hand around, that it isn't, you know, directly
12 linked, but in the reality of most circumstances, right,
13 it is either an item that with law enforcement or with
14 perhaps cooperation is sometimes -- maybe even often --
15 linkable to a person. So, I think let's take that over
16 there for a second and try and figure out, you know,
17 whether or not people are using it in a way that links
18 it to a person and pulls it into that category.

19 I think the second piece about it is it might be
20 a way that you can maintain state with users. So, it
21 might be kind of a really good cookie, right? It
22 frankly isn't as good as a cookie yet or you would find
23 most people using it. The industry is still using
24 cookies, A, because their technology is set up to do
25 that, and second, despite the messy frailty of the

1 cookie, it still is a bit more stable, it appears, and I
2 checked because one assumes with the increasing
3 stability of IP addresses and IP fixes and so forth, but
4 yet the most recent research, which isn't that fresh,
5 that I saw still shows that the average user can have,
6 you know, 10 or 12 IP addresses for whatever reason in a
7 month, and cookies end up being a little bit more stable
8 than that, although, frankly, probably not very reliably
9 good for more than another month, so as a tracking
10 device.

11 And then I think the third cut to think about
12 when you talk about IP addresses is does it allow that
13 correlation of non-PII, given that in the hands of some
14 folks, they do have a name behind it, and just like we
15 described the situation of a user coming to a site, you
16 know, registering, and the appended data being put over
17 on the cookie but no identification, clearly by working
18 with parties who have access, it can be a corrolator of
19 appended data.

20 So, I think when we look at these aspects of it,
21 you know, it fits in those buckets just because it has
22 this, you know, IP/IP. We spend so much time, I think
23 we ought to take a look at, you know, how is it being
24 used, how is it possibly, you know, going to be used in
25 practice, and then do these things fit into any of the

1 rules? I'd argue it's hard to easily fit it into the
2 rules unless you're doing the more explicit PII and
3 linking things to it.

4 MS. RICH: Heidi?

5 MS. SALOW: Gosh, I have so many things, I'll
6 try to cut it down.

7 So, going back to what Paul said, I don't know
8 if I agree that the IP address is -- I don't know the
9 word he used, but pervasively, you know, shared in the
10 way --

11 MS. RICH: Promiscuous.

12 MS. SALOW: Thank you -- promiscuously shared in
13 the way that you describe.

14 MR. OHM: I just meant between computer and
15 website. I didn't mean among website.

16 MS. SALOW: Okay.

17 MR. OHM: No that you're giving it on every
18 single packet.

19 MS. SALOW: So, I think there's a perception
20 that that's happening, but I don't think it is from what
21 I know. So, that's one point.

22 The other point -- two other points: I'll go
23 back to what I said before, which is -- I'm too much of
24 a lawyer, I guess, but I keep looking at this
25 definition, and I do think that what we're

1 contemplating -- I agree that an IP address, when
2 combined with other information, can make it personally
3 identifiable. I mean, I think it would be really hard
4 to argue otherwise. You can certainly attach a computer
5 to a person, okay? And I think this definition is broad
6 enough to encompass that.

7 It says a persistent identifier, and especially
8 when we're talking about iPB6, okay? And then it says
9 "such as." Well, the "such as" is just an example,
10 right? It's -- so -- and then if you combine that with
11 (g), and then if you look at the statute which gives the
12 FTC authority to expand, I think you can still stay
13 within the confines of this idea that it needs to be
14 linked, because what I get concerned about -- and I know
15 a lot of companies are concerned about -- is if you
16 start calling an IP address, in and of itself,
17 personally identifiable, the ramifications are going to
18 be huge, and it goes well beyond COPPA, well beyond.

19 I just -- it's really important to think about
20 that. It's going to have huge implications for COPPA.
21 For example, if you want to talk about real world
22 examples, what that would mean is that the second that a
23 child goes to a website, the second they go there and
24 look at content, if the server is automatically
25 collecting the IP address, which is a normal function,

1 okay, of servers, at that point, does that mean that the
2 site has already started collecting personal information
3 and has to then obtain verifiable parental consent?

4 What if the child is just, you know, browsing?
5 What if the child, you know, does not intend to go on a
6 blog or chat room or any of the above and they're just
7 looking at, you know, a picture or a game or, you know,
8 whatever, educational content, free content? There's a
9 ton of these sites out there. I'm telling -- and I've
10 polled people, and it will shut those sites down. It's
11 going to shut down the mom and pop sites. It's going to
12 shot down the not-for-profit educational sites if they
13 suddenly have to start worrying about COPPA when they
14 have never had to worry about it.

15 So, I just -- I really want to make sure that we
16 are -- you know, we can talk about sort of black letter
17 law, which is one thing, and we can debate about whether
18 an IP address, in and of itself, is black letter law PI,
19 but then, of course, we do have to talk about -- let's
20 talk about what that means in the context of not only
21 this set of rules, but in the context of other privacy
22 laws as well that could potentially be expanded down the
23 road.

24 MS. RICH: Well, relevant to your point, you
25 know, it's clear that everyone thinks when it's -- when

1 there's linking, it's frankly already covered and should
2 be covered, but what about -- is there some sort of
3 distinction -- and this is relevant to your point --
4 beyond linking about use?

5 I mean, Jules was suggesting that there's a use
6 component here that changes its nature. So, the
7 difference between the automatic transmission that
8 happens and retention, the use, the sharing. Is there
9 something around that that could make an IP address a
10 reasonable item for this list?

11 Anyone? Maureen?

12 MS. SALOW: Collection versus the use, yes.
13 Sorry, go ahead.

14 MS. RICH: Maureen?

15 MS. COONEY: Thank you. I think you hit exactly
16 on the point that we're concerned about as a safe
17 harbor, and I think probably the other safe harbors
18 would share that same concern, but as Jules, I think,
19 did a lovely job explaining, it is the linkability, but
20 it is the use. How do you do or design a compliance
21 program that keeps people attentive to what the purpose
22 of the statute was, which is to protect a very
23 vulnerable class, children, and really protect their
24 privacy? And it is about, you know, how that
25 information is used.

1 So, where's that IP address get you? What other
2 information is linked to it? And is the notice being
3 given in a vibrant enough way to tell the parent exactly
4 what is happening with that distinct identifier?

5 I think we looked at IP address and didn't
6 initially think that that should necessarily be
7 included, you know, as a rote or a default PII
8 identifier, because still, while you can attach it to
9 some individual children, there may be other members of
10 the family that are being -- so, if it's for behavioral
11 advertising that that IP address is facilitating
12 marketing, you know, to a particular IP address, it
13 isn't necessarily a particular child. It could be other
14 members of the family. It could be other children.

15 So, I think we -- you know, it is a matter, as
16 Paul said, of seeing how sophisticated are we as the
17 technologies evolve? What can we monitor? That's what
18 we look at. Can we monitor what the use is attached to
19 that IP address?

20 MS. RICH: Okay. So, we need to move on to
21 behavioral advertising, but I think we would be
22 particularly interested in comments on IP address and
23 how one could get at a standard -- you know, if people
24 think that's a good idea, that somehow links up to use,
25 that doesn't just say, "Trust me," you know, because it

1 has to be something that can be objectively measured and
2 doesn't just have the FTC and parents relying on how the
3 company decides to use the information, because that's
4 not protective enough. So, let's move on to behavioral
5 advertising.

6 So, behavioral advertising is an example of IP
7 address plus, and the question is, is data that may not
8 be personally identifiable in the traditional sense but
9 is used to target ads, would that be covered by COPPA?

10 And, Jules? Kathryn? Anyone else?

11 MS. MONTGOMERY: I'll jump in.

12 MS. RICH: I thought you would.

13 MS. MONTGOMERY: Okay. I would say yes. I
14 mean, my immediate response is the very nature of
15 behavioral advertising, and certainly the direction it
16 is taking toward personalized advertising, and if you
17 look and monitor the literature in the industry, this is
18 how the marketers are promoting what they're able to do
19 to deliver communications and establish relationships
20 with individual consumers. To the extent that that's
21 happening with children under the age of 13, I would
22 argue it fits under COPPA.

23 And I think, again, one of the problems for --
24 especially, I think, with behavioral advertising,
25 behavioral targeting, is that there really is not

1 sufficient transparency as to what's going on. You
2 know, it's not something that parents are necessarily
3 going to be able to tell, and I'm not even certain how
4 the FTC monitors this kind of thing, because it -- you
5 really do sort of have to trust that you are being told
6 what's actually happening, because where I'm finding
7 most of the information is from all of the other
8 literature in the field that describes what goes on in
9 many of these places, as well as promotional materials
10 for specific websites and content areas designed for
11 children.

12 MS. RICH: Jules, is the targeting of an ad
13 contacting a specific individual and can it be
14 correlated with other data, which is your other test?

15 MS. POLONETSKY: So, look, I mean, I think that
16 there's a problem that everyone wants to solve, and
17 whether squeezing it into the, you know, COPPA framework
18 is the best way to do it, I agree with Kathryn that we
19 shouldn't have, you know, kids being tailored with ads
20 that are going to be persuasive to them based on the
21 previous websites that they've been to.

22 Generally, that's not happening in the industry,
23 with the caveat that very often -- well, in ten years of
24 my experience, I've come across a couple -- and usually,
25 the reason it was there wasn't because somebody was

1 intentionally looking to create a -- you know, a profile
2 of, you know, here's this 6-year-old's surfing habits,
3 he'll click and he'll buy stuff. That's just not an
4 appealing audience, and at least most sites kind of got
5 the sense that tykes -- you know, junior ought not to be
6 there.

7 But what ends up happening often is you do a
8 deal with an ad network and you put in your 32 sites, as
9 one being bulk, and nobody says, "Oh, it's nonpersonal,
10 so nobody is going to talk about, you know, kids'
11 privacy." And so this small underage site ends up being
12 lumped in because the ad network doesn't have a way to
13 serve ads and not take the data.

14 So, over the years I have certainly seen, you
15 know, sites just inadvertently or because nobody had the
16 interest or capability of carving it out, throwing in
17 kids' sites, but generally, there isn't a big market --
18 in most of the leading ad networks, you can't go in and
19 buy the underage audience.

20 Where there's obviously gray around the edges is
21 that tween audience where there isn't clear personal
22 information being collected. The only information they
23 have about the age ranges are the services or, you know,
24 based on their marketing information. They've got some
25 big chunk of parents, and boom, there's a site in there,

1 and there are obviously some kids. And, again, they are
2 not collecting personal information, how you would
3 appropriately carve out the necessary audiences.

4 And so I think this is an area where, you know,
5 industry, when it did, I think, a fairly reasonable job
6 at putting together the behavioral advertising self-reg
7 rules, didn't nail it, because on the kids-related
8 marketing piece, they kind of stopped with, well, if
9 it's covered by COPPA, good, and if it's not, it's not,
10 when the reality is most folks aren't doing it. They
11 could have and should have taken off the table treating,
12 you know, a site that has a large audience of kids as a
13 profile that ought not to be created, just like other
14 sensitive information was excluded.

15 And so I think that would be an easy win for
16 kind of the industry to do, for the kind of marketing
17 practices to kind of get to. I don't see how, you know,
18 it fits easily into the COPPA bucket. It's just a
19 marketing thing that easily should stop. Most people
20 aren't doing it. It just ends up being, you know, let's
21 debate the tween piece, where I think there's
22 disagreement, or the teen piece, where I think Kathryn
23 and others have said, "Well, I don't even want them
24 advertising to teens." So that's where there's a
25 debate. There ought not to be a huge debate, but yet

1 it's not off the table technically under anybody's, you
2 know, practices, so...

3 MS. RICH: Well, why doesn't it fit into COPPA?
4 First, does it enable you to contact a specific
5 individual and does it satisfy the goals of COPPA? So,
6 we've talked about the goals all day, which is to give
7 parents more control, to protect kids, and, you know, to
8 reduce information collection from kids. I mean, would
9 covering this targeted advertising serve those goals?

10 MR. GALLIGAN: So that the question I think that
11 was originally posted was, does this constitute contact?
12 So, is simply delivering an ad to a child, knowingly
13 delivering an ad to a child, constituting contact? And
14 specifically as it relates to behavior, I think part of
15 what was discussed earlier was the transparency as to
16 whether or not it is behavioral or contextual
17 advertising.

18 And, you know, contextual advertising is no
19 different than a marketer wanting to advertise on
20 Disney, you know, so I know exactly who the audience is.
21 I know that when I'm getting ready for putting an ad buy
22 out and I want to do an ad buy on Sunday morning
23 cartoons, I know exactly who I am marketing to. And if
24 I am doing the same thing on a website, I am
25 specifically targeting a specific group of individuals

1 based on the context.

2 Now, understanding that, how do you define the
3 differences between the kinds of ads that are delivered
4 based on behavior versus context? Because presumably
5 they may be the same thing. And then as an outside
6 party, how do I determine whether or not that was
7 through behavior or context?

8 So, as a website serving up those ads, does the
9 responsibility lie that if I am providing contextual
10 ads, that I'm not contacting an individual, but if I'm
11 targeting those ads, that I am contacting an individual?
12 And actually, I think the line is so blurred there that
13 to define serving an advertisement as contact, that is a
14 disingenuous thing.

15 MS. RICH: Well, except that there may be a
16 difference in what's collected from kids.

17 MS. SALOW: And that's what I was actually going
18 to say. I was going to say, to add to what both of you
19 are saying, there's a distinction between contextual and
20 behavioral, right, so we can make a line there.
21 Contextual I think of as being sort of like a push
22 versus a pull, right? So, you're pushing out content to
23 everybody equally, just like you said, based on where
24 they are, what website the computer is visiting at that
25 particular moment. Pull is you are -- I think you can

1 make a distinction, are you pulling personal
2 information, however you define that, to determine what
3 ad gets delivered?

4 In my mind, I think that does very clearly
5 already fall under COPPA. I think that that's
6 already or should already be governed by the COPPA
7 rules, because you're collecting the personal
8 information from a child. Again, then we get into the
9 actual knowledge standard, but you know it's a child,
10 and then you decide to send an ad. Why wouldn't that
11 already be covered by COPPA?

12 I think where it gets much grayer is the
13 contextual advertising scenario where you're not pulling
14 personal information from the child.

15 MS. RICH: Let me just ask Maureen, who's
16 probably addressed this in her self-regulatory
17 standards, to comment on this.

18 MS. COONEY: We think it could already be
19 covered by COPPA, not just under (f), which is what
20 we've been talking about, but under (g), which is so
21 broad, you know, information concerning the child or the
22 parents that's collected. So, I think it could be
23 there.

24 In the area of behavioral advertising versus
25 contextual, I think we find in programs that we're

1 developing around behavioral advertising that there are
2 ways of monitoring, you know, whether or not advertising
3 was delivered in a behavioral targeted means rather than
4 contextually, and there may be additional ways that
5 industry will be adopting, through meta data taking and
6 other mechanisms, that programs like ours and others
7 will be able to monitor. So, we think it's important.

8 And then to the underlying issue of what's the
9 impact on a child, you know, the fact that profiles can
10 be built about children, delivered to them at a young
11 age, and then built upon as they're maturing, is that
12 fair? Isn't that fair? What does it -- I mean, how
13 does that impact them? We think that's very important
14 privacy-sensitive information that should be protected
15 and can be under COPPA.

16 MS. POLONETSKY: So let me just note, though,
17 that it's not necessarily a behavioral distinction that
18 we're kind of really talking about as well, right?
19 Behavioral is where and how I come up with the
20 assumption that this is a kid. So, that could be
21 because I'm at this kids' site or I've been at many
22 kids' sites, or it could be because I registered
23 somewhere else and, you know, this fact is now appended.

24 What we're really talking about is the cookie,
25 the IP, the identifier. Once we've decided this is a

1 kid and we've attached it to this identifier, this
2 identifier is something that now can be presented when
3 the user shows up in lots of other places, where they
4 don't necessarily present their name, and so I think,
5 you know, that's kind of the real question.

6 You know, the reason contextual is different is
7 because I'm not in any way doing anything about a
8 specific, you know, user. I'm saying "Put this here" as
9 opposed to "I can reach you and continue to market to
10 you as you go elsewhere," right?

11 MS. MONTGOMERY: Right, and retarget you and
12 tailor the advertising to you as a specific child, and
13 that's precisely the kind of thing we're concerned
14 about.

15 As to the monitoring issue, I am glad that you
16 are monitoring. I would hope that this information
17 could be made widely available. I know you can't always
18 do that, some of it's proprietary, but, you know, I
19 don't have a whole lot of confidence sometimes when I'm
20 just looking at a website and a privacy policy that the
21 marketer is engaging in practices that are completely
22 free and clear of, you know, of COPPA. So, I mean, I'm
23 glad you guys are around that. That's, I think, one of
24 the really good things about COPPA, is the safe harbor
25 provision and the combination of the government

1 regulation and the self-regulation and the education
2 that has to go on.

3 I don't see why we can't -- it seems to me
4 behavioral -- I'll get back to it again. Behavioral
5 targeting is included. I don't believe it's being done
6 in a widespread way -- you're right, Jules, I think
7 that's true -- with kids under 13, but I don't see why
8 it can't be clarified at this point in the rules and
9 just, you know, have us reach an understanding.

10 There are some areas that we're talking about
11 now where you'll have to kind of spell out when it
12 applies and when it doesn't, but I just think it's a
13 really important -- if there's one important message I
14 would like to make today, it's that these kinds of
15 business practices need to be effectively addressed by
16 the current law that we have on the books.

17 MS. RICH: Okay. So, let me take this one
18 question, then we are going to move on to aggregation.

19 UNIDENTIFIED SPEAKER: It feels like we're
20 putting the cart before the horse a little bit here,
21 because we haven't really -- you know, as the FTC has
22 addressed on a number of occasions, we haven't really
23 come to a conclusion about behavioral advertising in
24 toto and how it's going to be regulated and how it's
25 going to be governed, and in the absence of that

1 overarching framework, it seems kind of premature to
2 say, "Okay, we think behavioral advertising is an issue,
3 let's address it under COPPA," when we haven't looked at
4 how it's going to be addressed overall.

5 If we look at how it's going to be addressed
6 overall, then we can look at that and say, "Is there
7 something about that overarching framework that is
8 insufficient as it's addressed to COPPA but not the
9 other way around?"

10 MS. RICH: Your point is well taken, except that
11 here we're dealing with a statute and a congressional
12 intent, whereas in the behavioral advertising context,
13 it is still policy work that we're encouraging
14 self-regulation. So, there is a distinction there, but
15 I understand the relationship.

16 Sheila wanted to make one quick comment, and
17 then we need to move on.

18 MS. MILLAR: Yeah. I think when we talk about
19 online behavioral advertising, it's important to make
20 not only the distinction with contextual advertising,
21 but the underlying concept of OBA is across unaffiliated
22 websites, and I think there is a vast difference between
23 information collection practices by what we call
24 first-party website and those unaffiliated websites or
25 ad networks that are serving targeted advertising.

1 So, I think when we think about the framework of
2 the statute, we not only have to think about,
3 definitionally, whether it's an IP address or linked
4 information, aggregated information, and whether it fits
5 under (f) or (g). I tend to agree with Maureen, I think
6 it's more likely under (g). But we need to keep these
7 distinctions between the entities involved, because
8 depending on how we define these issues, I think a
9 number of us have said we're going to break the
10 Internet. We don't want to do that.

11 We need to find what we agree on, what's
12 potentially harmful to kids, what's appropriate business
13 practices, in order to maintain a vibrant Internet, and
14 then figure out how to manage it in a rules setting
15 within the framework of the statute.

16 MS. ROSENTHAL: Okay. I think we're going to
17 move on to what I like to call the Paul Ohm section of
18 the panel.

19 MS. RICH: But others can talk.

20 MS. ROSENTHAL: No, just kidding.

21 So, we talked a little bit before about the
22 aggregation of allegedly anonymous data, and here we're
23 talking about data points that in and of themselves are
24 not identifiers, are not -- what was the term we used
25 previously? -- exclusive -- what was your term, Matt?

1 MS. RICH: Exclusive.

2 MS. ROSENTHAL: Just exclusive identifiers,
3 okay, but that together, when combined, could identify
4 an individual. And, you know, Jessica talked a little
5 bit about Netflix as an example, and there has been
6 concern in the past about AOL, when they released data
7 that, you know, each data point in and of itself was not
8 identifiable, but together they were.

9 So, I want to make a quick distinction. In the
10 behavioral advertising report that Jessica mentioned
11 earlier, we did away with the PII versus non-PII
12 distinction, and we said "data that reasonably could be
13 associated with a particular consumer." Here, in Part
14 (f), we have the word "permit." And so the question is,
15 is that different? Is there a different threshold here?
16 Because "permit" means to make possible.

17 Paul?

18 MR. OHM: Yeah. So, "permit" is a fascinating
19 word, and I think we should spend a little time on it.
20 I wanted to start by clarifying a point, for those of
21 you who haven't encountered all this research, that I
22 think is really critical, which is Jules used the phrase
23 "rocket science," and what we are learning is this is
24 anything but. And so what I think astounds me most
25 about the research coming out of computer science is

1 every time a supposedly "anonymized" database is
2 reidentified, experts -- I don't mean casual
3 observers -- experts in the field seem surprised by how
4 quickly it's done, how cheaply it's done, with what
5 rudimentary tools and techniques, the slowness of the
6 computers that are used, so that Tonia Sweeney, who had
7 a landmark study, used VISUAL BASIC, I think, which if
8 you know anything about coding, is cause for derision.
9 We are not talking about rocket science.

10 And more to the point, I think that over the
11 next five years, we're going to see that this trend
12 accelerates, that as computers get faster, outside
13 information gets richer, and what we have to understand,
14 it's all about the outside information, that we're going
15 to slowly but surely recalibrate our intuitions and
16 we're going to slowly but surely just lose the faith
17 that we have in "anonymization" today, okay?

18 So, what does this mean? This means that in
19 today's conversation that we're having on the panel, I
20 think we keep really bouncing back and forth between two
21 questions, which are very different. Question one is,
22 does the FTC have power underneath the definition in (f)
23 to extend the regulations to things like IP addresses?
24 And I think unequivocally the answer to that is yes. I
25 absolutely think it is. And you will have an amicus

1 brief written by me and my students when this gets
2 litigated someday in federal court.

3 But if the question is "should" we include
4 things like IP addresses, then I'm right on board with
5 Jules and Heidi and everyone else who's talked. You
6 know, it's the classic, with great power comes great
7 responsibility mean, right? So, the idea here I think
8 is it's a really dangerous thing to tell a federal
9 regulator, which is, "You now have the power of God.
10 Any piece of information out there that you want to deem
11 suddenly within this regulation, you have a very
12 colorable argument, based on lots of recent computer
13 science, that you have the power to do it."

14 And so then it gets to questions like, well,
15 then, should you and how are you going to break the
16 Internet? So, Heidi's point was we can't include IP
17 addresses in the list, because then every website will
18 be covered, but of course not, because we still have the
19 knowledge requirement, right?

20 MS. SALOW: Yeah, but that's a whole other --

21 MR. OHM: Which doesn't have to turn necessarily
22 on how we define personal information, at least as I
23 read the statute. So, we can have an expansive
24 definition of personal information and interpretation of
25 the knowledge requirement that still excludes --

1 MS. SALOW: But they tie together, correct? I
2 mean, they tie together.

3 MR. OHM: Not necessarily. Look at the
4 language. I'm not sure they are tied together.

5 MS. MILLAR: I think the task is that if, for
6 certain policy reasons, we want to expand the definition
7 and that there is a, for the sake of argument, a legal,
8 colorable basis to do that, then I think the response
9 is, does it make sense? Should there be exclusions?
10 And let me give you one good example.

11 You collect, as many of us have noted, IP
12 addresses. They're immediately logged when the visitor
13 hits the page, regardless of who that visitor is. Now,
14 for many kids' sites, their sites are structured to
15 following the COPPA FAQs and the guidance of CARU and
16 others to promote an anonymous experience. So, many,
17 many children's websites will allow that child to
18 participate by signing in with a user name and password.

19 If suddenly those items are personal
20 information, plus the IP address, you undercut this
21 assumption of how you provide a pretty anonymous
22 experience to a child and you force the websites to turn
23 to a more privacy-invasive model, perhaps, because you
24 have to collect more personal information.

25 The IP address alone will not allow that website

1 to contact the parent to get parental consent, and so
2 you have to really think through, with all of the
3 elements of the statute and the regulations, how would
4 such a universe look if we redefine these terms in a
5 different way? And then how do you practically offer
6 appropriate content intended for kids and get meaningful
7 parental consent?

8 I would say that an IP address, user name, and
9 password won't allow you to do that, and if you define
10 that as personal information, you then would force the
11 website operator into a different data collection
12 construct.

13 MS. ROSENTHAL: Okay. So, Sheila, you're
14 offering an example where the website is not -- you
15 know, they're getting this information, they're not
16 using it, they're promoting anonymity on the site.

17 What about an example where the website has
18 access to a large database or is appending data? Should
19 there be a difference if the website is actually getting
20 information elsewhere?

21 MR. OHM: So, let me just summarize really
22 quickly, and I think this is responsive to your
23 question. I think our conversation should be about
24 policy and not power. I think the question of power is
25 actually one where you've got angels on your side,

1 because of the way computer science has been evolving,
2 and so the question is what are our guiding principles
3 that -- because I don't think anyone's making the
4 argument -- and I'm not an admin law expert -- that you
5 need to regulate anything that could colorably be called
6 personal information. I think the FTC is free to make
7 choices based on lots of policy.

8 So, I've heard lots of different policy
9 proposals thrown out. So, Jules said, "are you actively
10 reidentifying?" That's a wonderful principle on which
11 to build the rule. The second is, you know, think about
12 the policies behind COPPA. Why are we having this? So,
13 let me add one more to the mix. Quantity. So, the one
14 thing I would say is the research has suggested that the
15 more data you warehouse, the easier it's going to be to
16 do the kind of reidentification I'm talking about. And
17 so, and I might even write a comment to this respect in
18 this proceeding.

19 I would argue that once you get past a certain
20 amount of data living somewhere in your company, and
21 then you have actual knowledge that you're reaching out
22 to children, yeah, you probably fall within COPPA. You
23 probably should fall within COPPA. Let me be clear.

24 MS. POLONETSKY: And to stay at a policy level
25 for a second, you know, we don't really have an identity

1 -- you know, a parental verification access and methods,
2 but what we're really sort of doing here is we're saying
3 that there is this kind of identity that's out there
4 that can be, you know, achieved, that other people can
5 create about you, and just one thinks that if we want a
6 solution here, whether we would maybe push the focus
7 more towards how do we advance the identity solutions
8 that come along with the full package?

9 And obviously they come with the privacy
10 challenges, but they also come with the, you know,
11 solution instead of sort of deeming identity to have
12 been created. I think until recently it probably just
13 wasn't really ripe, but when you take a look at, you
14 know, Facebook as a social media layer kind of -- where
15 people kind of got some use or websites thought it was
16 useful, boom, hundreds of thousands of sites kind of
17 adopting the various tools; the Government making
18 progress with, you know, access to various government
19 services.

20 We're probably at a more ripe time today, and
21 maybe the NTIA task force will come out, you know, with
22 some progress and there are the companies throughout the
23 room here from MakeSure and Privo and others, and if we
24 start looking at them not solely as verification but as
25 ways to solve identity, that's obviously the most

1 attractive privacy solution that could come along.

2 MS. MILLAR: And I think retention also has a
3 role when you're talking about aggregated data. Some of
4 these issues potentially could be solved by limited
5 retention as well. And so the question, again, from a
6 policy standpoint is, what is the problem that we're
7 trying to solve? What are the benefits that kids have
8 from accessing the Internet? How do we address this
9 potential, but according to Jules and others, apparently
10 not reality of a lot of data aggregation and online
11 behavioral advertising targeted to teens?

12 But we want to be proactive in trying to
13 anticipate, how do we address issues that might affect
14 children's privacy? And I think we're all here to try
15 to solve some of those issues and be creative about
16 looking at ways to do that, and it may be that, you
17 know, retention and other approaches would be one way to
18 look at the issue and solve the problem.

19 MS. MONTGOMERY: Can I just respond?

20 MS. ROSENTHAL: You can respond, then we are
21 going to get to one more question and move on.

22 MS. MONTGOMERY: Okay. Well, I think these are
23 all really important questions, and it isn't a black and
24 white issue, but I do think what it suggests to me is
25 that we need more information on what the actual

1 practices are, and we need independent information. And
2 I would hope that there would be some way that the FTC
3 could do an audit.

4 I mean, one of the most useful things -- and not
5 just an audit of what you can see on the website, but an
6 audit that looks really at what the contemporary
7 practices are and what the best practices are. One of
8 the most useful things that led to COPPA was the study
9 that David Vladeck talked about earlier today that the
10 FTC did. So, I think we're talking somewhat
11 hypothetically here, and it would be really useful if we
12 could have more information.

13 And I also just want to say that I agree that
14 there is a need to be able to create an accessible
15 experience for kids online. It's a terrific tool. I
16 want them to be able to go online and have a
17 personalized experience, but to do it in a way where
18 they're not being targeted with personalized advertising
19 and to do it in a way where the minimum amount of data
20 are collected.

21 So, those are the goals, you know, and I think
22 there are ways to do it, but we do need to take into
23 account what the current capabilities are with the
24 contemporary business models and make sure they're
25 covered.

1 MS. ROSENTHAL: All right. So, I wanted to get
2 to one more question sort of in this category before we
3 move on to geolocation, which I know Matt is itching to
4 talk about.

5 Part (g) of the rule says, "Information
6 concerning the child or the parents of that child that
7 the website collects online from the child and combines
8 with an identifier described in this definition."

9 So, Maureen, you mentioned earlier that
10 behavioral advertising might actually fit under (g). If
11 there's no specific identifier involved, how would that
12 fit under (g)? You know, does (g) contemplate that type
13 of information?

14 MS. COONEY: So, I think we would look at that
15 in a couple of ways. One is the identifier may in some
16 cases be an IP address or it may be a cookie that's been
17 dropped, but what we would be looking at -- and, in
18 fact, so far we've been talking about pretty
19 sophisticated collection from children online, and
20 they're not really, you know, the types of experiences
21 that we're seeing at TRUSTe in our COPPA program, but
22 what we are seeing are some types of information about
23 children's interests that are so vibrant in the ways
24 that they're doing them now, through videos, where
25 there's no name attached to a picture but plenty of

1 other identifying information, including not necessarily
2 what we talk about as geolocation, but basic address
3 kinds of identifiers that you could pick up a lot of
4 information about children's interests through photos
5 that are being put on services or through videos. Those
6 are the two main areas that our clients are dealing
7 with.

8 And then from those interests, it would be
9 possible to do some targeted advertising, but that's not
10 what we're seeing as the present-day issue. It's safety
11 concerns for children and really reputational risks,
12 about building a profile, about their interests, that
13 they're a little bit naive and putting information out
14 there that, you know, may not be appropriate if it were
15 tracked.

16 MS. ROSENTHAL: Okay. I am going to move on to
17 geolocation, and I think it would be helpful to sort of
18 note that we're starting with the premise that what's
19 already covered is part (b). So, a home or other
20 physical address, including street name and name of a
21 city or a town.

22 So, the big picture question is whether that
23 language is adequate, given current business models, or
24 whether we need to move beyond that. So, Matt, maybe
25 you can talk about what geolocation means.

1 MR. GALLIGAN: Sure. So, you know, I'll first
2 start off to answer that question. It absolutely is not
3 adequate in the current language. If I were to give
4 anybody in the room my current coordinates, which would
5 be, you know, whatever, negative 37.0 -- blank and then,
6 you know, 105-blank, that would mean absolutely nothing
7 to anybody in this room, you know, and it, on face
8 value, means absolutely nothing. Sure, you might be
9 able to plug it into Google Maps or any of these other
10 services, but at face value, it means nothing.

11 However, you can take that and make a much more
12 accurate reading of where something has happened, an
13 event, you know, a physical address of where somebody is
14 standing. Under the current ruling or under the current
15 rule, it says, "a home or other physical address,
16 including street name, name of city or town," which
17 means that coordinate is not defined in that rule.

18 Now, I can correlate the coordinate to come up
19 with that but the coordinate itself is not specifically
20 called out in that rule. Coordinate may or may not be
21 able to be included in (b), because the information that
22 you get from the coordinate is derivative. So, it's not
23 necessarily identifying at face value, but as soon as I
24 plug it into a service that can identify that, then I
25 get some information back about the street name, you

1 know, city, town, things like that.

2 MS. ROSENTHAL: Okay. So, how specific should
3 geolocation be in order to trigger COPPA, if we were to
4 say geolocation is personal information?

5 MR. GALLIGAN: You know, I think that it
6 actually falls under the (f) or the (g), and I'm not --
7 probably the (g), or at least somewhat falls under that.
8 I don't know if the language itself needs to be
9 specifically called out, but on its own, it would need
10 to be combined with any of this other information for it
11 to become effective, because, you know, for instance, an
12 iPhone, as soon as you open the camera app for the very
13 first time, it says, "Would you like to allow this app
14 to use location?" And you never see that prompt ever
15 again, and every single picture that's then taken with
16 that iPhone stores the meta data of where that picture
17 was taken. And on its own, each one of those
18 coordinates may be an identifier of where somebody is,
19 but it's ethereal. It's where they were at that given
20 time.

21 Now, if you have enough information collected --
22 and this goes back to aggregate knowledge. If you have
23 enough information collected and you can start seeing
24 trends about where that person is, you might see two
25 locations, which might be school or work and home, and

1 you might see those things happening over and over and
2 over again.

3 Now, I think that it absolutely goes back to
4 aggregate knowledge, that with all of that information
5 put together, then you can start to build a profile
6 about somebody, but without any one of these other
7 identifiers, I don't think that it is an exclusive
8 identifier.

9 MS. ROSENTHAL: So, Jules, should geolocation be
10 included in the definition of personal information and,
11 if so, what would that look like?

12 MS. POLONETSKY: So, maybe let me again cop out
13 by saying, what should the question be, right? So, if
14 there's precise geoinformation that, frankly, acts as a
15 substitute for home address, if I actually have a
16 coordinate that can identify that precisely, that, you
17 know, this is the user's home address, how is it not
18 different than that user's home address, whether or not
19 you have got to go look it up or not? It's just a coded
20 term for a particular address.

21 I think the trickier issue is what about when
22 it's not your home address or, you know, this
23 identifying address, your place of work, your home,
24 whatever the category is that you've captured? What
25 about when it's just this body is here now? Is that

1 just another interesting data point, which, you know, is
2 no different than, okay, here's what we now know about
3 this person, and whether I have a lot of data points and
4 I know a lot about your activity, you know, it's no
5 different than, well, having lots of, you know, specific
6 marketing or interesting points, or is there something
7 about the fact that at some time we could walk over and
8 find you, because of the geo, that makes it interesting?

9 So, I think the latter example, I disagree with
10 Matt, in that in some cases it may just be a substitute
11 for a very precise coordinate that indicates your, you
12 know, permanent PII home address. In the other case, I
13 think it's a little trickier to figure out whether what
14 we -- is there a contact here? Is there -- you know,
15 what is it that we're capturing about this moving set of
16 information?

17 MS. ROSENTHAL: Okay. So, Kathryn, and then we
18 have a question from the audience.

19 MS. MONTGOMERY: I think, first of all, when we
20 talk about geolocation, generally the technology we're
21 talking about now is the mobile phone. I mean, there
22 may be others, but right now, that's, you know, what the
23 issue is. And I think you have to look at this in the
24 context of emerging practices with mobile marketing.

25 So, what can happen by having the location,

1 you're also going to know who the phone belongs to, and
2 you'll know more information by the very nature that
3 that's the device that's being used, you will know more
4 than just where that person is. You'll know that that
5 is the user of that telephone, right?

6 And then --

7 MR. GALLIGAN: Not necessarily.

8 MS. MONTGOMERY: Let me just --

9 MS. MILLAR: Not necessarily true, and you may
10 not know it's a child.

11 MS. MONTGOMERY: You'll know things about who's
12 been on that phone, too, or you might also, because you
13 might be collecting all kinds of other information about
14 how that phone is used. So, it would make it possible
15 to be able to identify when a child is near a particular
16 business, like a McDonald's, and send a coupon. And,
17 again, those are the kinds of things that we're
18 concerned about.

19 MR. GALLIGAN: So, knowing that it is a child is
20 the important component there and the phone --

21 MS. MONTGOMERY: Well, under COPPA -- under --
22 you know --

23 MR. GALLIGAN: Under COPPA, absolutely.

24 MS. MONTGOMERY: It is.

25 MR. GALLIGAN: That's what we're talking about

1 right?

2 MS. MONTGOMERY: What we're talking about today.

3 MR. GALLIGAN: So, under COPPA, you know, you
4 have to know that it's a child to have it defined in
5 that way. Now, I certainly agree with actually both of
6 you in the regard that --

7 MS. MONTGOMERY: But you just said no.

8 MS. ROSENTHAL: You said it's not true.

9 MR. GALLIGAN: I agree to the extent that the
10 targeting based on geolocation should be covered.

11 But going back to his point, which is what is
12 this distinction between home and some other point that
13 you exist, and first off, the home question, yes, you
14 can determine that a coordinate is home, but you require
15 aggregate knowledge before you can determine that that
16 is home, because it's just a number, but with enough
17 numbers that is all within a similar area, you might be
18 able to determine that that is home.

19 But another point, without any other
20 information, say, other than with what Apple considers
21 device data, they actually specifically call it out as
22 TOS. Device data is defined as IMEI, which is the
23 specific device identifier, your SIM card number, your
24 phone number, and a couple other things that Apple just
25 has available in their DI. They specifically have

1 called out in their TOS -- now, this is just Apple, it's
2 not across everybody else, and it probably could be a
3 best practice -- they specifically call out that you
4 cannot use that data to market.

5 MS. MONTGOMERY: Oh, Apple, yeah, and that could
6 be a best practice.

7 MR. GALLIGAN: It could be a best practice, but
8 it could also mean that it could be a baseline for a
9 rule. Now, I'm not a proposer of that, but I'm just
10 saying that that could potentially be that.

11 Now, I don't necessarily think that with device
12 data that you can still identify that it is a child,
13 because you also don't get access to what other apps are
14 included, are on that device; you don't know through
15 behavior necessarily, except for maybe --

16 MS. ROSENTHAL: Right, and we're assuming,
17 though, for purposes of the discussion that they know
18 that it is a child, that it's directed at a child, just
19 for this.

20 MR. GALLIGAN: Sure.

21 MS. MONTGOMERY: Because of the cross-platform
22 content networks, for example, whether it's social
23 networks or something else, you may very well know.

24 MR. GALLIGAN: Sure.

25 MS. ROSENTHAL: John, did you still have a

1 question?

2 UNIDENTIFIED SPEAKER: No. Matt eventually got
3 to it, but just to make very clear that two location
4 points really can be a unique identifier. I mean, there
5 is only one person on the earth who regularly travels
6 from my home to her high school, and that's my daughter,
7 and, you know --

8 MS. ROSENTHAL: So, if we were to include
9 geolocation in the definition of personal information,
10 should there be a requirement that it is collected over
11 time, that it's not just one piece of geolocation data,
12 that it's aggregated in some way, or can we -- you
13 know --

14 UNIDENTIFIED SPEAKER: Well, to some extent, in
15 (g), you have kind of a catch-all, but the catch-all
16 correlates back to something in (a) through (f).

17 MS. ROSENTHAL: Exactly, right.

18 UNIDENTIFIED SPEAKER: And I think the point is
19 that you can have some (g)-type data points that taken
20 with other (g)-type data points could be a unique
21 identifier, and so, I mean, you know, it gets a little
22 harder on -- I mean, all you guys have been talking
23 about, you know, can you go back to a use, you know, an
24 idea of, you know, well, how do you use the IP address
25 or how do you use these data points and do you use it as

1 a unique identifier? And that's a possible approach.

2 MS. ROSENTHAL: Heidi, you have some clients
3 that are --

4 MS. SALOW: Oh, yeah. No, I was just going to
5 say, not even just on behalf of clients, but I think to
6 assume that because it's a mobile device, that suddenly
7 you -- whoever the "you" might be, because I think
8 that's another thing. We're talking a lot sort of very
9 generally about one or you having this information. I
10 think it really depends on who are we talking about,
11 right? To assume that because a person has a mobile
12 device, the world then knows I'm the owner of this
13 mobile device, I was in the Starbucks this morning, I --
14 you know, I bought a latte, and, you know, all of --
15 that's not really the case at all.

16 And, in fact, you can't even get -- Mike will
17 know this. You can't even get a cell phone number -- I
18 can't look up a cell phone number, okay? I can't find
19 your cell phone number. You have to give it to me.
20 It's not publicly available. So, no, I don't know who
21 you are.

22 MS. ROSENTHAL: So, let me just offer -- okay,
23 so it's not about necessarily knowing who you are. If I
24 have your email address, I don't necessarily know who
25 you are, but I can contact you online, and if I have

1 your geolocation, maybe I don't know who you are, but I
2 might be able to physically contact you. So, let's just
3 make sure we phrase it that way.

4 In that case, do you think --

5 MS. SALOW: So, now I think we're going to the
6 device versus individual, right, because you're
7 contacting my device? I'm just trying to clarify.

8 MS. ROSENTHAL: Okay, yes, right.

9 MS. SALOW: You don't know that I -- I know, I
10 realize -- I don't want to be the bad guy, but I just
11 want to --

12 MS. ROSENTHAL: No, I don't mean to -- right. I
13 don't want to put you on the spot but I want to make
14 sure that we explore that.

15 MS. SALOW: Just to be practical, because I
16 think we need to really think practically speaking
17 what's happening and who are we talking about has this
18 information. The wireless carrier knows who I am,
19 because I subscribe to the service, and when I signed up
20 for the service, I told them who I am.

21 And by the way, I know we talked about this
22 earlier, Michelle, but when you go back to IP addresses,
23 an IP address alone is not going to be the only
24 mechanism by which you can identify a mobile device.
25 There's already -- this already exists. The SIM card

1 identifies the mobile device already today. Everybody
2 has a SIM card in your device that's unique. So, you
3 know, we get worried when we talk about -- and, again,
4 I'm not saying it's not something we shouldn't be
5 concerned about, but it's already identifiable.

6 But anyway, going back to that, so I think the
7 carrier knows a lot about me as a subscriber, and the
8 carrier is subject to very strict rules, both under the
9 CPNI regime and under ECPA, the Electronic
10 Communications Privacy Act, as to who that information
11 can be shared with and for what purposes. So, you know,
12 I just wanted to make sure we were talking about the --
13 who we're talking about here.

14 MS. POLONETSKY: I think there's a simpler
15 example that maybe highlights this a little easier,
16 because the mobile starts bringing in all these other
17 factors that are -- so, here's a more real world
18 example.

19 Today, I'm at a website. A website obviously
20 can geo, in a general way, because of IP address, but
21 today, many computers that don't have built-in GPS,
22 however, can download a little plug-in that relies on
23 your WIFI antenna, you know, great attention in recent
24 weeks to the kind of Google WIFI, but obviously there's
25 Skyhook, there are other companies, and WIFI networks

1 are mapped. So, do we want to say, for instance, that
2 if you're a -- what we would be saying if we extended
3 geo is that if I'm a kids' site and it said, "Here,
4 click here so that you can get your precise whatever," I
5 click here to allow us to use -- most of the browsers
6 require this on sort of an opt-in basis. Firefox
7 actually is launching a little icon that's going to let
8 you know when their next version -- IE, may do that. I
9 have to check.

10 So, do we want to say that a child's site could
11 not collect -- right, that's not collecting any other
12 explicit personal information, that it couldn't use this
13 WIFI/geo thing to precisely take the location? That's
14 kind of a clear, clean shot at this question.

15 MS. ROSENTHAL: So, do we want to say that?

16 Paul?

17 MR. OHM: So, I see why you're all COPPA
18 experts, because it's like a beautiful Matrishka doll,
19 and every time you read this, you see a different layer
20 you didn't notice before. I might become a COPPA expert
21 after this.

22 So, look at (b). First of all, (b) is not
23 restricted to homes, right? It's any physical address.
24 Aren't you intrigued by the fact that Congress did not
25 care about the street number? All you need is the name

1 and the city? So, what is this, the megaphone rule? If
2 I can drive to your street and yell an advertisement at
3 you?

4 But it does suggest to me that when you ask a
5 question about one coordinate at one moment in time, why
6 isn't that, exactly, the kind of interest that Congress
7 had in mind, right? I don't know what Congress was
8 thinking there, maybe they were worried about
9 megaphones, but again, I hate to be a broken record, I
10 don't think this is about power. I mean, Congress was
11 writing lots of blank checks here, I think this is about
12 whether is it a good idea or bad idea?

13 MS. ROSENTHAL: All right. So, let me attempt
14 to wrap up a little bit on the geolocation so we can get
15 to a couple more questions before we finish the panel.

16 Is there a way to articulate a clear standard on
17 geolocation? If we were to include it in the
18 definition, how would we do that? What would it look
19 like?

20 MS. MILLAR: Well, I think that we have talked a
21 little bit, and Paul's made a good point here, that
22 under (b), how different is precise geolocation where
23 you either have actual knowledge that you're dealing
24 with a child or on a kid-directed website or online
25 service that your kid targeted, then potentially it's

1 already covered.

2 I think the issue is whether or not there is any
3 reason to exclude it, as Paul suggested. You know, are
4 there beneficial reasons to include that sort of
5 information? Otherwise, currently, under COPPA, beyond
6 the exceptions, you're required to get parental consent,
7 and if you're getting the home address for purposes of
8 internal marketing to a child, you have the email-plus
9 option. So, maybe geolocation fits in the email-plus
10 construct; maybe it doesn't.

11 But I think that for the geolocation
12 information, if you're either kid-directed or have
13 actual knowledge -- and I think the actual knowledge is
14 the tough one, because I think in most circumstances,
15 you don't know. If somebody's going between school and
16 home, you know, dad may know that it's my daughter, but
17 service provider, assuming there's a website or an
18 online service involved, they may have no idea. They've
19 got a number and a location. So, they don't know.

20 So, again, I think you have to put the pieces
21 together to determine what's the right rule, but if you
22 have a kid-directed website or online service or
23 something with actual knowledge, I think geolocation
24 probably fits right within (b).

25 MR. GALLIGAN: I think it actually fits better

1 within (g), just because, like I said earlier,
2 exclusively, a single point does not constitute -- well,
3 I guess it says "or other physical address." I am going
4 to agree with her. It's (b).

5 MS. ROSENTHAL: Final answer? Is that your
6 final answer, Matt?

7 MR. GALLIGAN: You know, in terms of calling it
8 any other physical address, I mean, it just -- any
9 coordinate defines any other physical address.

10 MS. MONTGOMERY: I just want to make sure COPPA
11 covers mobile marketing.

12 MR. GALLIGAN: But the one thing I will say
13 about coordinate and (b) is that coordinate will likely
14 need to be spelled out.

15 MS. SALOW: I was just going to say the same
16 thing. If you do -- I don't disagree that it falls
17 within (b), but if you are going to add geolocation,
18 please make it clear.

19 MS. ROSENTHAL: Sure. We'll do that.

20 MS. POLONETSKY: And I just want to throw in the
21 complication that the wireless carrier usually knows who
22 the account holder is, not who has the phone. So, the
23 five phones in my family, I haven't told anybody who has
24 which one of them and --

25 MS. MILLAR: Well, and that gets back to the

1 fundamental point that it's directed to children or
2 actual knowledge, and if you -- I mean, I can go as a
3 small business and buy six phones and give them to my
4 employees. There is no automatic assumption that just
5 because there's multiple cell phones attached to a
6 single subscriber that there are some kids in there, and
7 even if there were, you wouldn't know how old they were,
8 because they would be minors perhaps, but they may not
9 be. So, I think we really need to keep coming back to
10 the required statutory language and understand that
11 there are some limits to what people actually know about
12 you.

13 MS. ROSENTHAL: Okay. So we're just going to
14 wrap up, because I don't want to deprive you-all of your
15 break, but we, again, urge you to submit comments on all
16 of these topics and anything else that you think we
17 should cover.

18 MS. MONTGOMERY: We didn't cover H.

19 MS. ROSENTHAL: We're back at 3:00. Thank you
20 all.

21 (Applause.)

22 (Recess.)

23 MS. KRESSES: Let's go ahead and get started on
24 the parental verification panel. So, this panel, Panel
25 Four, is kind of a COPPA specialist panel. Many of you

1 perhaps have never had the joy of considering all the
2 different methods of parental verification and, you
3 know, looking at them closely and wondering what works
4 and what doesn't, but what we'd like to do is take a
5 little bit of the panel, the start of the panel, and go
6 through the methods that have been outlined in the rule.
7 They're not exclusive. The rule was never meant to
8 confine anyone to those methods, but talk about whether
9 they're being used, how they're being used, are they
10 effective, and do they still make sense, and then move
11 into considering other potential methods and the pluses
12 and the challenges of potential new methods.

13 So, in this regard, also, you know, we really
14 would encourage audience participation and questions,
15 and we'd also encourage ideas. So, if you've been
16 thinking, "why hasn't anybody ever thought up this
17 perfect parental verification method," speak up.

18 Oh, let me introduce the panelists. Sorry.

19 To your left, we have Jules Cohen, who is the
20 Senior Trustworthy Computing Specialist with Microsoft.

21 We have Rebecca Newton, who is the Chief
22 Community and Safety Officer of Mind Candy, Inc.

23 We have Martine Neijadlik, who is the Senior
24 Director of Risk and Business Intelligence at BOKU,
25 which is a mobile payment system.

1 And then over here, we have Alan Simpson, who's
2 the Vice President of Policy for Common Sense Media.

3 And Ron Zayas, who is the Chief Executive
4 Officer of eGuardian.

5 And then Denise Tayloe, who is President of
6 Privo, Inc., which is -- has one arm of Privo, Inc.,
7 which is a COPPA safe harbor.

8 So, let's -- okay, so just to take a minute to
9 look at the verified parental consent requirement of the
10 Rule, and there is a general standard, which is
11 basically that operators must make reasonable efforts to
12 obtain verifiable parental consent, taking into
13 consideration available technology, and that
14 requirement -- the methods have to be reasonably
15 calculated, in light of that technology, to ensure that
16 the person providing consent is the parent.

17 And then on the other side of the slide are the
18 methods that are laid out in the Rule, and, again, were
19 not meant to be exclusive but were deemed to meet those
20 requirements.

21 So, here we are, however many years later, and
22 the online world has changed a lot, and there's a lot
23 more potential things out there. So, we want to look at
24 the old and see how they're working and then look at the
25 new.

1 So, let me start with Rebecca Newton, and I want
2 to start with the email-plus standard, and email-plus,
3 the Rule designated that where the collection of
4 information from a child was only for internal purposes,
5 so it was for the purposes of the website or the online
6 service, and not to be shared with third parties or to
7 be publicly disclosed, either by the website or by the
8 child, at the time the Rule was put into effect, that
9 was considered a less risky, a less disclosing method of
10 taking personal information.

11 And so the Rule carved out an exception that
12 where the information was only to be used for internal
13 purposes, that one could send an email to the parent
14 with notice, allow the parent to confirm, by email, that
15 they had received the notice and that they were
16 consenting, and then to follow that up with either
17 another email, a phone call, or a variety of other
18 options, but this was not considered an adequate method
19 for situations where personal information would be
20 disclosed publicly.

21 So, with that, Rebecca, does email-plus actually
22 meet the standard of ensuring that a person providing
23 consent is the child's parent?

24 MS. NEWTON: Well, that's a tricky question, but
25 I think as well as any of the others, it meets any of

1 the other standards. You never know that it's really a
2 parent, and I haven't done any of the science behind
3 this, but just from being in this business for 16-plus
4 years, I think that it's fair to say that a
5 percentage -- I don't know what -- I can't be accurate
6 about the percentage -- of the registrations are kids
7 using their email addresses or possibly putting in their
8 parents' email address.

9 But I do see, where I work now, a fair amount of
10 bounce-backs. These are emails that aren't legitimate,
11 that say things like mymom@herwork.com, and so, you
12 know, they want to -- I see a fair amount of that every
13 day, and so that sort of speaks to Dr. Gwenn's point
14 about they want to tell the truth. A certain percentage
15 want to do the right thing and want to tell the truth.
16 So, you know, it's as valid, I think, as any of the
17 other methods.

18 MS. KRESSES: So, in your experience, then, is
19 email-plus -- do you think it has the same assurance of
20 actually reaching a parent as the other methods in the
21 rule?

22 MS. NEWTON: I think it's as valid as the other
23 methods, yes.

24 MS. KRESSES: So, let me turn that then to Alan.
25 Do you have any experience from the parents and do you

1 have any knowledge of the effectiveness of email-plus?

2 MR. SIMPSON: Not directly, but I would echo
3 Rebecca's point, that there's a -- the standard may be a
4 little too high, recognizing that we know that kids will
5 cheat the system in some cases, but that a lot of kids
6 don't want to. I mean, the whole point of verification
7 is obviously making the best effort that we can, and
8 there is no such thing as a perfect effort.

9 We do get a fair amount of parent feedback on
10 our site around what my kids are doing that I didn't
11 know about. So, that's not a direct aspect of
12 email-plus. It's just more of a matter of the challenge
13 that all of these technologies and all of these
14 approaches will face.

15 MS. KRESSES: So, we wanted to touch on
16 email-plus first, because email-plus has had a long
17 history. It was supposed to be a very temporary
18 solution, and we extended it, because we didn't come up
19 with other technological choices that worked with the
20 same ease as email-plus, and then we ultimately, in our
21 2007 report, said that email-plus would be a permanent
22 standard for the foreseeable future.

23 And so it's interesting what you're saying,
24 Rebecca, that -- do you feel that the -- would you say
25 that email-plus, if it has the same reliability as other

1 standards, do you think that it still makes sense that
2 email-plus is limited for internal uses?

3 MS. NEWTON: I mean, I am probably going to say
4 the same thing over and over. I think it's -- yes. I
5 think it's as valid as the other methods, and I think it
6 still makes sense, unless we adapt available technology
7 and take a whole different sort of turn on this and go
8 for real parental verification as much as we possibly
9 could. Otherwise, there's no -- I mean, it's the most
10 valid thing we have, other than available technology
11 which is out there now.

12 MS. KRESSES: Let me ask a slightly different
13 question. Jules, actually, do you have any experience
14 from Microsoft on how consumers -- not just parents, but
15 computer users generally do -- how do they view the
16 distinction between internal uses and external uses?

17 MR. COHEN: No, I don't. I don't have --
18 actually, I don't have good data to suggest that they
19 think about them differently or that they think about
20 them one way or the other, but I would note that -- you
21 know, I think it's a valid distinction, because in the
22 internal case you have -- one org will hold the data,
23 and they will have stewardship mechanisms to manage the
24 data, and in the other model, where it leaves the org or
25 whatever stewardship mechanisms exist, you have much

1 looser reins on what happens with the data.

2 So, you know, as policy-makers are thinking
3 about, you know, sliding scales for different kinds of
4 risk, this distinction seems to map pretty clearly to
5 two different kinds of risk.

6 MS. KRESSES: Actually, Denise, I wanted to ask
7 you, too, from your experience with Privo whether or not
8 you -- following up on what Rebecca said about
9 email-plus and whether it's a reliable method, in your
10 experience, do you have a comment on that?

11 MS. TAYLOE: Well, I would say that I
12 respectfully disagree with Rebecca that it is as good as
13 the other methods. I don't think any of the methods are
14 perfect, as Alan just mentioned, but if the goal is to
15 use reasonable methods in light of available technology,
16 and ten years later the best we can do is send an email
17 to a parent that a child provides us and get a
18 click-back, I would say that we, industry, haven't done
19 a good job of adopting new methods, creating new
20 methods, and that people are heavily relying on it. So,
21 that's one thing.

22 The second is that if you're supposed to be
23 reasonably assured you're dealing with a parent, I would
24 say that most of the methods don't do that and that
25 email-plus in no way even allows you to say you're

1 dealing with an adult. So, you know, yes, kids have
2 credit cards, but most don't.

3 You know, other methods that are available that
4 we're going to discuss later will help to do identity
5 verification to at least know that you're dealing with
6 an adult, so you can make the leap of faith that it's
7 likely to be a parent who's asserting that child.

8 So, you know, my thought is email-plus, as an
9 industry, we need to start moving away from it and find
10 other methods, and the quickest method that I see is let
11 a parent short code a message back from their cell phone
12 and use that as the mechanism as opposed to clicking a
13 link. Let a child give a parent email. If they don't
14 have a parent email, more kids know their parents' cell
15 phones than know their parents' email address.

16 MS. KRESSES: And do you know that doing that
17 SMS-type thing would give you more assurance that it's a
18 parent or the same as email-plus or less?

19 MS. TAYLOE: I think it would give you more
20 assurance. It's not the kids -- I mean, kids absolutely
21 have cell phones, but at least there is a cell phone
22 tied to a parent somewhere in the -- or tied to an adult
23 somewhere in the path. So, you can tell whether or not
24 the short code is coming back from a Verizon or a Sprint
25 or an AT&T versus, you know, a throw-away phone.

1 MS. KRESSES: Phyllis?

2 MS. SPAETH: (Off mic.) How do you know that
3 it's coming back from the parent as opposed to the
4 child?

5 MS. TAYLOE: I would just say you have
6 absolutely no assurance with an email. You have a
7 little -- at least we're moving up the scale versus sort
8 of staying and waiting for it to be perfect.

9 MS. SPAETH: Denise, I have no quibble with you
10 about that fact, but I think email-plus is nothing.

11 MS. TAYLOE: It's a joke, and everybody knows
12 it, yeah.

13 MS. SPAETH: Everybody knows it's a joke, yeah.

14 MS. KRESSES: Was that clear?

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

19 MS. KRESSES: And let me turn to Martine.
20 Martine operates BOKU, which is a -- it's a mobile
21 payment system, so this might be sort of a loaded
22 question, but if email-plus is a sufficient method to --
23 you know, assuming for the moment that it is a
24 sufficient method to get permission for internal use,
25 should the standard for a simple method be limited to

1 email or are there other equally facilitative methods
2 besides email that would work for these purposes?

3 MS. NIEJADLIK: Hi. Let me just say a couple
4 things, I think. First of all, prior to BOKU, I was
5 actually at PayPal, and I used to manage risk detection
6 for PayPal, and when I think about laws on the Internet,
7 the first two words that come to my mind is scalability
8 and global. So, is it global and is it scalable? And
9 if we are going to have rules that apply to the Internet
10 and enforce those on these companies, now think about
11 every country also having different rules, which is
12 something we're dealing with right now. It's got to
13 encompass both of those things.

14 Now, I think email-plus -- I would agree, it is
15 not as strong as some of the other methods, but when you
16 sort of intersect practicality with safety, you know,
17 it's really one of the only ones on the list that I
18 think is a viable option for people. So, I don't know
19 if it's the appropriate time to just sort of talk about
20 mobile -- what BOKU is doing --

21 MS. KRESSES: We are going to get to that.

22 MS. NIEJADLIK: Okay.

23 MS. KRESSES: When you say mesh practicality
24 with safety, what do you mean by that?

25 MS. NIEJADLIK: I mean something that's

1 completely automated, right, where a human being is not
2 getting on the phone with a parent, is not, you know,
3 looking at a fax machine, is not -- something that does
4 not require human interaction, that's completely
5 automated.

6 MS. KRESSES: Okay. Does anybody have any
7 other -- we're just trying to touch slightly on each of
8 the existing methods so we have time to go into other
9 things. Does anybody have any other observations or
10 questions on the email-plus method, whether or not, you
11 know, it should be limited to internal uses only?
12 whether or not it works? whether or not it's time for it
13 to go, as Denise would say? Anybody have any comments?

14 Yes, Parry.

15 MS. AFTAB: I think we need to recognize the
16 practicalities of all of this, and as you know, we have
17 been in this space forever. So, as you move out of
18 email-plus -- and Denise and I, I think, will disagree
19 on this one, because it's a great way of getting parents
20 out there to do something. They're uncomfortable with
21 credit cards, and a lot of people in this country don't
22 have them, and I don't want to lock children whose
23 parents don't have credit cards off of the Internet.

24 So, they don't know what a fax is. They, you
25 know, see licking a stamp as just beyond everyone. The

1 kids are on to a new site by the time a letter arrives.
2 Unless you can find a new way of doing this, and
3 email-plus works. Right now, it works. It's easy way
4 in, easy way out. It can be automated.

5 And so when you have got 8 million, 10 million,
6 12 million users in the kids' space, it allows you to do
7 something, but we need to recognize -- it may not be
8 time to kill it. It may be time, as we start looking at
9 this, to expand it.

10 MS. KRESSES: And by that you mean what?

11 MS. AFTAB: I think as we start looking -- you
12 know, the whole sunset provision, we thought this would
13 be out there for, like, two and a half minutes, but the
14 reason it's still there is because it does something
15 none of the other ones did. So, when we move from \$45 a
16 kid to \$15 a kid to get COPPA compliance on verifiable
17 parental consent -- and parents just aren't doing it
18 unless the kids pretend to be their parents -- we need
19 to find something parents will do.

20 Parents will send an email. So, we need to find
21 maybe that there's a way to expand it so it's even
22 beyond where it is on something that's a bit more
23 verifiable.

24 MS. KRESSES: Okay. I think Gwenn has a
25 statement or question.

1 DR. O'KEEFFE: I just wanted to echo quickly
2 what Parry said. I was about to say the identical
3 thing, so I'll just truncate it really quickly.

4 As somebody who also talks to a lot of parents
5 and sees the technology gap, parents -- Denise, I agree
6 with most of what you say, but texting just won't work
7 right now with today's parents, because there is a huge
8 technological gap in this country that we just simply
9 have to embrace. We have to embrace it. We have to hug
10 it. We have to notice it. We have to name it as the
11 experts, because you know what? Parents don't text.
12 And you know why? Because they're barely on the cell
13 phone themselves.

14 We have a lot of parents in this country who
15 don't even own cell phones themselves because they can't
16 afford it or they just don't know how to use it or
17 they're intimidated by it, but they do use email. Every
18 parent in this country uses email, even the
19 unsophisticated ones. So, let's not make this into more
20 than we have to. Let's keep it simple. I do agree that
21 someday we need to go to other technologies, and I love
22 texting myself, but I'm with Parry on this one. I think
23 we need to go the email route.

24 MS. KRESSES: Okay. Let me go to Shai, and then
25 I will go to Amanda, and then I will go to you, and then

1 we will move to the next topic.

2 MR. SAMET: I am going to agree and disagree. I
3 am going to agree with Parry and I am also going to
4 disagree with Gwenn to some degree. By the way, Shai
5 Samet. I run a privacy consulting firm and have done a
6 lot of work on COPPA in the past ten years.

7 I think email-plus has served a very beneficial
8 purpose, and somewhat unrelated to what the law
9 requires, what we're finding is that many of the kid
10 friendly websites, especially those for younger kids,
11 who have designed their chat functionalities so as not
12 to allow personal information to go through, are still
13 using email-plus to notify and get parents involved with
14 the fact that their kids are using those sites, and
15 that's an extremely valuable benefit and I think one
16 that could easily carry over to SMS.

17 I'm a parent, I have four kids all under the age
18 of 13, and I use my cell phone. My mother only uses her
19 cell phone, doesn't use email at all. So, I think --
20 you know, I think we would have to look at that data
21 more closely before we determine whether or not SMS is a
22 viable mechanism. It is true that kids know their -- my
23 daughter knows my cell phone number. She does not know
24 my email address. But then again, also, the fact that
25 she doesn't know my email address usually requires her

1 to call me to the computer and say, "Hey, dad, you know,
2 what's your email address?" And through that I get
3 involved as well.

4 So there's a lot of mixed data out there and a
5 lot of opportunities here as well, but to get rid of
6 email-plus would be a very dangerous proposition,
7 especially given its benefit for those sites that are
8 using it.

9 MS. KRESSES: Okay, if we can pass the
10 microphone to Amanda.

11 MS. LENHART: I'm Amanda Lenhart from the Pew
12 Research Center, and we have done some research on how
13 teens and parents and families use mobile phones, and,
14 in fact, in many cases families are more likely to have
15 a mobile phone than a computer, and, in fact,
16 particularly with low-income families who often do not
17 have a computer at home or who have a highly shared
18 computer, but they do have mobile devices.

19 So, again, this begs the question, of course,
20 whether these kids are going to be going on websites and
21 whether -- if you don't have a computer in the home,
22 whether you actually necessarily need to be able to do
23 some of this verified parental consent, but parents are
24 actually more likely to have cell phones than other
25 adults. They are more likely to use them to text their

1 kids.

2 So, they don't always know how to text. There
3 is a substantial subset of parents, about 25 or 30
4 percent, who don't text at all, don't know how to text,
5 and so they don't use that, but a lot of parents are
6 actually drawn into texting by their children.

7 Also, parents of younger kids now are in that
8 generation of people who actually do text and actually
9 text more than older adults. So, I wouldn't totally
10 eliminate text messaging or SMS as a potential way. I
11 would add it on. I would not substitute.

12 MS. TAYLOE: It's about options. I wouldn't say
13 any one. I'm all about providing options.

14 MS. KRESSES: Okay. And do you still --

15 UNIDENTIFIED SPEAKER: Nope. She covered
16 everything.

17 MS. KRESSES: Okay. All done.

18 And way in the back? Then we'll move to
19 something else.

20 TIM SPARAPANI: I think Parry is onto something,
21 and I think we should definitely be keeping email-plus
22 as an option. Recognizing that there isn't really any
23 way of authenticating anybody online, I think we should
24 be at least exploring the possibility that lots of
25 companies, mine included, are starting to get the

1 opportunity to have multifactorial ways of making
2 educated guesses about who people are online, what their
3 ages are, what they're up to, et cetera, and it seems to
4 me that the FTC would do itself a great deal of good to
5 allow for continued exploration by companies in this
6 area, because I think you will actually find that
7 companies will have the opportunity to do more
8 verification in the future.

9 MS. MARCUS: Well, and just to kind of build on
10 what Tim has said, we do interpret the general standard
11 that you see on the slide as the baseline standard, and
12 so the methods that satisfy the rule are illustrative
13 only. They are not meant to be exclusive, and the
14 general standard does provide for the kinds of
15 exploration that you've suggested.

16 Now, it might be -- and we'll certainly talk
17 about this -- that people are too nervous to try
18 something other than that which is set forth in the
19 rule, but, you know, we have to meet this baseline
20 standard, that we have to at least try to ensure that
21 it's a parent, but it wouldn't be meant to preclude
22 exploration.

23 MS. KRESSES: It is any method reasonably
24 calculated, so it was never intended to be an exclusive,
25 you know, list. So, let me go to Peter, and then

1 let's --

2 MR. ZAYAS: Maybe if I can just interject for
3 one second, the thing I think we keep missing here is
4 that the intent is to get parental consent, and that
5 seems to be very absent from the net effect here. There
6 is no way to verify that it's a parent. There is no way
7 to verify that the kid isn't making the address up or
8 doesn't know the address or whatever the case may be.

9 I think phones are a great way to do it, but
10 nonetheless, if the intent here is to get verifiable
11 parental consent, the fact that a system works but
12 doesn't do that I think means it's not a very effective
13 system to use.

14 MS. KRESSES: Okay. Phyllis, you already had a
15 turn on this one.

16 You gave up your turn, but we'll let you go
17 anyway.

18 UNIDENTIFIED SPEAKER: I was trying to be
19 efficient. Going back to the point you just made about
20 being conservative, I advise a lot of companies in this
21 space, and I would never advise one of my clients to do
22 anything beyond what is on the list for fear that it
23 wouldn't be acceptable. I mean, because the standard
24 says to ensure that the person providing consent is the
25 child's parent, and that's the point that was just made,

1 and living up to the "ensure" is virtually impossible,
2 but it's really impossible outside of the six things
3 that are there from a legal standpoint.

4 MR. SIMPSON: Don't we all agree that the six
5 things there don't really ensure?

6 UNIDENTIFIED SPEAKER: I'm agreeing with you
7 that those don't work either, but from a liability
8 perspective for my clients, at a thousand bucks a pop,
9 I'm not going to tell them to go beyond that.

10 MS. KRESSES: Okay, let's do this: Let's move
11 on to the other existing methods up here, and we'll try
12 to go through them, you know, fairly expeditiously.

13 So, it is not a rhetorical question, but I want
14 to know if we are seeing people still using the print
15 and send method or an equivalent of that or the print
16 and scan -- yeah, we, a couple years ago, Phyllis and I
17 revised our website -- the agency's COPPA website -- to
18 say that, you know, we would recognize a scan as a
19 print-and-send, obviously in the modern world.

20 But, Denise, in your experience, is that a
21 format that is still being used and why or why not?

22 MS. TAYLOE: Okay. So, yes, some people use it.
23 If you try to use it as your sole method, you'll fail
24 miserably. If you only offer things like credit card,
25 you'll scare the bejesus out of people and they, not

1 having choice to do something less personal, is a
2 problem.

3 So, here's my experience: We offer five methods
4 as a sort of standard: last four digits of Social,
5 driver's license, credit card, print and send, whether a
6 fax or in the mail, or a phone call. And consistently,
7 we get about 7 percent that will choose phone and a
8 printed form; 82 percent that will choose last four
9 digits of Social, because it happens in nanoseconds,
10 it's automated; and then the credit card is very low, 4
11 or 5 percent; driver's license, low, because it's just
12 hard -- it's hard data to get.

13 So, I would say that I would not want it to be
14 taken off the table, because I think that if I'm looking
15 at choices and the fact that I can do something offline
16 makes me feel more comfortable maybe about choosing
17 something that's online.

18 MS. KRESSES: Okay. And just so we are all on
19 the same page, when you collect the last four digits of
20 the Social Security number, what other information do
21 you take from the parent to make that work?

22 MS. TAYLOE: So, it's up to the relying party's
23 site that uses the service what level of assurance they
24 want. The minimum data that you need in order to decide
25 whether you've got an identity is the last name and last

1 four, but typically a parent account is a first name,
2 last name, a zip code, a date of birth, and the last
3 four.

4 And then, of course, just like credit cards, the
5 last four are not retained. So, you hit the data
6 aggregator, you get data back, we pine through. If we
7 can find a match, then we process a pass, we flush the
8 last four, and we're left with a parent account that has
9 an email address associated. So, from that point
10 forward, the parent can permission off of their email.

11 MS. KRESSES: Okay, thank you.

12 All right, and then let's go to the credit card
13 use, too, and then we'll go into some new methods.

14 So, Jules, do you know to what extent an --
15 well, actually, let me ask this to Rebecca. I think
16 this would be better for her.

17 So, Rebecca, to what extent is the credit card
18 method being used for verification? And also, so we can
19 think about both issues, is it being used the way the
20 Rule contemplated that it has to be used, in connection
21 with a transaction rather than just as an identifier?

22 MS. NEWTON: Well, we don't use it, so -- but I
23 went out and did my own research, and I went on 11 top
24 kids' sites, and out of those 11 sites, four demanded or
25 required fax back or what we call a print-and-send; four

1 required credit card or some kind of a membership
2 transaction; three of them used email-plus; nobody used
3 the digital cert or toll-free.

4 So, I mean, I think it's just -- I'm just going
5 to be singing this same song. It's as -- I see a lot of
6 credit card fraud every day on our site, a lot, and it's
7 kids taking their parents' credit card and also people
8 buying credit cards online. So, I think it's just as --
9 it's used, but -- on some of these major sites, four of
10 the top 11, but I think that it's not any more valid
11 than any other site.

12 And the one point I want to make is that it -- I
13 think it also -- in a lot of cases for kids, it forces
14 them to lie about how old they are, and so, you know, we
15 know that that's -- that's something we talked about
16 this morning, and that's true with a lot of these
17 methods. But in my opinion, email-plus doesn't force as
18 much lying as the rest of these methods, in my
19 observation as well.

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

1 MS. TAYLOE: That's what Yahoo does. If you
2 identify yourself as 12 and under, they process -- I
3 think it's 50 cents. They take the transaction fee out,
4 and they donate the rest to NCMEC.

5 Now, for a number of years, they were just doing
6 an algorithm to see whether or not it was actually a
7 MasterCard or Visa number, which was not -- didn't have
8 a transaction, and I don't see as many people doing that
9 now.

10 And, Jules, what do you guys do at Microsoft?
11 Don't you use a credit card?

12 MR. COHEN: We use a credit card today.

13 MS. TAYLOE: Yeah. And I agree with Parry, you
14 know, there is Sol, there is some huge percentage of
15 parents that don't have credit cards and it's a tough
16 method if it's the only one you give people.

17 MS. KRESSES: Do you get any feedback on whether
18 people are comfortable with that?

19 MR. COHEN: I haven't seen any feedback, and I'm
20 not the COPPA expert. I have some expertise in this
21 space, but I don't have data on that one.

22 MS. NIEJADLIK: Jules, are you guys charging or
23 just authing?

24 MR. COHEN: Right now, we're just authing, but
25 there's a process in place to move to another standard.

1 MS. NIEJADLIK: Just coming from the payment
2 industry, the card associations, they have always said
3 that it's not okay to auth a card without a charge, and
4 they're actually starting to crack down on that now.

5 MS. KRESSES: And we don't think that's okay
6 either. I mean, the Rule was intended for a
7 transaction, and there's a little bit of discussion in
8 the rule about why that's the case, and a part of that
9 is that with a transaction, you have some recourse, too,
10 that you will get a bill. If something sticks out, you
11 would investigate it, you know, if it's a dollar -- you
12 know, we don't know how practical that is, how much it's
13 being investigated, but actually, the language of the
14 Rule actually requires a transaction. So, that's been
15 something that we've been educating people on in the
16 last few years, because it has come to our attention
17 that there's some -- you know, that there is a lack of
18 clarity there.

19 Roz?

20 MS. KITCHEN: I would just suggest that if
21 you're going to charge the under 13s a transaction fee
22 in order to get verifiable parental consent, that's not
23 going to work in the promotion industry, where we want
24 to possibly allow the child to participate in a
25 sweepstakes. You're going to have a situation of

1 potentially an illegal lottery at that point. So, in
2 complying with COPPA, you're violating all of the 50
3 states' lottery laws.

4 MS. TAYLOE: Well, email-plus is good enough for
5 sweepstakes and promotions and all the internal use,
6 right?

7 MS. AFTAB: There can be an exception, too.

8 MS. KITCHEN: (Off mic.) It depends how the
9 operator is using that information, if it goes
10 further --

11 MS. TAYLOE: You mean whether they share it?

12 MS. KITCHEN: (Off mic.) -- and also if you
13 collect user-generated content, perhaps you can't use
14 the exception.

15 MS. KRESSES: Okay, Parry, and then we want to
16 move on.

17 MS. AFTAB: I will be fast. I represent a lot
18 of the newer companies now that are looking for
19 COPPA-cleared communities and that kind of thing, and
20 they're all trying to charge a dollar or 50 cents, and
21 they are trying to donate it back to Cyber Safety and
22 the rest of it. Huge push-back. Parents aren't doing
23 it at all. So, if you're doing it, it's nice to saying
24 you're doing it, but if you don't have a backup that's
25 going to work, you're out of business.

1 MS. KRESSES: Okay. And, Alan, do you have any
2 sense of whether the use of a credit card still provides
3 as much assurance of a parent or an adult, let's say, as
4 it may have ten years ago?

5 MR. SIMPSON: I don't think it's changed much.
6 I mean, I went back and looked at this after we talked
7 about that earlier. Those numbers -- and in college
8 kids, you see a huge boost in credit card or debit card
9 ownership, but when you talk about under 13, those
10 numbers aren't really significant.

11 So, does it prove -- again, what standard of
12 verifiable are we looking for here? It's as reliable as
13 anything else, and it's not likely to see -- have
14 someone under 13. It's a very small number.

15 MS. KRESSES: Okay. Does anybody -- yes?

16 MR. LEMONS: Chris Lemons from RelyID. A couple
17 points to throw in.

18 One is that a lot of credit card companies, the
19 banks now are moving purely to online statements. The
20 way you used to know that you had gotten a charge
21 against your credit card is you got an envelope in the
22 mail, and you opened it because it came in to see what
23 was in it. Now, it's more you have to click onto the
24 email that they sent you saying your online statement is
25 available, go to the website, remember your log-in and

1 password, then scan through a couple pages of
2 transactions.

3 I think that's much less reliable in terms of
4 ensuring that a parent knows that transaction ever
5 occurred. And all the kid has to do is sneak downstairs
6 and get mom's wallet, right? So, there's less of the
7 feedback loop than there used to be.

8 The other point is that I think the credit card
9 associations are moving strongly away from using credit
10 cards as authentication, period. Visa has come out with
11 a statement saying that they don't want to use for age
12 authentication, right, which is just a step from
13 identity authentication.

14 MS. KRESSES: Thank you.

15 Alan or Denise or Rebecca, any of you, are you
16 hearing many complaints about parents -- about kids
17 falsifying verification?

18 MS. NEWTON: Well, yeah, I mean, I get some. I
19 don't -- you know, out of 70,000 a day, I think I maybe
20 average a half of one a day or something like that. So,
21 I mean, it definitely -- it -- I mean, this is a
22 different question, I guess, than you're going to ask
23 about deleting PII. Is that right? You're not asking
24 about that.

25 MS. KRESSES: Yeah. No, we will get to that,

1 but yeah, that was my question, is whether -- are
2 parents -- are parents calling and complaining, "well,
3 my kid used my credit card without authority or my
4 kid -- you know, somehow my kid got on there and I never
5 consented?" Are we hearing a lot of complaints?

6 MS. NEWTON: Some of that. I wouldn't say a
7 lot, but I definitely hear it.

8 MS. KRESSES: Ron?

9 MR. ZAYAS: One of the things we did, not a
10 formal survey, but we went to about a hundred different
11 schools and we matched the parents and the kids to the
12 schools, and we asked the parents, how many of your
13 kids -- and these are between middle school and
14 elementary -- how many of your kids have a Facebook or
15 MySpace account? And almost universally, the parents
16 said "my children don't." And then we matched it up
17 with their actual children, and we asked them how many
18 of you have a MySpace -- and about 60 to 70 percent of
19 them did.

20 So, I don't know that it's so much are parents
21 complaining that they're not getting asked or that they
22 even know it exists would be a better question.

23 MS. KRESSES: All right. Okay. So, let's move
24 to the last -- in the Rule, there's also the language
25 about using a digital certificate that uses public key

1 technology. Where is that at?

2 MS. NEWTON: I've never seen it anyplace, so I
3 don't know about that.

4 MS. KRESSES: What happened with -- Jules, do
5 you have just some brief thoughts on what happened there
6 or didn't happen?

7 MR. COHEN: So, a couple thoughts on digital
8 certificates in general. One of the -- so, the way I
9 think about digital certificates is that they're
10 generally being analoged to the cards that you have in
11 your wallet. So, you have a bunch of identity tokens in
12 your wallet as an adult, and they represent different
13 things that people have said about you. Your driver's
14 license, the DMV says you have passed the test to drive;
15 the AAA card in my wallet says I'm current with my AAA
16 membership if I have one; my student ID says something
17 else about me. Those are certificates in the real
18 world.

19 So, digital certificates would be essentially
20 the same thing, analogous to each of those things in the
21 virtual world, and they can carry the same kinds of
22 identity information about the bearers, you know, a set
23 of claims, he's over the age of something, has brown
24 hair, you know, whatever the claims may be, is a student
25 at, you know, some university.

1 And so in the context of COPPA, what a digital
2 certificate might do is allow somebody who has been
3 issued the digital certificate by, you know, an approved
4 issuer, like Denise or somebody, the ability to present
5 that token at a bunch of relying parties, a bunch of
6 sites who will accept it. So, it's more of a vehicle
7 for conveying the trust that's been created during an
8 issuance process, during the approving process, than
9 necessarily an approving process that would stand alone.

10 So, the interesting question is, where are they?
11 And, you know, that technology was nascent ten years
12 ago. It continues to be nascent. And part of the
13 reason for that is that there haven't been huge needs
14 over the last ten years, although we're beginning to see
15 them now, that would drive that kind of technology into
16 consumers' hands, into citizens' hands. The kinds of
17 needs that we see are the kinds of ones that we see
18 here, where you need to get a reasonable proof of
19 something, in this case verifiable parental consent, at
20 a reasonable level of assurance, you know, how strongly
21 do you want to know that that is the case, and we see
22 similar needs in other industries that are, I think,
23 going to drive some of the adoption of this stuff.

24 Denise has done some pioneering work in this
25 space. Microsoft actually has spent some time with her

1 collaborating, but, you know, in places like health care
2 and places like finance and places like, you know, tax
3 and government transactions, as those kinds of things
4 move online, I think we'll see more needs to use digital
5 certificates in a significant way, and that might help
6 bring it in a more meaningful way into this space. But,
7 you know, at this point, it's rather nascent, and we can
8 talk a little bit more about it if --

9 MS. KRESSES: Do you think that the popularity
10 or the rising popularity of OpenID and, you know,
11 services like OpenID or Facebook Connect, Google Buzz,
12 and all the other ones that I can't think of, whether or
13 not that in any way could push a movement towards, you
14 know, using some sort of digital certificate or ID for
15 parents?

16 MR. COHEN: So, here's the way I would think
17 about it, is that there are lots of ways to issue IDs.
18 OpenID is an ID, my driver's license is an ID, and those
19 IDs are only as good as the strength of the issuance
20 process. And so one of the things that I think
21 policy-makers need to grapple with is you can apply a
22 very robust issuance process, you know, the kind you get
23 when you go through -- when you get a passport or a
24 driver's license, to an OpenID, and that would be a very
25 strong process backing a not-so-strong usage, or a

1 different way to say that is you can issue me a very
2 strong credential, but if there isn't security attached
3 to it after the fact, it's just a user name or password,
4 and I can give it to you or I can give it to Denise or I
5 can give it to Ron. The subsequent uses aren't very
6 robust, and that's sort of challenging, or I can attach
7 to a smart card or something very robust, and then I end
8 up in a place where I have a much higher level of
9 assurance that the person coming back is the person it
10 was actually issued to begin with.

11 So, the things like Facebook Connect and OpenID
12 and Info Cards and the various technologies in this
13 space are all great things to pass around claims about
14 people that have been made, but they're only as strong
15 as whatever offline or, you know, online issuance
16 process backs them. So, we end up in the same place.

17 I can issue you a very strong digital credential
18 based on email-plus, but it's only as good as the
19 verification that occurred up front. So, they are a
20 vehicle for disseminating proofs.

21 MS. TAYLOE: I would say Facebook Connect and
22 OpenID and all of that, though, works great for the
23 parent. So, earlier somebody was talking about how
24 Facebook Connect works. So, if you said, "Hey, parent,
25 we need you to create your parent account, you can use

1 your Facebook log-on to do that," most parents or a lot
2 of parents now have Facebook accounts. You can suck up
3 the data about them from their Facebook through the
4 open -- the API that's provided, present that to the
5 parent so they don't have to fill in any of the
6 information, then layer it with it's either an email to
7 them that they click, now you have an email-plus, but
8 they can now do this with their Facebook account, you
9 know, logging on to deliver the consent going forward.
10 So, I think those things actually play in in creating
11 the accounts as well.

12 MS. KRESSES: We got a comment just a couple
13 days ago about advocating for the use of eSign for
14 parental consent, and actually, this is something that
15 we thought about. You know, it's not uncommon to just
16 now type your name into forms.

17 And, Alan, how do you see -- do you see the use
18 of eSign as workable for providing reasonable insurance
19 of parents or --

20 MR. SIMPSON: I think it's a reasonable place to
21 look, because Jules' point is very valid. I mean, all
22 of these are undergirded by how robust is the system
23 beneath it, and actually, when we were talking about
24 that, I had a flashback to friends of mine -- not, of
25 course, me -- faking their IDs back at certain ages.

1 All of these things can be built around.

2 But having something better, having something
3 like eSign, where the balance between accessible
4 technology, easy technology, and some greater level of
5 verification is where we're, I think, aiming. The
6 perfect won't be reached. So, is eSign an option?
7 Would it get more parents engaged?

8 I liked the point that someone made earlier
9 about not even just some of the benefit here of
10 notification, at least getting parents engaged in the
11 fact that your kid is now going to this site. Okay,
12 maybe I didn't really get an informed consent there, but
13 maybe I got a slightly greater awareness on the part of
14 that parent that this is what my kids are doing.

15 MS. KRESSES: And with that would you want to
16 see an opt-out as far as your parent -- your children --
17 your parents are engaging on a site.

18 You know, would you want to see an opt -- do you
19 think it would be sufficient to give parents an opt-out
20 in certain circumstances?

21 MR. SIMPSON: I think it would help a lot. I
22 mean, that's sort of shorter-term engagement that we can
23 kind of guess in this space that those things might be
24 helpful. Getting an 18-page document isn't going to
25 work. Being asked to print out and sign and fax

1 obviously has only been taken up by so many.

2 MS. KRESSES: Um-hum, okay. Let's go into
3 mobile phones, and we're going to delve a little into
4 Martine's experience and really do welcome, you know,
5 questions and comments, too, as we face new -- you know,
6 new possibilities and we closely consider them.

7 So, obviously it's been said many, many times
8 that mobile phones are becoming a central mode of
9 communication, and we know that they're being used as
10 payment devices as well, and, you know, in other parts
11 of the world, it's been going on longer than here. So,
12 you know, I want to ask the question of what role can
13 they play in parental verification and when? When would
14 it work if there's a role?

15 So, let me just start with you, Martine, and if
16 you could give a little background on what you're
17 contemplating for a potential mobile phone method.

18 MS. NIEJADLIK: Okay. So, first, let me just
19 say that mobile obviously comes up a lot, and it can
20 mean many, many different things. It can be used in
21 many different ways. And even when you talk about
22 mobile payments, which is what I say we do as a company,
23 if you talk to PayPal, they'll say they do mobile
24 payments and it's actually very different from what we
25 do.

1 So, let me just take a minute quickly and just
2 describe what it is that we do and then what we're
3 thinking about in terms of authentication. So, some
4 people joked earlier about texting American Idol and
5 weren't really too familiar with that or hadn't had that
6 experience. I'm going to take you into another
7 experience now.

8 So, pretend you're on Facebook and you're
9 playing a game, Farmville -- who's heard of Farmville?
10 -- a lot of people, okay -- and so you want to buy a
11 tractor for your farm, right? You want your farm to be
12 really great and you want to get a tractor, because
13 you're tired of mowing the lawn, and the tractor costs
14 \$5. So, one of the things that you can do now is you
15 can pay with your mobile phone, and what that means is
16 that we will charge direct to the carrier.

17 So, there's no credit card, there's no bank
18 account. The way the flow looks is that you say I want
19 to buy a tractor, you click on "pay by mobile," you give
20 us your telephone number, and then what we do, for every
21 transaction that comes through our site, is we send an
22 SMS message to confirm that it's actually you who is
23 giving us the phone number and I'm just not giving
24 Rebecca's number, and then you have to reply to that
25 text message, and when you reply, we go ahead and we

1 bill the carrier.

2 The billing, by the way, the way we do it occurs
3 through a platform called Premium SMS, which is
4 something that has existed for a long time for the
5 purchase of ringtones and other things that people use
6 on mobile, so we're leveraging that now to offer mobile
7 payments as an option. We're particularly focused on
8 digital goods and virtual worlds and social networking
9 and that whole sort of space, and one of the main
10 reasons for that today is because the carriers charge a
11 very large fee to be able to use one of these payments,
12 and so it doesn't make too much sense in the physical
13 world at the moment, but we certainly see it moving in
14 the direction -- and very quickly -- that it's going to
15 start applying to many other areas as well.

16 So, it's sort of the fact that we're in social
17 networking and digital goods and all that sort of stuff
18 is the main reason I'm here today. We certainly
19 recognize, as everybody knows in the room, that there
20 are children who are using these services, despite the
21 fact that, you know, Facebook says you have to be 13,
22 and particularly because we're a payment service, we
23 feel the responsibility to ensure that children are not
24 spending exorbitant amounts of money online, right, not
25 buying all this stuff and playing these games.

1 And so what we are contemplating doing now is to
2 introduce another step into the payment flow whereby
3 instead of just directly texting the child to confirm
4 that they want to make a payment, the child's got the
5 phone, so, sure, great, let me make a payment. We would
6 instead text the parent. We may offer email as an
7 option as well if that continues to exist, ask the
8 parent if we have consent to, (a) collect the phone
9 number from the child to do the billing, and then (b) to
10 process the transaction.

11 We see actually some super-interesting things in
12 utilizing this technology. Number one is that one of
13 the downsides I think of email is that people can create
14 many, many, many, many different email addresses. You
15 can't really do that with a phone. I mean, yes, you can
16 buy prepaid cards. They're not very popular in the U.S.
17 They're more popular internationally, but it still would
18 be a burden to go and buy many, many prepaid cards to
19 try to get around that. So, it's very sticky, right?

20 As soon as somebody gives us a phone number and
21 gives us an age, you can't really just go back and say,
22 "Well, no, let me give you another phone number,"
23 because that's not your phone anymore. So, that's one
24 of the big benefits.

25 Two, we're doing this actual physical device

1 verification, which is extremely unique. I've been in
2 the fraud space on the Internet pretty much since it
3 existed, and, you know, lots of companies now are
4 issuing these tokens, like you have a little PayPal
5 token you can carry around in your wallet. The fact of
6 the matter is nobody has them, and nobody wants to carry
7 around, you know, 50 of these things on their key chain.
8 So, this is a physical device that has already been
9 issued, is available to people, and people have it,
10 which is wonderful.

11 And so by doing this type of verification, it's
12 much different from just asking questions -- you know,
13 what's your mother's maiden name, what's your password,
14 what's this, what's that -- and then you get people who
15 try to steal that information or guess that information,
16 those kinds of things. So, that's a big benefit as
17 well.

18 Today, in the mobile industry, there are tools
19 available, and we actually see there being even more
20 tools being available. So, in the U.S., for example, I
21 think pretty much all the carriers offer the ability to
22 block Premium SMS. So, when a parent issues a phone to
23 a child -- and they may or may not realize today that
24 that's a payment instrument, they will figure that out
25 eventually soon -- they have the ability to say, "Well,

1 I don't want this physical device to be used for
2 payments," and they can issue that block.

3 I've already, just yesterday actually, heard
4 that there are other countries that are getting on that
5 bandwagon as well. So, that's great. It's a very
6 global payment option. So, we today are live in 60
7 countries with almost 200 carriers, and we reach 2
8 billion people out of the 6 billion in the world. So,
9 there are 2 billion people that have phones that could
10 pay through our service that are SMS-enabled, et cetera,
11 et cetera. So, that's fabulous as well. So, a lot of
12 people have phones.

13 MS. KRESSES: If you could -- I am going to ask
14 you the question first, and then I am going to ask some
15 other folks on the panel, too. What do you see as --
16 you know, looking at the standard that, you know, it has
17 to be a -- you know, a method reasonably calculated to
18 obtain verifiable consent and reasonably calculated to
19 ensure that it -- that the person giving consent is the
20 parent, what do you see as the challenges to having that
21 level of assurance and what would you like to see, you
22 know, from other -- what would you like to see from the
23 carriers or the device makers, et cetera, that would --
24 if there are challenges that would change those
25 challenges?

1 MS. NIEJADLIK: Um-hum. So, Mamie, you and I
2 have chatted a little bit about this. I think another
3 thing that we're sort of thinking about is when a child
4 is coming through to process this payment, should we
5 bill the child or should we bill the parent, right? We
6 now actually have the opportunity to do either, because
7 we have collected the phone numbers of each one.

8 So, if, for example, we introduce the option of,
9 well, let me just bill the parent, the child is
10 certainly going to be less incented to provide their
11 best friend's phone number, because their best friend is
12 going to get in trouble when that charge shows up on
13 their bill. So, that's one thing that we're sort of
14 thinking about.

15 I think there's benefits to billing the child
16 and billing the parent, and I think that's something we
17 will probably test to sort of see what the acceptance
18 is.

19 I think in the mobile space, again, there are
20 tools, like blocking the Premium SMS that's out there.
21 We actually also got notice very recently that at least
22 one carrier in the U.S. is planning to build a zip code
23 verification tool. So, one thing we could do is we
24 could pass in the zip code and we could find out if that
25 was really the zip code associated with the plan.

1 So, we could say, for example -- we could even
2 do it location-based right? You could say, well, give
3 me the zip code of the child and give me the zip code of
4 the parent, and if those were in two totally different
5 places or neither one of them verifies with the carrier,
6 that could indicate that maybe this wasn't really the
7 parent. You could expect if the kid and parent is on
8 the same plan, they probably have the same zip code as
9 well.

10 So, lots of things like that that are coming out
11 in the industry that will make the verification even
12 stronger, but even today with the charge happening in
13 combination with the phone and just to your point about
14 parents not really using SMS, you know, I think -- I
15 think the tendency to use SMS is probably also a little
16 bit different if I'm just picking up my phone and I'm
17 just texting you versus if I have my phone and all of a
18 sudden it beeps and it says, "Oh, your child it trying
19 to do something. Are you okay with it? Respond yes or
20 respond no." I'm probably much more likely to be able
21 to do that and follow those instructions than just sort
22 of creating my own SMS.

23 DR. O'KEEFFE: I think the 30 percent of parents
24 that Amanda is mentioning are a lot of parents that
25 aren't using texting, so, you know, I was making

1 obviously a sweeping generalization, but when I see
2 parents come into a clinic, for example, or just walking
3 down the street or even my own town in Massachusetts,
4 which is a nice middle class town, you would be
5 surprised how many parents still aren't embracing
6 texting. So, some are cultural, some are socioeconomic,
7 we can't make global generalizations, but 30 percent is
8 still 30 percent. That's a lot of people.

9 MS. KRESSES: Let me ask Alan, and then we'll
10 take some questions. What do you see -- I shouldn't say
11 what do you see. Do you see challenges from either the
12 reliability standpoint or parents' acceptance of a
13 mobile system like this?

14 MR. SIMPSON: I see opportunity. I mean, there
15 are the same challenges for all of these things, but in
16 the earlier discussion about mobile -- and we talked
17 about this a little bit in our earlier call and I've
18 talked to a number of people about it -- I don't see why
19 you don't have mobile phone companies already out there
20 proactively saying, "Hey, when you're coming in here to
21 get five phones, we're going to make a hunch that you're
22 doing a family plan. Do you want to register those
23 phones to specific ages?" Totally an option. The FTC
24 obviously wouldn't mandate it, but why not enable those
25 phones so that you know which one belongs to the parent?

1 There is a signature on those phones. You know which
2 ones belong to kids that are under 13.

3 I'm not a technologist, but some of this stuff
4 seems -- the fact that we are increasingly moving into a
5 space where we can pay for things with our mobile phones
6 means we can do a lot of other things with them as well,
7 and I see a lot of opportunity there. I fully
8 appreciate Gwenn's point, but none of these things solve
9 for every family, and adding technologies that would --

10 DR. O'KEEFFE: What you said is perfect for
11 safety. That's a whole another issue.

12 MR. SIMPSON: Right. For safety, for a better
13 verification, that, okay, this phone -- again, there
14 should be an option, but why not have a family phone
15 system where we know that these phones are kid phones
16 that belong to this phone, which is a parent phone?

17 MS. KRESSES: And, Ron, you looked like you had
18 something to say.

19 MR. ZAYAS: Yeah. I think that it's a great
20 layer for three different reasons. Number one, it's an
21 opt-in from the parent. By saying at the point of
22 purchase when you're buying an iPhone or you're buying
23 any kind of a mobile phone or an iTouch or anything
24 else -- not that I'm a heavy Apple person -- but you're
25 making it aware to the parent that here is an extra

1 parent.

2 Sprint -- we have both AT&T for our iPhones and
3 then we have Sprint for our children's phones, and they
4 do a very good job of saying, "Look at all the things
5 that we have for kids' phones. You can locate them.
6 You can, you know, limit their amount of time. You can
7 do all these things with it." It's a great marketing
8 for the phone companies. It's a great way to make the
9 parents aware.

10 Second, the opt-in is good, because now the
11 parents who want to put this protection, put it in, and
12 the ones who don't, don't. The second thing is that it
13 can apply to lots of different areas. Cable connectors
14 can do -- you know, your cable provider can do this in
15 many different ways, too, obviously limit it to the
16 computers, but you can have a token where they log in --
17 where the child logs in or the computer IP comes in, and
18 right away, you can log a computer and say, "This is a
19 computer that my child uses, and I want them to know
20 that."

21 The third level, though, here that needs to be
22 very important, and if it becomes one of these standards
23 where the FTC can help promote this, is if you say to
24 the Facebooks of the world and the MySpaces, "This is
25 something that's available. This is something that

1 meets this requirement, and we think it's a good way of
2 doing this," it puts a lot of pressure on the content
3 ones to not only say the token exists, whether it's an
4 OpenID or whatever it is, the token exists, but on the
5 other end, if the token does exist, you probably should
6 be listening for that token and you should probably be
7 respecting that. That's a very strong rule that, when
8 you put it on top of all the other ones, ends up
9 covering a lot of people.

10 MS. KRESSES: Okay. Yes, Peter.

11 UNIDENTIFIED SPEAKER: (Low mic). There's
12 clearly a lot of vendors trying to solve this problem,
13 okay, and the big problem is the cost of going beyond
14 the email-plus, right, that no one wants to do the big
15 authentication piece, because the cost of acquisition of
16 a user is so high when you do that piece. But all the
17 different providers that have got solutions, I would
18 urge you, as a plea, to come up with a protocol, lay it
19 on top of OpenID or (inaudible) something like that,
20 that allows all providers to exchange the policy
21 information that the parent wants to that site, either
22 be it as simple as authorizing them to use that site or
23 to say I allow them to use this type of chat level or I
24 allow them to make purchases on the site or make friends
25 on the site.

1 But that's something the FTC could get behind.
2 They can't get behind the vendor. They can't say, "Hey,
3 use this vendor or that vendor," but you could say,
4 "This is the protocol that will allow parents to share
5 the policy requirements to that site," and that's
6 something I'd like to see everyone get together and say,
7 "Let's do that." Hey, we're not in that business, but
8 you guys all are, so...

9 MS. KRESSES: Okay, yes.

10 MR. O'HENRY: Mark O'Henry with the Software &
11 Information Industry Association.

12 The only problem -- our industry is one of the
13 biggest fans of using encryption digital technology to
14 authenticate. The problem, though, is the standard that
15 the gentleman just uttered is not the standard of COPPA,
16 and that's the problem we have, which is how does the
17 infrastructure of digital certificates ensure that the
18 person providing consent is the child's parent? That is
19 a very unique standard which would require, based on our
20 experience, and I worked in the Federal Government on
21 this issue when you-all were -- I think I was still
22 trying to put together a bridge certificate policy.

23 That's not just a technological investment.
24 It's a broader investment about a structure that
25 verifies that, and that's the challenge we're going to

1 have with trying to take commercial models, which may
2 not need to have that level of insurance as it happens,
3 and applying it to the COPPA standard. That's the
4 fundamental problem we've got, is having it be
5 pervasive.

6 MR. ZAYAS: But nothing up here would meet that
7 standard today, so --

8 MR. O'HENRY: But because of the nature of
9 digital certificate technology, it's held to a higher
10 standard, because these things get as close as possible.
11 There is no equivalent in the digital certificate
12 environment.

13 MS. MARCUS: Did you still have a thought?

14 UNIDENTIFIED SPEAKER: Yeah. I was just going
15 to go back to the voluntary offering up of information
16 and designating individual devices as children's
17 devices. Since Heidi's not here to speak for the
18 telecom industry, I'll step in.

19 To what -- going back to our earlier sessions,
20 to what extent, if that's not in any way regulated, if
21 it's not required, if it's not designated as being
22 authorized, to what extent does that type of provision
23 of information to the telecom carrier constitute
24 constructive knowledge or actual knowledge and to what
25 extent do those telecom carriers have to process that

1 through all of their systems and to any of their
2 suppliers? Just the question is how far does that have
3 to go if you give that knowledge?

4 MS. KRESSES: Okay. And then let me turn the
5 question back, too, let's assume -- we're talking about
6 a lot of sort of at-purchase ideas, which are, you know,
7 great ideas, and we -- you know, we've heard talk of
8 them before, but let's just assume for the moment that
9 we have a parent who, you know, gave their kid a phone,
10 but they -- you know, they got it at the mall, and they
11 want to be out of there in five minutes, and they didn't
12 do any of that, and now, they have a phone for -- and
13 they want to use it as the means to getting payment, and
14 we'll assume for the moment that they're a law-abiding
15 child that identifies themselves as being 11.

16 Rebecca, in that situation, do you see any
17 concerns with the use of mobile or how do you equate it
18 as far as reliability to other systems?

19 MS. NEWTON: Well, in that instance, I don't
20 think it's any more reliable than any other method. I
21 think in the instance of -- where they've gone in and
22 they've registered and they've said this is my kid, then
23 it's obviously -- to me it's obvious that it's much more
24 reliable.

25 MS. KRESSES: Okay. And are there -- and I

1 guess I would throw it out, too, are there -- I think
2 Martine raised a lot of suggestions for ways to increase
3 the reliability as the technology develops. Are there
4 other suggestions on using mobile and at the same time,
5 you know, ensuring added layers of reliability?

6 MR. LEMONS: Chris Lemons with RelyID.

7 I think part of the problem that we're seeing in
8 the market is that the methods on the right-hand side of
9 the slide up there don't actually achieve the general
10 standard that's on the left, but because everybody knows
11 they can do what's on the right-hand side, no one has a
12 marketplace to serve. So, as somebody mentioned
13 earlier, the conservative approach is pick one or two or
14 three of the things on the right-hand side and let the
15 kids lie, instead of going out and searching for
16 something that actually achieves what's on the left hand
17 of that slide.

18 I think one approach for the Commission might be
19 simply to get rid of its listing of methods and fall
20 back on the standard that the general standard is the
21 standard, and use some discretion about not enforcing
22 that strictly until there's good technology out there,
23 but signal to the market that what's currently
24 acceptable isn't gonna be.

25 MS. KRESSES: Okay. Well, that's a lot -- doing

1 a lot of things, so changing it just to the general
2 standard and sending a signal and you're probably
3 scaring a lot of people in the room, but actually, that
4 is one of the questions that we wanted to touch on
5 today, and we'd love to hear other opinions, is what is
6 the better way to move forward and what is the better
7 way to give guidance?

8 Is the better way to give guidance to simply
9 have the general standard? Is it helpful to enumerate
10 possibilities and potentially add more to the list or is
11 it better to get rid of the list? So, for a couple
12 minutes, we would welcome thoughts on that.

13 Parry?

14 MS. AFTAB: The real problem here has always
15 been, from the beginning, is you never know if you have
16 got a parent, and not only if you have got a parent, you
17 don't know if you have the custodial parent who has the
18 legal rights over this kid, and the only people who know
19 that, if the kids are in school, are schools. So,
20 they're the ones who know which parents are really
21 parents, who has the authority, the people who are on
22 the forms, the people who can do that, and until
23 somebody works on a model that can deal with schools and
24 not offend FERPA, so that you can conform, and I think
25 as we're looking at mobile technologies, finding schools

1 that will partner with you, maybe if we just start with
2 private schools that don't have to contend with some of
3 these issues, you turn around and say to the parents,
4 "You can authenticate with the school, one-time
5 authentication, we will know that you're the parent,
6 thereafter you'll have it," you are starting to see that
7 model work.

8 It's not scalable at 425 million people on
9 Facebook, but it will work for the sites that are 500
10 million to -- 500 million -- 500,000 to 2 million, which
11 is a lot of the preteen stuff. It's a good way to get
12 there. Unless you work with the schools, you're never
13 going to get the stuff, because nobody else has this
14 information.

15 MS. KRESSES: Okay. And we are going to go
16 right to that in a second. I just don't want to
17 preclude the opportunity if anybody else has a thought
18 whether the standard should be broad, narrow, longer,
19 shorter.

20 Sheila?

21 MS. MILLAR: Yeah. I think there are two
22 things. One is that the different methods that satisfy
23 the rule are related to the information collection. So,
24 you allow for email-plus where you're only doing interim
25 marketing to the child. The other more robust methods

1 involve data sharing and disclosures, and so I think we
2 need to keep those different marketing opportunities or
3 different disclosure issues in mind when we think about
4 the methods that satisfy the rule.

5 I think having the enumerated methods which
6 people are accustomed to after 12 years of dealing with
7 COPPA remains helpful, but exploring new methods,
8 whether it's new ways to look at digital signatures
9 where you can actually sign on your computer or mobile
10 technologies, mobile phone technologies, all of that is
11 worth exploring, but I think we have to go back to
12 certain methods, you may require more robust methods for
13 different types of data collection and use than others.

14 MS. KRESSES: Okay. I think we had a question
15 here first and then we'll go to Phyllis Spaeth, right in
16 front of you.

17 UNIDENTIFIED SPEAKER: Let me just say that I
18 feel like it's deja vu all over again. It's like we're
19 repeating the conversation from when the Rule was first
20 adopted, which is the problem with just going to a
21 general standard, is read literally, we would have to
22 provide a birth certificate and DNA sample to meet the
23 standard. Everyone realized that was absurd for a lot
24 of reasons. It didn't achieve the goals of the Act and
25 it also was just impractical.

1 So, the methods, again, to repeat -- and we can
2 go back and check the transcripts from ten years ago --
3 these came as close as we can to creating a legal nexus
4 that suggests, better than nothing, that the parent is
5 the person signing this or doing the things that are
6 there, so...

7 MS. KRESSES: Okay. Phyllis, can I bump you,
8 because the other Phyllis just told me how little time
9 we have left. So, let's save it until the end of the
10 discussion.

11 So, Parry raised the school model, and, wow, Ron
12 has something to say about the school model. So, I --
13 you know, and again, because I poorly managed our time
14 here, Ron, if you could give us just a brief synopsis
15 of, you know, what you're trying to do and a little bit
16 of what you see as the opportunities and the challenges.

17 MR. ZAYAS: Very quickly, eGuardian came up with
18 the idea or worked with -- everybody comes up with
19 different ideas -- of going through the schools and
20 saying the school is a great place to verify. They know
21 the parent. They know the custodial parents. They know
22 the age of the child, and it's very hard to fake. You
23 can't just say "Well, I screwed this one up, let me
24 create another child at another school." You just can't
25 do that.

1 So, we work with the schools, and originally,
2 there was some push-back from the schools of dealing
3 with a private entity and saying, "Why would we give you
4 that information?" And the legal hurdles were cleared,
5 you know, because again, the parent is initiating this.
6 The school is not giving out the information. The
7 parent is initiating the information. The school is
8 verifying it.

9 But realistically, we found a non-profit should
10 do this. A private entity should never have this
11 information. We looked at people who were trying to buy
12 our company, and we realized they were trying to buy us
13 for the wrong reasons. A non-profit, a third party, can
14 have this information, but that information exists.

15 Tap into that information. Tie it into an
16 OpenID or tie it into a type of token or certification,
17 and you now have something that you can uniquely give to
18 a parent who they can control, and they can opt in and
19 say, if this exists, places like Facebook should read
20 it, and MySpace and whoever else, if it exists, if the
21 parent or if the unit, the phone, whatever it is, sends
22 you an ID that says "this is the child and I'm the
23 parent," that should override anything the child types
24 in.

25 And, again, obviously our company does this, but

1 it's not the point of our company doing this. This
2 should be open to everybody. This -- as you were
3 saying, open to every company that's out there, but we
4 have that information, at least in the U.S., and in most
5 western nations, it exists, and if somebody just pushed
6 it a little bit, if somebody said this could be one of
7 the ways to meet that, I think you'd see a lot of
8 websites starting to take that information.

9 MS. KRESSES: Adam?

10 MR. THIERER: A very brief question on that
11 point. Adam Thierer with The Progress & Freedom
12 Foundation.

13 I do wonder if we want to make schools into DMVs
14 for kids, because there are liability questions and
15 privacy questions that pervade the use of personal
16 information about kids, and if we made this a new COPPA
17 standard, I mean, we'd be requiring, you know, check
18 points at every school door for credentialing kids to
19 say, you've got to hand over information to do what? I
20 mean, that puts the schools in a really difficult bind.

21 It also raises the question of is there greater
22 potential for identity theft because of this? And then,
23 of course, there's the question of what about -- are we
24 incentivising kids, instead of to lie about their age,
25 to trade -- to barter in digital credentials? I mean,

1 older brother giving to younger or whatever?

2 MS. KRESSES: Let's do this: Let's let Ron --
3 can you back up a little and tell us actually what
4 information you get, who you get it from, who verifies
5 it, and then what people either carry in their heads or
6 in their hands?

7 MR. ZAYAS: The parents tend to provide -- first
8 of all, it's always initiated by the parent. The parent
9 has to say, "I want to verify my child." So, the parent
10 would say the child's name, the child's age, who they
11 are, and a physical address and a signature, and there's
12 an electronic way of doing that, we won't go into that,
13 but the school then gets the information and verifies
14 it.

15 By the way, schools do that today. There's the
16 YMCA, there's soccer, there's lots of different areas
17 where you have to verify the name and age of child, and
18 the school is the way to do it, and they already have a
19 process for doing it. They already have an individual
20 there generally who's bonded to be able to do this. So,
21 the liability already exists or the function exists to
22 do that.

23 The second thing is that once the parent does
24 that, then they're issued an ID, and that ID should not
25 have anything other than the parent's email, their

1 verified email, tied to it. So, you're not pushing out
2 information on this is Bobby Smith. That should be an
3 anonymous token. It simply says, though, that now that
4 it's tied to this log-in, if there's ever a problem or
5 we need any verification, we know the email that we're
6 going back to. And if you do that, I think you're
7 protecting a lot of information.

8 The parent can even release and say, "You know
9 what? I want to release my child's age," which
10 automatically gets updated, but it's the parent's
11 decision to decide what gets updated, and by the way,
12 you could have different levels. For one type of
13 website, you might want to release other information.
14 For some, you might only want to release the most basic
15 information. But it puts the control back in the
16 parent.

17 MS. KRESSES: Okay. And I think, John, you had
18 a comment on this procedure as well?

19 UNIDENTIFIED SPEAKER: Yeah. I mean, just kind
20 of the broad comment that, you know, imagine we could
21 come up with a system that provided a unique digital
22 certificate for all school-age kids in the country. I
23 actually still don't understand how that works in
24 practice for sites like Facebook or MySpace that are, in
25 fact, intending to reach both older minors and adults,

1 because, I mean, you know, a child gets on and says,
2 "I'm 18 years old," and so, you know, do we have to go
3 verify and identify all 400 million Facebook users in
4 order to be able to force those who have these
5 identifiers to come up with it? You know, so, I mean,
6 it can work in some scenarios, but I'm not sure it works
7 on a Facebook.

8 MR. ZAYAS: And we see it -- and we worked very
9 closely with Facebook, by the way -- we didn't get
10 anywhere, but we worked very closely with Facebook --
11 and now that Chris Kelly is running for Attorney General
12 of California, we haven't gotten his full attention.

13 The main thing here, by the way, is not
14 necessarily that you go backwards, but it's tying that
15 ID to certain -- if I say, "I want that ID sitting on my
16 child's computer," then when my child uses that computer
17 and goes to Facebook, it's being transmitted then. If I
18 say I want it on their phone, it's being transmitted
19 then. And if I don't want to have it on their phone,
20 then I don't do it, and my child is free to do whatever
21 I want.

22 But the idea would be that as Facebook gets
23 somebody coming onto their site that's saying, "I am on
24 a protected or I have an ID that's being transmitted,"
25 that they would listen for that ID, and that now they

1 know who the parent is. That's the whole idea.

2 MS. KRESSES: And, Jules, do you have any
3 thoughts on how -- whether this is a useful system and,
4 if so, how it could be furthered? Is there -- it sounds
5 like, you know, Adam's raised the concern, you know, of
6 privacy concern, and John has raised more of a
7 technology concern. Do you have any thoughts on either
8 of those and whether this could be use understand some
9 way that would avert those?

10 MR. COHEN: There are certainly ways -- so,
11 generally speaking, the schools are an authoritative
12 source for some pieces of information, just like for
13 adults, you know, there are other institutions that are
14 an authoritative source, and if you want to -- as a
15 policy-maker, if you want to say this is the level of
16 assurance that would be required for this kind of a
17 transaction, then it might be interesting to look at
18 schools as a source of that information. We've talked
19 about this in the past, you know, as a group.

20 The thing that I think is important is to
21 separate the method of getting that level of assurance,
22 the school or the DMV or the email-plus, whatever that
23 method is, from the technology that's used to convey
24 that piece. So, the technology that's used to convey it
25 might be a phone or it might be email or it might be a

1 smart card or various different levels of assurance, but
2 that's the piece that the technology can manage, and the
3 technology can manage how secure that is, how privacy
4 friendly that is, and there are a bunch of policy levels
5 that you can tweak inside the technology ecosystem.

6 But I think the key thing is to separate the
7 technology decisions that are made from the policy
8 decisions that are made about the proofing process and
9 what is the right level of assurance. I think
10 separating those two helps sort of keep the conversation
11 going.

12 MS. KRESSES: I hate to do this, but I am going
13 to take two questions or thoughts and then we have to
14 stop. I think Kathryn's hand was up first.

15 Oh, yeah, you know what, that would not be
16 right. Phyllis has been waiting, and then we'll do
17 Kathryn.

18 MS. MONTGOMERY: All right.

19 MS. SPAETH: I'll be really quick.

20 I was just wondering -- and I know we've
21 discussed this, Mamie -- in light of the fact that all
22 new computers now come with internal cameras and
23 internal mics, what about using something like Skype?

24 MS. KRESSES: And that's a very good point that
25 we were going to get to, so I'm glad that you raised it.

1 And Kathryn?

2 MS. MONTGOMERY: Well, this is a very
3 interesting discussion, and whenever we go down this
4 road, I start getting the heebie-jeebies, I have to tell
5 you. As a parent and as a privacy advocate, a lot of
6 these solutions sound like they may, you know, raise
7 more problems, and some people have, you know, raised
8 that question as well.

9 I want to ask a couple questions. One, you
10 know, we know these methods are imprecise, you know,
11 faulty. From the beginning, we knew that. Has there
12 been any assessment of how they're being used, how
13 effectively they're being used, what works and what
14 doesn't work? And I had to step out for a few minutes,
15 so if you've addressed it, I apologize.

16 And secondly, you know, to what extent are
17 parents opting in to things they don't fully understand?
18 And because one of my concerns is that these methods --
19 that everybody is focusing on these methods in order to,
20 you know, maximize data collection, and I want to ensure
21 that the principle of minimizing data collection is
22 adhered to here and the focus on marketing safeguards
23 for children.

24 MS. KRESSES: And those are good questions, and,
25 you know, we don't have any data on that, and we can't

1 really answer this second, but these -- you know, again,
2 I mean, I think a lot of good thoughts have been raised
3 from a policy perspective, a technology perspective, and
4 a parental acceptance, and other things. So, I
5 really -- again, as in every panel, we urge you to
6 comment from any of those perspectives, and, you know,
7 if you know of others that should be commenting, to get
8 the word out.

9 So, we're going to end this panel and move on to
10 Panel Five. Thank you.

11 (Applause.)

12 (Brief recess.)

13 MS. MARCUS: I really thank everybody for
14 hanging in there with us. This has been an enormously
15 substantive day, and I know that it's a lot to wrap your
16 heads around. Mamie and I often joke that COPPA is
17 Talmudic in its complexity, so we have dealt with a lot
18 of brain-benders today and we will deal with just a few
19 more as we talk about COPPA's exceptions to parental
20 consent.

21 I'd like to introduce our panelists.

22 On your left is Parry Aftab, the Executive
23 Director of Wiredsafety.org.

24 Next to her is Izzy Neis, the Director of User
25 Engagement for Gazillion Entertainment.

1 Then Dona Fraser, the Director of Privacy Online
2 for the Entertainment Software Rating Board.

3 Mamie is directly next to me.

4 To your right, Susan Linn, the Director for the
5 Campaign for a Commercial-Free Childhood.

6 Then John Smedley, the President of Sony Online
7 Entertainment.

8 Roz Kitchen, Partner at Cohen Silverman Rowan.

9 And finally, Peter Maude, Chief Technology
10 Officer for Crisp Thinking.

11 In this panel, we are going to talk about
12 COPPA's exceptions for parental consent, which were
13 actually built into the statute. I am going to put an
14 enormously densely-worded slide up. You do not need to
15 memorize it or read it now. I am small enough that I
16 think I am not blocking the little bit of language at
17 the bottom, and you also have it in your packet.

18 But suffice it to say that there are some
19 exceptions built into the statute where the requirement
20 of prior parental consent would not come into play,
21 primarily for an operator's collection of a child's
22 online contact information. And just as a reminder, the
23 Rule defines online contact information both as an email
24 address, an IM identifier, or -- I don't have the slide
25 in front of me -- it would be other means to connect a

1 child online, but not as expansive necessarily as we
2 were talking this afternoon about personal information.

3 I'd like to start with a basic question for
4 those of us at the table -- myself excluded, actually --
5 who were there at the beginning of COPPA as to why
6 Congress built in any exceptions to verifiable parental
7 consent.

8 Parry?

9 MS. AFTAB: Okay. When it comes to the oldest
10 person at the panel, I tend to fit there. So, we were
11 there in the very beginning of when COPPA became law and
12 when the FTC said if you don't listen, we're going to
13 make a law, and everyone said yeah and didn't listen, so
14 they made a law.

15 We need to understand that in the beginning, it
16 came out against marketing. It all started with
17 kidscom.com and then the CME letter that Kathryn's
18 talked about, and it was all about marketing. What
19 information are you collecting from kids? How are you
20 using it? How are parents engaged? What do they know
21 about what you're doing?

22 During the process, however, it also became
23 about safety, and because the FTC has dual prong, both
24 consumer protection and safety jurisdiction, it became
25 about protecting children from sexual predators. And

1 you have to remember, we're talking about 1997, 1998.
2 That was what everything was about on the Internet.
3 Everyone was afraid that their children would be
4 abducted immediately if they met anyone on the Internet.

5 So, as they started looking at what we can do,
6 we recognized that we wanted to protect children from
7 giving away too much personal information online and
8 communicating with Internet sexual predators, who would
9 immediately come to their house and abduct them, and an
10 awful lot of that had to do with offline contact
11 information. Where do you live? How can I find you?
12 How will I find you on the street and grab you and steal
13 you? And so a lot of it came from there.

14 At the same time, we recognized that if we were
15 going to get parents involved in whatever was going on
16 and try to get their consent or notify them, we had to
17 reach them, and we were concerned that any other way
18 wouldn't reach the parents unless we did them through
19 the kids. So, we had the ability of the sites to
20 collect certain kinds of information for certain limited
21 purposes and deal with it in that way, and at the same
22 time, we were protecting children from sharing offline
23 information.

24 We further recognized that there was a need for
25 the sites to protect themselves -- the security of the

1 sites themselves, the safety of the children while they
2 were there -- and if parents weren't giving consent, did
3 that mean that these children would be lost forever in
4 cyberspace? And so as we looked at the exceptions, it
5 was you don't have to get prior consent, you can keep it
6 under certain circumstances, and here, more than any
7 other place, you will see that you deal with use, not
8 information.

9 So, although we deal with offline contact
10 information there, a large part of it is, how are you
11 using the information you have? And so we see more of
12 that in this section than you do in others. So, it was
13 very practical and fear-based as we were doing that.

14 Now we recognize cyberbullies are kids who go to
15 the kid's school and they know where you are all the
16 time. There is less of a concern about Internet sexual
17 predators -- serious risk, but not as prevalent as
18 others -- and I think that sometimes the exceptions are
19 eating the Rule.

20 MS. MARCUS: Okay, and we will definitely
21 discuss that in this hour together.

22 Dona, do you agree or is there something you
23 would like to add?

24 MS. FRASER: No, I agree. I think, in addition,
25 Congress I think did not want to unintentionally

1 interfere with a child's ability to enjoy the Internet
2 as well as be able to access timely information, either
3 from their schools or libraries or things like that.
4 So, I think there was certain consideration given to
5 that as well.

6 MS. MARCUS: Kathryn or Angela, what do you guys
7 think?

8 MS. MONTGOMERY: Oh, thank you, I am sitting
9 here trying to remember it all. I don't remember in our
10 discussion so much of a focus on safety. You know,
11 Parry's right, that was the kind of era that we were in.
12 There was a lot of public debate about it, and COPPA got
13 discussed in that context, but as I recall, it was to
14 try to create some balance between ensuring an online
15 experience for young people that would allow them to
16 interact and enjoy and be online, but to do it in a way
17 that circumscribed the ability of online marketers to
18 effectively target them and to maintain ongoing
19 communication with them.

20 So, I remember examples -- and, Angela, you can
21 correct me if you remember it differently -- but I can
22 remember discussions about creating an online
23 newsletter, for example, that you would like to be able
24 to have them get and could we do that. My concern was
25 always, is that an online newsletter that's basically a

1 marketing message that's going to come to them every day
2 or every week? But it was really framed more in the
3 context of educational content, informational content
4 and a good experience, and --

5 MS. AFTAB: But the chat part about posting
6 personal information had to do with -- predators.

7 MS. CAMPBELL: The chat was a kind of add-on.

8 MS. MONTGOMERY: And you're right, it was a set
9 of hopefully practical ways to deal with all of these
10 things.

11 MS. MARCUS: What I'm hearing is that, you know,
12 for a variety of reasons, the collection of online
13 contact information was seen as possibly slightly less
14 of a privacy concern in this context.

15 MS. MONTGOMERY: Yes, that's true.

16 MS. MARCUS: And I'm wondering if that's still
17 the case.

18 Susan?

19 MS. LINN: Well, I was struck by what Parry just
20 said, that what we found is that there's -- that sexual
21 predators are less of a concern.

22 MS. AFTAB: Not less of a concern. Less of a
23 overhyped concern.

24 MS. LINN: But no, you're right. No, I'm
25 supporting what you said, but I think that the converse

1 of that is that marketing to children has escalated just
2 exponentially on the Web, and that's really where the
3 primary harms are, and I think that we've hardly touched
4 on marketing today, really, and what we haven't talked
5 about are the harms of marketing to kids, and I think we
6 need to at least say that marketing -- research shows
7 that marketing is a factor in childhood obesity, eating
8 disorders, precocious sexuality, youth violence, the
9 erosion of creative play, which is the foundation of
10 learning, and also the acquisition of materialistic
11 values, the false notion that things we buy make us
12 happy, to say nothing of underage tobacco use and
13 alcohol use.

14 So, I think, you know, that I, you know, share
15 Kathryn's wish that children have a nice, happy, fun,
16 productive, educational time online, but I really think
17 we have to deal with the marketing.

18 MS. MARCUS: Roz, what do you think?

19 MS. KITCHEN: I honestly disagree with Susan,
20 because I think that generally as COPPA has evolved and
21 more and more responsible companies are reading the
22 statute and thinking, "oh, my gosh, what do I have to
23 do?" they're tending to take a step back and saying,
24 "you know, we might have a couple of kids' products out
25 there, but we're not -- our target audience is not the

1 child. It's the mom who's going to the store and buying
2 it or dad who's going to the store and buying it."

3 And so they are -- from what I've gathered and
4 from my clients, I'm seeing less of a push to market to
5 the under 13s, more of a push to market to their parents
6 for sure, and a lot more responsible -- you know, the
7 companies that are sending people here today, the
8 companies that pay for me and other people to represent
9 them, they are the ones that are kind of making sure
10 that they've complied, because they are a direct
11 children's website or they are directly involved only
12 with that space in the marketplace, so they have to
13 market to children, there's no way around it, or they're
14 saying we really don't have to do this by virtue of the
15 products, the information, the services that we offer.
16 So, they're taking a step back.

17 MS. MARCUS: Dona, are these exceptions widely
18 used?

19 MS. FRASER: I think that they are. I think
20 primarily you're probably looking at the ability to
21 obtain verifiable parental consent, and the one-time use
22 for the companies that we deal with, those are the ones
23 that I think they are mostly used.

24 MS. MARCUS: And the one-time use, we
25 affectionately call it the "one-time use exception," it

1 is number 2 on the screen behind me, which permits the
2 collection of online contact information for the sole
3 purpose of responding directly to the child one time.
4 The information is not to be used to recontact the
5 child, and it's to be deleted by the operator
6 immediately thereafter. So, you see the use of the
7 one-time use exception in your experience?

8 MS. FRASER: Right. I think you're looking at
9 the password reset, you're looking at tech help, you're
10 looking at send-a-friend thing, those types of things,
11 one-time use.

12 MS. MARCUS: Roz?

13 MS. KITCHEN: "Why don't you offer this product
14 in green? I really like green. "

15 MS. MARCUS: But in addition to the one-time
16 inquiry by a child, what about what we call the
17 "multiple-use exception," which is number 3 and the most
18 densely worded of the exceptions? Do you see a lot of
19 use?

20 This permits an operator to collect the online
21 contact information from a child to be able to
22 communicate with that child more than once, but
23 immediately after communicating with the child the first
24 time, the operator has to send the parent an opt-out
25 notice.

1 Roz, do you see the multiple-use exception?

2 MS. KITCHEN: Initially in the promotions
3 industry, this exception was being used quite widely
4 with regard to sweepstakes entries, but more and more,
5 as we've kind of moved towards the collection of
6 user-generated content in connection with a contest, for
7 example, we're not -- you really don't fall within the
8 exception. So, if you're being responsible and you're
9 reading the statute fairly narrowly -- and you guys know
10 I take a fairly conservative position, especially with
11 regards to sweepstakes and contests -- but when you're
12 talking about children's entry into that, what
13 information they had to provide, this online contact
14 information, which can't be used for any other purpose,
15 well, if you're in connection with a contest and you're
16 collecting user-generated content, that perhaps you're
17 putting a video on a website where they have
18 identifiable features in that video, it's more than
19 online contact information, and the marketer isn't going
20 to go to the trouble of doing all of this if they can
21 only use it in connection with that contest. They may
22 want to go beyond that, and if they've got -- you know,
23 so they'll take other steps to get parental consent
24 without falling under this exception, is the things that
25 I am seeing.

1 MS. MARCUS: What about Kathryn's example of
2 newsletters, an ongoing communication with the child?

3 MS. AFTAB: That's where we're seeing it used
4 most often, is newsletters, e-news, alerts, new
5 products, information about a new feature on the site,
6 something really cool that's come out, and so we see
7 that repeated newsletter or notices to the kids at the
8 site.

9 MS. KITCHEN: Signing up for a catalog, consent
10 to a catalog.

11 MS. AFTAB: An online catalog, sales, that kind
12 of thing, new offerings in virtual worlds. Now you can
13 buy a new tractor, now you can buy a new fish, now you
14 can go to outer space.

15 MS. MARCUS: Izzy, what's your experience?

16 MR. NEIS: I'm pretty well immersed in the
17 industry in general for kids. I have my email all over
18 the place, like logging in as a child, because I want to
19 watch how safety is used in practice, in follow-up. For
20 the most part, I am not as concerned about the
21 collection of this kind of data for companies that are
22 built for kids, because they understand these
23 limitations. They're following the rules for the most
24 part, and if they don't, they usually get their hand
25 slapped relatively quickly, because everybody is very

1 concerned about making sure we stay with safety.

2 Where the concern comes with marketing-type
3 collection of data isn't so much in this process. It's
4 more what everybody has been talking about all day long
5 about data mining and all of that, and that doesn't have
6 necessarily anything to do with this directly, what
7 we're talking about at this time. So, getting off on
8 that tangent probably isn't ideal for this conversation.

9 But for the most part, everybody is dealing with
10 newsletters, alerts, just as Parry said, 1V1 email
11 contact, so it's basically customer service stuff, like
12 "I lost my potion. Where is my potion?" You know, you
13 tell the child, "Well, here's your potion," that kind of
14 stuff, or whatever game they're playing.

15 MS. MONTGOMERY: Can I ask a question, because I
16 wanted to know how this all turned out?

17 So, am I hearing you correctly that kids are
18 being targeted then with email communications for
19 products and with advertising?

20 MS. NEIS: No, because of the --

21 MS. MONTGOMERY: I'm asking Parry, actually.

22 MS. AFTAB: I wasn't sure. What will happen
23 is -- well, yeah, I don't know that it's targeting
24 specific kids. It's targeting all kids. So, if you are
25 not XYZ Virtual World and they have a new character that

1 you can now earn, they'll say there's a new character
2 out there, and you're going to have to earn 2000 points
3 or you'll have to do that, or there's a new section of
4 the world that has these new things that you can engage
5 with.

6 What we're seeing as the multiple-use exception
7 is it's the constant communication about the world,
8 about opportunities, about newsletters, about alerts,
9 about a whole bunch of different things. It's not
10 profile targeting to kids in that specific instance. It
11 is information that's out there about anything new
12 that's happening at the site.

13 MS. MONTGOMERY: I want to follow up.

14 MS. MARCUS: Hold on, Kathryn.

15 MS. MONTGOMERY: I just want to --

16 MS. MARCUS: Well, wait. We are definitely
17 going to get to misuse. That's my next question.

18 MS. MONTGOMERY: I worry that these will create
19 some loopholes.

20 MS. MARCUS: Okay. Well, we're getting there.

21 Guillermo?

22 MR. ROSCHKE: Yes. I have a question about the
23 newsletter issue as well, and I'm wondering if people
24 have more information on how they work. My
25 understanding is most of email newsletter services

1 actually track whether the emails have been read. They
2 track what links people are clicking on. Would that
3 information collection stay under the exception of, you
4 know, here, this exception is only for online contact
5 information. That means that I shouldn't be allowed to
6 track whether the email has been read and whether any
7 links have been clicked on from the email. Is that
8 correct?

9 MS. MARCUS: Maybe. Maybe not.

10 MR. NEIS: From an operator's perspective, it's
11 very hard to narrow down to an individual which
12 person -- it's kind of costly to be like, okay, I sent
13 out 30,000 emails to the people who opt in to the email,
14 and now I'm going to track down to this one person to
15 see if they've opened up the links. It's timely and not
16 necessary. You don't really see that happening in
17 operations.

18 MS. MARCUS: Dona, let's talk about misuse. Is
19 this what -- you know, what your interpretation of this
20 narrow exception is?

21 MS. FRASER: I think that you have companies
22 that are -- oh, thanks. I think that you have companies
23 who are collecting the information and using it in ways
24 that clearly are not intended and are not giving the
25 parents notice, they are not giving them opt-in or

1 opt-out consent, and it may be -- I don't know, I don't
2 see Denise -- oh, there she is, okay. She and I have
3 talked about this on multiple occasions. I am going to
4 use the example that we've talked about, which is a
5 company that sends out a birthday notice email, and
6 they're collecting the email address simply to notify
7 you on your birthday. The next thing you know -- which
8 only should be one time a year, but now, the next thing
9 you know, you're receiving ten emails in the matter of
10 two months.

11 So, those types of things are happening, where
12 there's no disclosure of that information, where there's
13 no -- they have not allowed -- they have not told you
14 from the outset what they are going to do with that
15 information. They have only told you this is simply for
16 a birthday club or a birthday newsletter.

17 MS. TAYLOE: Which, technically, adding the data
18 for -- technically, adding data for -- to the email --
19 so, if you are going to use notice and opt-out, you are
20 supposed to have first name and email address. When you
21 add a date of birth, you have added a piece of
22 information that are you aggregating against that, that
23 should step you up to email-plus. If it stepped up to
24 email-plus, then they could ask permission to have this
25 sort of interaction, but instead, they are using notice

1 and opt-out in place of email-plus and adding this other
2 data.

3 And the other big one is user name and password
4 against an email address. The email is for newsletters,
5 but the user name and password is gathering points and
6 likes and dislikes. So, it's not that every kid gets
7 the exact same newsletter. They get something tailored
8 based on when they were last in that game or how many
9 points they might have or what they can do, so...

10 MS. FRASER: Right, and I think that -- I mean,
11 there are companies who are obviously using deceptive
12 practices. Whether or not it's an intentional act I
13 think is -- we don't really know unless we're dealing
14 with those companies specifically. There are some
15 companies who are just not aware of the law.

16 MS. MARCUS: Just not aware of the law or
17 perhaps reading this exception more broadly than it was
18 intended?

19 MS. FRASER: I think it's both.

20 MS. AFTAB: I think lots of confusion. They get
21 them all mixed up.

22 MS. TAYLOE: And copycatting. They go steal the
23 privacy policy from the other site. It's a big site
24 that sometimes gets it wrong. You guys have nailed a
25 couple big brands, right, that have big fancy lawyers,

1 and then other little companies are following them
2 saying, "Well, they do it so I should do it," but they
3 don't understand that, you know, Club Penguin actually
4 does a really good job of deleting a whole ton of data
5 that you type on one end that doesn't show on the other,
6 but the little new site that looks at it says, "Well,
7 they're using email-plus, so I can use email-plus, even
8 though I have a black list, not a white list." It's
9 copycatting from bigger companies.

10 MS. AFTAB: Most of them have no idea what
11 they're doing with information. They really don't
12 have -- they haven't mapped data, haven't mapped
13 information, and that's part of the problem. They think
14 it's just a newsletter, and they haven't thought it all
15 through, and that's a big problem. Big companies and
16 small companies alike.

17 MS. FRASER: I think because they don't know
18 they have to, honestly. I think there are some people
19 who are ignorant to the fact that this law even exists.

20 MS. KITCHEN: And I would also say, too, that a
21 lot of big companies rely on third-party vendors to
22 provide this service, and they're huge companies relying
23 on these little tiny vendors that don't go get the big
24 fancy lawyers or -- you know, and so it's kind of this
25 trickle-down effect of nobody knows what anybody else is

1 doing, and everybody thinks, well, because they're
2 so-and-so, they must know, but they're relying --

3 MS. AFTAB: And games and virtual worlds have
4 changed everything.

5 MS. KITCHEN: They really have.

6 MS. MARCUS: Susan, what do you think?

7 MS. LINN: The multiple-use exception is the one
8 that really troubles me the most of all of these
9 exceptions, and it troubles me for lots of reasons, and
10 one of them -- I'd like to go back to cell phones and
11 texting and the fact that kids are contacting these
12 companies. I mean, these companies -- like McDonald's,
13 for instance, had a text McFlurry campaign, and kids are
14 being encouraged to text just about everywhere they
15 look. So, they're contacting these companies. The
16 companies are getting back to them. Then they can keep
17 doing that or they can keep, you know, going back
18 without getting parental permission.

19 That's really, really troubling to me, because
20 the parents aren't going to have any idea of what's
21 going on. Once a child has a cell phone, there is no
22 way that the parents can know what that child's doing on
23 the phone. It's really -- I mean, it's really, really
24 difficult. So, once we get to mobile marketing, I think
25 that some of these loopholes and exceptions really need

1 to be closed, and that's the one that troubles me the
2 most.

3 MS. NIEJADLIK: I'm not sure if many folks know,
4 and I have no idea what the McFlurry campaign was -- can
5 you hear me? Okay.

6 When they create those sorts of campaigns, what
7 they are doing is they are doing it through a short
8 code, and so McFlurry is something that has been
9 assigned to McDonald's in that particular case, and
10 Haiti is another example that the Red Cross used when
11 there was the disaster in Haiti, et cetera, et cetera.
12 And in order to get a short code, which is the entire
13 way our company operates, you have to go specifically
14 request through the carriers, you have to submit a
15 campaign, and you have to say exactly what it is you're
16 going to do, and they specifically approve that one
17 thing, and you don't get to use that short code for
18 anything else. So, just a tidbit of information. I
19 mean, presumably --

20 MS. LINN: They don't get the child's cell phone
21 number or they can't contact the child again or --

22 MS. TAYLOE: Yes. You get -- I mean, when we
23 have a parent hit a short code back to create their
24 parent account, we get the cell phone number and the
25 carrier that it came from. So, is that typical? I

1 don't know if that's typical.

2 MS. NIEJADLIK: You have to receive that as part
3 of receiving the message, but there is an organization
4 called the MMA, which is the Mobile Marketing
5 Association, and they have rules against what you're
6 able to do with respect to SMS'ing people, and you can't
7 just randomly SMS them with marketing messages. You are
8 not allowed to do that. So, if somebody is doing that
9 in a short code, they are violating the rules, and they
10 can have the short code turned off.

11 MS. TAYLOE: Can you take the cell phone number?
12 Is there a rule against taking the number that you
13 receive and doing a data lookup, at Targets or Axiom or
14 Equifax or any of the other guys that have the cell
15 phone -- every time we make a purchase online and we
16 give them our cell phone, that data now goes to Axiom
17 who has 300 million of us sitting in their database, and
18 you can -- marketers can legitimately submit a cell
19 phone or submit a phone and get back the data that's
20 associated to it if it exists. Are there rules about
21 that, do you know?

22 MS. NIEJADLIK: I would have to check on that
23 specifically. Most of what we do is a response to our
24 own message and not just inbound, you know, receipt
25 randomly of messages.

1 MS. TAYLOE: Right.

2 MS. MARCUS: So, okay, we could go on this
3 thread for a while, but I want to get back to the
4 exceptions themselves, and what I'm hearing in the room
5 is that this multiple-use exception should be read very,
6 very narrowly. Do I see some assent on that? And
7 that -- and if people disagree, I would like to hear
8 that, but what I've been hearing from people is that it
9 should be read strictly to include only a child's online
10 contact information. So, if we're getting some other
11 piece of personal information from a child, for example,
12 their cell phone, that would be outside of this
13 exception at the outset.

14 Is there someone in the back?

15 UNIDENTIFIED SPEAKER: Yeah. I don't disagree
16 with that interpretation at all. What I think is
17 interesting is you can look at this as an exception or a
18 loophole that's being misused or you can kind of look at
19 this as being kind of almost like a lower verifiable
20 parental consent method, because it has this opt-out
21 requirement.

22 So, it might be interesting to think about this,
23 instead of them being misused, maybe -- or maybe
24 people -- instead of looking at this as people are
25 trying to rely on the exceptions too much, maybe this is

1 a reason for why we should expand the list of approved
2 parental consent methods and provide more granularity,
3 like maybe email-plus filtering or email-plus parental
4 controls, so that people go outside of relying on these
5 exceptions and go more the parental consent realm.

6 MS. MARCUS: I would say yes, but in this
7 instance, these exceptions were set forth by Congress,
8 so this is not a change that we could make here at the
9 Commission level. They were carved into the statute
10 themselves.

11 MS. KRESSES: You know, if that's a comment
12 that -- if people want to comment on added uses in this
13 regard, certainly they should do it, and if people want
14 to comment on, you know, restricting it, certainly they
15 should do it, because everything is open for discussion.

16 MS. MARCUS: And one last question for the
17 people on the panel with respect to this, is it possible
18 that what marketers and other operators thought was that
19 they could build, on top of the collection of online
20 contact information, other items of information that are
21 not considered personal under the Rule? So that perhaps
22 there was a misunderstanding, that they could collect
23 zip code, for example, which is not enumerated as
24 personal, and they could put that on top of online
25 contact information and then personalize a message to a

1 child and wouldn't run afoul of COPPA?

2 MS. AFTAB: Yeah, and, Phyllis, that's what I
3 see often enough, with even sophisticated people, they
4 think that they can do this because it's nonpersonally
5 identifiable on other things and it's attached to the
6 email. What we need to remind them is it's like the
7 Midas touch. You have got personally identifiable
8 information, you touch anything else, it becomes gold,
9 and they don't understand that, and that's been part of
10 the problem.

11 But they think it's okay that I understand that
12 this child likes baseball and this child has this
13 account and other things, because I'm only asking for
14 this piece of personally identifiable information. I
15 see that 80 percent of the time when I find problems.

16 MS. LINN: I think that's a really good point,
17 Parry, because one of the things that is concerning is
18 that younger and younger children are engaged in virtual
19 worlds where you bring a lot of yourself into the world,
20 and so these companies are getting lots and lots of
21 information about children's preferences, and, I mean,
22 it's really troubling, that information combined with
23 whatever personal information that they're allowed to
24 have, and that's concerning. They learn a lot about
25 these kids.

1 MS. MARCUS: So, I would like to move on to
2 another very hot topic, which is that of chat, and it
3 seems that chat in kids' spaces has become an
4 increasingly popular feature and with many sites
5 offering some format of filtered chat.

6 I'd like to talk about how children's sites that
7 offer chat are handling the parental consent process,
8 and I'll start, John, with you.

9 MR. SMEDLEY: So, I'm from Sony Online. We make
10 a game called Free Realms. We have had just about 12
11 million people come through, and probably 90 percent of
12 them are kids, and --

13 MS. MARCUS: Just to clarify, that's kids under
14 age 13?

15 MR. SMEDLEY: Yes. What we've found is that the
16 smartest thing to do is to use a white list chat method
17 and apply it to everybody. You simply cannot have a
18 really safe place where a 14-year-old and a 12-year-old
19 are going to have a conversation with open chat. It's
20 just -- I don't believe that's possible. I've been
21 making these games for, you know, 12 years now, and I've
22 got four kids under the age of 15, and, in fact, I've
23 been bitten a few times by a few sites. One of my
24 daughters got asked to be somebody's girlfriend, which I
25 was thrilled about, she was 11, so it was great.

1 It's a tough thing, because kids want to chat,
2 but there is no possible way to keep them safe without
3 doing some kind of a white list chat. They are smarter
4 than we are, and a black list chat simply doesn't work,
5 and we've seen both sides of this, and that's just
6 simply the conclusion we've come to.

7 MS. MARCUS: So, in your case, I'd like you to
8 describe what you mean by white list chat and then talk
9 about what Sony does on the parental consent process,
10 and before you do that, I just want to draw everyone's
11 attention to this slide.

12 Under the Rule, an operator would be deemed to
13 have collected information not just when they actively
14 collect information by requesting that a child submit
15 her information online, but also where an operator
16 enables a child to post her personal information; for
17 example, in a chat room or on a message board or by
18 other means. And then we have an exception: Except
19 where the operator deletes all personally identifiable
20 information from the postings by children before those
21 postings are made.

22 And so what that means is that when an operator
23 strips out personally identifiable information before it
24 goes live on a site, then that operator won't be deemed
25 to have collected that information. The information

1 will never have been disclosed to the public. And so
2 conceivably, in that case, an operator won't have had to
3 obtain parental content for that use if the operator
4 isn't collecting anything else.

5 And so what, John, you're describing is a white
6 list chat, and what is that exactly and do you have to
7 get parental content?

8 MR. SMEDLEY: So, our view is that you do not
9 have to get parental consent, because we're never in any
10 way, shape, or form letting a child give any kind of PII
11 whatsoever. So, we do not -- for example, our message
12 boards, we do not let under-13s post, period. We took
13 the safest approach. In our chat, you can only use
14 words that are preapproved. Does this make it really
15 messy and hard for kids to communicate? Yes. Do they
16 try to get around it? Yes. Are they successful? No.

17 And it's a constant battle, because they're
18 trying to come up with new ways, and you have to
19 constantly be trying to think ahead of what they are.
20 For example, oh, so let's not use numbers, so that
21 people can't communicate phone numbers. Well, you would
22 be amazed how many kids out there know Roman numerals.

23 MS. NEIS: Or fort fort high stick steven, ate,
24 A-T-E.

25 MR. SMEDLEY: Exactly. You constantly get into

1 this -- it's a never-ending battle, but we decided that
2 the right way to fight is simply not to let kids chat.
3 They are basically picking from a preapproved list of
4 words, period, and we're making it that simple, and
5 we're applying -- because this game is directly designed
6 for young kids, we have made the choice that we don't
7 want older kids to be able to communicate with the
8 younger kids in any kind of, you know, really easy
9 manner.

10 MS. MARCUS: Peter, what's your experience here?

11 MR. MAUDE: I think, you know, our experience is
12 that the white list gives you that better protection,
13 but, you know, there are ways around it, and the
14 examples we have just been giving, sticks having to give
15 out numbers. If I give you two communication tokens, a
16 one and a zero, I can give out personal information. I
17 mean, it takes a lot to get around it, and there is no
18 way that can end up in the marketing database, right,
19 but it goes out. So, we need to except where the
20 limitations -- if we are going to have communication,
21 the smart kids are going to find ways around it.

22 MS. MARCUS: What's the difference between a
23 white list and a black list?

24 MR. MAUDE: The white list is a preapproved
25 list. So, it's safer because you can't give out street

1 name, right, because it's not on the list. So, I can't
2 say it's the intersection of Chestnut and High, Balsam
3 and Fillmore, right, because those words wouldn't be in
4 the preapproved white list.

5 Now, there are ways around that. Salt Lake City
6 is a great example, okay? You can describe Salt Lake
7 City in words that are on the white list, but it takes
8 some doing. So, we think that the kind of white list
9 approach is safer, but there is no panacea in the sense
10 of absolutely eliminating personal information from your
11 chat.

12 MR. NEIS: There's a lot of different ways of
13 doing it. White list is a good example. There is also
14 ways of kind of managing almost a black list/white list
15 approach as well. You can have dictionary chat. The
16 point is you have to understand what's in your lists.
17 You have to have a full grasp of what you're providing
18 for your community, because, like, some of the issues
19 I've come across, say you have a sports site for kids,
20 and what the operators of that sports site don't
21 understand is numbers equate all sorts of varieties of
22 PII, like you may say, "Okay, well, you know, three
23 digits," and three digits in a sentence is fine, because
24 those three digits don't equate a phone number. All you
25 have to say is, "Hey, my digits are 815," enter that,

1 then have another one go through, "455," enter that, and
2 then finish off the -- there's tons of ways around it.
3 It's just being smart.

4 Now, aside from disallowing kids straight off
5 the bat, there are other Jedi mind tricks, if you will,
6 of allowing kids to feel like maybe they're not as
7 frustrated, because the problem that we have as
8 operators for kids' sites is kids get frustrated, so
9 they see a word redDED out and they can't type it
10 anymore and they're mad, right? So, what are they going
11 to do? They are going to phonetically spell it out.
12 And, man, I can give you tons and tons and tons and tons
13 of examples for that. It becomes a nightmare, and it
14 becomes a nightmare for your list to manage.

15 There are other ways to allowing the user to
16 think that they said it. So, they type what they are
17 trying to say; maybe they see it but no one else in the
18 room sees it. I mean, if you have been to Club Penguin,
19 this is just my guess, about 60 percent of what you
20 think you're typing no one else can see. And that's not
21 educationally fantastic, because kids are like, well,
22 you know, they think they can say it, they think they
23 can say it anywhere, but the grander problem is kids
24 don't understand why they can't tell you -- like, they
25 grew up knowing their basics, right? You have to know

1 your phone number to -- you know, if you ever get lost.
2 You have to know these things, very -- they hold their
3 personality very, you know, close to them. So, if
4 they're in a world, sharing any information about
5 themselves is kind of exciting, you know? So, how do
6 you protect them?

7 If you say to a kid, "Okay, so I'm going to
8 black list or I'm going to not allow the word 'Street,'"
9 and they're trying to say, "I want to go -- let's go to
10 Main Street," which is maybe a room in the world, that
11 becomes very frustrating if they get a pop-up message
12 that says, "That language is not allowed. You're on 30
13 minutes silence." They are like "Aaah, that's not fun."

14 So, how do you allow them to feel that way? And
15 that's why some sites, like, say, Club Penguin, allow
16 the Jedi mind trick of the author saying it, no one else
17 in the world says it, have post-talk moderation tools on
18 the back end that find that, and then you as an operator
19 of the site can then decide, is this child innocently
20 trying to talk about something or is this somebody who's
21 trying to get personal information out of children,
22 because if that person then broke your TUS, get them out
23 of your world. So, sorry, my little tangent there.

24 MS. MARCUS: Dona, I want to -- you know, we
25 have this very strict requirement, and, you know, the

1 Rule says what the Rule says, and unless all information
2 is prestripped, it is considered to be a collection, and
3 so what kind of rules of the road should we have at the
4 FTC and then what advice should we be giving, because we
5 get this question all the time about what formats of
6 chat are permissible, and, frankly, the questions come
7 from people who are trying to figure out if they can
8 offer chat without obtaining full-blown verifiable
9 parental consent, which, as we've discussed during the
10 day, is seen as somewhat of an obstacle to some fun,
11 enjoyment, and instantaneous enjoyment.

12 MS. FRASER: I think John has it right in
13 regards of what Free Realms is doing, you know, there is
14 no open chat. I think once you are engaging children in
15 open chat, you must get not just parental consent, you
16 know, plus you must get some form of heightened
17 verifiable parental consent, because you don't know what
18 kind of information is going to be exchanged or
19 disclosed, and if you're not monitoring that chat room,
20 if there's -- if you're not doing what Izzy was talking
21 about where you have somebody who's just typing in and
22 it's not popping up on the screen first and it's just
23 instantaneously going out there, then you must obtain
24 that verifiable parental consent.

25 MS. MARCUS: Peter, what do you think? I mean,

1 you know, we get a lot of questions from people who want
2 to know about automated systems and whether their
3 automated systems are good enough under COPPA.

4 MR. MAUDE: I think, you know, you can never
5 take people out of the equation. You can deal with the
6 scale, and our solutions help deal with the scale. I
7 think one of the issues is to not look at a very narrow,
8 is this line of content a problem? You need to look at
9 the person behind the content, and that's one of the
10 things that we do.

11 If you are constantly trying to get personal
12 information from people, your score as an information
13 threat will rise, and that means it brings it up onto
14 the radar of the moderators to say, why does this person
15 keep asking for personal information?

16 Again, another important point is to always take
17 what they intend to say and use that. Intent is so
18 important. You may be filtering it, but if they are
19 trying to get out personal information, you need to let
20 them know. So, even though it's -- even though it goes
21 red and no one gets to say it, we still look at that and
22 say, you know, "Stop doing this, stop giving out
23 personal information;" or if it's worse than that, we're
24 seeing profanities or cyberbullying, even though it's
25 not going through, the offensive, profane words, we

1 still say, "Hey, stop doing this, you know, you
2 shouldn't be talking to people in the world like that,"
3 even though it's not getting to...

4 MS. AFTAB: I think it's important, though, that
5 we separate the law from safety, and what you're talking
6 about is safety, and COPPA here has something very
7 specific. The question is, can the kid share personally
8 identifiable information through the use of technology?
9 And if you're using it with seven tabs down, white list
10 only, you're smart about what you do, you understand the
11 use of numbers and all of their symbols and all of their
12 code, in this case, they're not going to be able to
13 share personally identifiable information for the
14 purposes of COPPA.

15 The problem here is you've got white lists and
16 you've got white lists. So, a lot of people put them
17 together and think they're fine, and they are not high
18 quality, they don't understand what they're doing, and
19 the right ones that work for the purposes of making sure
20 kids can't share this stuff are old-time things that
21 have been out there for a really long time that kids
22 have tried to break forever. When you look at Neopets
23 and some of the older ones that are out there and
24 Toontown, the first time -- before COPPA, in 1998,
25 Toontown had a drop-down menu that I designed for

1 Disney, because we couldn't figure out anything better
2 in 1998.

3 So, the world has changed now, but we -- unless
4 we come up with standards on best practices on white
5 lists, on what parents are allowed to expect at a site,
6 we're in a lot of trouble.

7 MS. MARCUS: Roz, is there any room here for a
8 safe harbor situation? I mean, I'm definitely hearing
9 white lists as kind of the gold standard, but Peter
10 raised some other issues, some posting chat or live
11 moderated chat, which Izzy was talking about, too. Is
12 there a construct that we can use here where we can
13 check down a list and say, okay, or in these instances,
14 it's going to be good enough for now, but you have to
15 make your list or your filter better each night? What
16 do you think?

17 MS. KITCHEN: I don't know if I'm the best
18 person to answer that, I have to be honest, but -- I'm
19 going to -- I'm going to pass on that question.

20 MS. MARCUS: Okay.

21 Dona, what do you think?

22 MS. FRASER: I was going to go back to the point
23 we were making before in regards to engaging parents. I
24 think that we're leaving out the parent in this whole
25 process, and I think that if you are going to have a

1 site that's engaging children under 12 years old, you
2 have to engage a parent from the outset. I think
3 setting up parental controls the same way that we do in
4 an offline environment with handhelds, it can be used in
5 an online environment. That's what we advise our member
6 companies to do, is set up parental controls, so that
7 the only information that you're collecting from the
8 child at the beginning is the parents' email, and after
9 that, the entire account is set up by the parents.

10 MS. MARCUS: We have this kind of strange
11 situation that I think Shai was pointing out during the
12 last panel, which is sites that don't have to collect
13 information from the child about the parent, but are
14 choosing to contact a parent and notify them. How does
15 that fall within COPPA's --

16 MS. AFTAB: Good policy.

17 MS. MARCUS: Well, it's good policy, but we end
18 up in this strange situation where the site might be
19 risking a COPPA violation because they're collecting the
20 parents' online information from the kid for a different
21 purpose.

22 MS. AFTAB: I wanted to stay on best practices,
23 if I could just answer that last question, and it's my
24 ad of the day. We have something called the Socially
25 Safe Seal, which is the first best practices seal that's

1 being offered, and a lot of the people in the room and a
2 lot of people not in the room have applied for it, and
3 we actually go out and audit the site, we look at the
4 white list, we look at the black list, we try to break
5 them, we check the training and vetting and
6 certification of moderators and their practices from
7 start to finish.

8 If they do that and they do it right, they get
9 the seal, and if there's a safe harbor, that's a great
10 standard that we can start looking at. Do they know
11 what they're doing? Can we trust them with our kids?
12 And if not, then they're going to have to go through
13 verifiable parental consent, and good luck. And I think
14 we need to start looking at that standard and find
15 others like it.

16 MS. MARCUS: I think that's -- is that Amy? Hi,
17 Amy.

18 MS. PRITCHARD: Hi, I'm Amy Pritchard. I'm an
19 attorney and also the CEO at Metaverse Mod Squad, and I
20 would say with our company, we have spent hundreds of
21 thousands of hours with these kids and have hundreds of
22 clients, and so I see -- what I'm worried about is the
23 "white list good, black list bad." It's case by case.

24 I have worked with horrible white lists, as
25 Parry pointed out, and I have worked with absolutely

1 ironclad black lists. So, I just want to go on record
2 as saying let's look at the filter itself and not the
3 label.

4 MS. MARCUS: This is a very hard standard for us
5 to apply, because what ends up happening is, you know,
6 1-800-Mamie and Phyllis, and then we're asked by
7 operators to --

8 MS. AFTAB: That's because you own the COPPA
9 site for the FTC.

10 MS. MARCUS: We're asked to assess a filter in a
11 chat room that we don't have enough information on. We
12 are not, you know, spending a hundred thousand hours
13 with kids in a room trying to figure out how to crack
14 it, and then everyone is pointing to some of the other
15 operators and saying that "they do it this way, why
16 can't we do it that way?"

17 So, I think my entire body of questions here is
18 aimed at trying to figure out if there are some
19 articulable rules that we can put out there with respect
20 to chat, which is this increasingly popular feature of
21 sites, that would help website operators but would not
22 obviate COPPA's original intent.

23 MR. NEIS: It is only going to get harder.

24 MS. AFTAB: And it's not a rule, it's a
25 combination of things, so that if you have got

1 premoderation, you are tracking reputation, you are
2 dealing with different things, you can find things
3 faster beforehand and you can stop them afterwards. So,
4 it's not -- it's as you were talking about, you know,
5 and I have a great deal of respect for you. If you have
6 got really well-trained moderators, you can deal with a
7 little bit less technology. If you don't, you need a
8 lot more technology, and it has to be updated. So, it's
9 kind of this flow, and at the end --

10 MS. PRITCHARD: We always need great technology.

11 MS. AFTAB: But you know what I'm talking about.

12 MS. PRITCHARD: And it is definitely a piece.

13 So, what I'm concerned about is a piece is going to be a
14 stand-alone, yes, good, or no, bad, and that's -- that's
15 where we get dangerous. And also, if we lock down chat
16 to -- let's say even just a drop-down list, because
17 let's face it, if you really want to prevent any PII,
18 it's no chat.

19 MR. NEIS: It's scripted, and that's when your
20 numbers go "whooo."

21 MS. PRITCHARD: And you know where our kids are
22 going to go? Our kids are going to go to World of
23 Warcraft.

24 MS. AFTAB: And Blizzard was here and we liked
25 them.

1 MS. PRITCHARD: My husband said this is why they
2 created skate parks, got the kids off the streets.

3 MS. MARCUS: I'd like to move now -- you guys
4 have given us a lot to think about, and I really will
5 encourage people in this room, and tell your friends,
6 you know, that we need to hear more on this point,
7 please, because I'm still, you know, hearing a
8 vacillation between a potential safe harbor system or
9 the ironclad Rule right now, but, you know, what Mamie
10 and I are pretty much telling people that are calling
11 now is "stay tuned, but, you know, right now we have got
12 this strict rule, and that's it, and unless you can
13 guarantee 100 percent stripping, 100 percent, we don't
14 have leeway within this Rule."

15 I'd like to move to the black listing of a
16 child's online contact information, because we get a lot
17 of questions from operators about that and where that
18 falls within one of the exceptions, and we've heard that
19 a strict interpretation of the Rule wouldn't permit
20 operators to retain a child's online contact information
21 for the purpose of preventing that child from
22 reregistering on a site; for example, when she's
23 underage.

24 Is this right or would exception 5 -- whoops, I
25 have got to move back to exception 5, which is the

1 safety -- is it exception 4 or exception 5? Exception
2 5, which permits the retention of child's name and
3 online contact information to protect the security or
4 integrity of a website or online service.

5 Would keeping a child's online contact
6 information fall within exception 5 if you are trying to
7 keep them off the site and keep your site secure from
8 underage participation?

9 MR. NEIS: It depends on the information
10 collected. I mean, a lot of the kids' sites these days
11 are going straight to email-plus, which is kind of the
12 parents' email -- assumed, right, we have to look at it,
13 that for the most part people hold it the way it should
14 be. So, if you're collecting a parent's information, I
15 mean, the child that's attached to that parent's
16 information is breaking the rules, and they've been
17 parent-verified through the click-through, you have to
18 be able to protect your overall audience, right?

19 For me this becomes more of a larger billing
20 question, too. It goes into the whole area of if you
21 have a paying member, you have to collect that
22 information, and it should be the parents' information,
23 right? So, there's a lot of variables in that one.

24 MS. AFTAB: I'm sorry. I think what it comes
25 down to, what's personal information? So, that IP

1 question, if IP information becomes personally
2 identifiable information for the purposes of this, we
3 are in a lot of trouble, because the sites are
4 collecting IP for security purposes, but they are not
5 keeping email addresses and names to protect the site
6 unless you have got a known hacker, a kid who is trying
7 to hurt somebody else.

8 MS. MARCUS: But theoretically, if we read
9 exception 5 this way, they could keep a child's online
10 contact information. Yes?

11 MS. TAYLOE: Yeah, but it doesn't do you a lot
12 of good, because you can't add date of birth to it, and
13 so you can't age out of it. I mean, isn't the issue
14 that I say I'm 11, here's my email address, submit, we
15 have to do the drop the cookie and all of that, and what
16 some of us are saying is, "Gee, it would be really nice
17 if the kid comes back tomorrow and gives us that same
18 email, we could say, 'Sorry, you need to now prove
19 yourself as an adult versus being able to change your
20 age,'" but we can't keep the date of birth against the
21 email.

22 MS. MARCUS: Well, sure. What's good for goose
23 is good for gander. So, you know, if we're reading
24 these narrowly, we have to read all of them narrowly.

25 Is anyone using exception 5?

1 MS. AFTAB: Yes. We use exception 5 when you
2 are dealing with kids who are trying to take down the
3 site, so kids who are gaming the site, security risks to
4 the site, kids who are trying to collect passwords from
5 other people, and that's where you're seeing it used,
6 really to protect the integrity of the site. And as we
7 know, our best hackers are sort of 8, but, you know,
8 they're out there and they're doing that. So, you're
9 seeing that there.

10 Four you're seeing when you're dealing with kids
11 who have indicated suicide or molestation issues, and
12 then the question is, do you have to notify the parents?
13 That's where we're seeing a lot of confusion. So, if a
14 kid -- and they do it at the age of six, seven, eight,
15 ten -- tell you that daddy's hurting them or they're
16 going to kill themselves or something, especially when
17 you have put them on hold for 30 minutes, now what do
18 you do to protect the safety of that child, because you
19 are required that you are using it only in a certain
20 way, and you have to have reasonable efforts to notify
21 the parent, and that's very confusing when you're
22 dealing with a high-risk situation.

23 MS. MARCUS: Some of these exceptions, I will
24 say, you know, you can get mired in them, and we scratch
25 our heads and say, "Gosh, why did we collectively say

1 that?"

2 And here's, you know, kind of a gimme:

3 Exception 3 provides for a parent to be notified by
4 postal mail. When we read this again -- I will say I
5 was not involved in drafting the Rule, and I said,
6 "What?" You know, postal mail? You know, now you've
7 collected a parent's or a child's home address on this.

8 Do operators use the postal address in order to
9 do the opt-out?

10 MS. KRESSES: None of you ever noticed that.

11 MS. MARCUS: Well, we can't hide from it
12 anymore. That's what I'll say. This is the grand
13 outing.

14 MS. MONTGOMERY: It includes postal mail.

15 MS. MARCUS: Methods to notify parents.

16 MS. MONTGOMERY: That was the olden days.

17 MS. KRESSES: That's what the question is. Is
18 there some reason that that was in there that we haven't
19 figured out?

20 MS. MARCUS: Dona, what do you think?

21 MS. FRASER: I think that if the initial contact
22 happens online, it should remain online. I think the
23 problem is that there's this -- you know, from the point
24 that you decide to put something in the mail and by the
25 time it gets there, the parent has forgotten. You are

1 going to think it's spam. You are going to throw it
2 out. I think once you're online, I think that's the way
3 to remain online. Whatever the initial contact was,
4 that's how it should remain.

5 MS. AFTAB: It came from the olden days where
6 the kids might have access at school and parents may not
7 have access at home, especially lower income and
8 disenfranchised people, and those things are -- I'm not
9 saying that they're fully over, but I think everybody
10 has connection to something electronic.

11 MS. MARCUS: I mean, it seemed curious to us,
12 because we started this entire conversation by saying
13 that online contact information was seen as having --
14 carrying less of a privacy risk, and then if you're
15 adding onto that a child's home address, that's a great
16 expansion of your information collection.

17 I think, unfortunately, we have got to wrap up
18 now. Thank you, guys. I mean, this is a good audience
19 for the end of the day, and we really, really thank you
20 for coming.

21 Should we do a little closing remarks? Okay, we
22 are not going to do the traditional closing remarks,
23 where we say, "In Panel One we heard this, and in Panel
24 Two we heard this," because all of you guys have been
25 here all day. I think we have gotten a tremendous

1 amount out of this.

2 The story isn't written yet. We have until June
3 30th to collect your feedback and then to start
4 seriously process it. Thank you, enjoy the rest of your
5 week, and good night.

6 (Applause.)

7 (Whereupon, at 5:13 p.m., the roundtable was
8 concluded.)

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

