

>> Jessica Rich: Okay. Everyone can sit down. So, welcome back after lunch. This is Panel Three. Is this too loud?

>> Male Speaker: No.

>> Jessica Rich: No. It's good. Okay, good. My name is Jessica Rich. I'm director director of the Bureau of Consumer Protection here at the FTC. And this is Michelle Rosenthal from the FTC's Division of Advertising Practices. We're going to co-moderate. So, this is the panel on personal information. As you all know, FTC issued its COPPA rule in 1999, which, as David previously note, now seems like the Dark Ages in the online world. As part of this rule review, we're examining the rule's definition of personal information. Does it still make sense? Certainly, the kinds of information that can be used to contact an individual -- I'm having some trouble with this mike -- got to make it [ inaudible ] -- okay -- have changed over the last 11 years. Companies are collecting, retaining, combining, using, and sharing data in ways we never could have anticipated a decade ago. The key question for us is, "What information permits the physical or online contacting of a child under 13?" During this panel, we'll focus on the definition of "personal information," both in the rule and the COPPA statute. As you may know, when promulgating the rule, we did not stray far from the definition in the statute. And as shown on the screen -- and I think each of you has a handout -- the COPPA rule currently includes in its definition the following pieces of data. First and last name, home or other physical address, including state name and name of a city or town, e-mail address or a screen name that reveals an individual's e-mail address, telephone number, Social Security number, persistent identifier if it's associated with individually identifiable information, or a combination of last name or photograph with other information, if the combination permits physical online contacting, or information concerning a child or his parents that the website collects from the child online and combines with one of the identifiers we've already listed. In addition, Part "F" of the statute gives the FTC authority to include any other identifier that permits the physical or online contacting of a specific individual. So, the big question is, "What does it mean to contact a specific individual?" In the past couple of years, we've had some experience with the evolving nature of data and data use and personal information and

what that means in other contexts. In 2008 and 2009, we issued a report and a set of principles to address online behavioral advertising. In that context, which is the use of data to target personalized advertising, we said that the traditional dividing line between personally identifiable information -- PII -- and non-PII has become blurry and may not make sense anymore. Staring at the person who wrote that report. He's sitting right across from me. [ Light laughter ] That's because certain data, once thought to be anonymous, may no longer be so, due to technological changes. And just as important -- and this came up in some prior panels -- little bits of anonymous information, if pieced together, may actually become personally identifiable, once those pieces are put together. And we also... We held some recent round tables on commercial privacy writ large, not just about kids. And, there, we discussed the need to look at geolocation data and static IP addresses and consider how those -- you know, how identifiable those pieces of information are and how they implicate consumer privacy. And just a few months ago, we expressed some concern to Netflix, that the release of large amounts of consumer data that everyone thought was anonymous may actually be re-identifiable given the state of technology and the large quantities of available data that's out there. So I imagine, with this great group of panelists, these issues are going to come up today. And we want them to, but we need to remember and keep in mind that the particular context and focus here is children's online privacy and the concerns and objectives that led to passage of COPPA and the promulgation of the COPPA rule. So we want to keep bringing it back to that. So, let me briefly introduce our panelists. To my right, we have Maureen Cooney of TRUSTe, a COPPA safe harbor. We have Paul Ohm from the University of Colorado Law School. We have Sheila Millar from Keller and Heckman, Michelle over here, Kathryn Montgomery from American University, Matt Galligan from SimpleGeo company, Jules Polonetsky from the Future of Privacy Forum, and Heidi -- is it Sallow?

>> Heidi C. Salow: Salow.

>> Jessica Rich: Salow -- sorry -- from from DLA Piper. And Kathryn and Sheila, among others - - me too, actually -- have been members of the COPPA family from the very start. So they, along with Toby, who's still here -- and I'm sure many others of you can...

>> Kathryn C. Montgomery: Angela.

>> Jessica Rich: Oh, Angela. Can pipe...

>> Kathryn C. Montgomery: There she is.

>> Jessica Rich: Oh, yeah. There you are.

>> Angela Campbell: I'm here.

>> Jessica Rich: Can pipe up with a historical perspective when needed. So, let's get started. So, we talked about the language of COPPA and the rule and how -- and the personal identifiers that are in that now. So, speaking of historical context, maybe we can talk about how we originally identified those list of identifiers and what was the significance of those identifiers. Some of them are obvious. But, Kathryn, you want to take that?

>> Kathryn C. Montgomery: Sure. And it's really heartening to see, you know, 10 years later, how well we've done implementing this law and how robust it is. We were talking about words we weren't gonna use anymore. And we had a very granular discussion today. [ Light laughter ] And as we all know in Washington, when we talk about policy, the devil is in the details. You didn't have that on your list. [ Light laughter ] But, you know, it was a challenge to do all of this. I do want to remind people that -- and a couple of people have already mentioned it, maybe, including me -- that we created COPPA, and we advocates pushed for COPPA, because of concerns about digital marketing and about the need to ensure that there were some safeguards in the new digital marketing environment, which was in its earliest stages at that point. And even then, we could see that the business model that was governing most all of digital marketing at the time was called "one-to-one." It was the idea of personalized marketing messages, targeted at individuals. And children were one of the most powerful, most lucrative markets at the time, and there was an enormous amount of energy and innovation going into developing commercial applications aimed at children. So what we wanted was to ensure that there were some safeguards, based on long-term studies over a number of decades, that showed children simply didn't have the developmental capacities -- the cognitive capacities -- to deal with all of this and to respond to many of the

personal appeals, with marketers talking at the time about wanting to develop personalized ongoing relationships between product spokes-characters and children. That was the one comment in the trade conference -- trade-association conference -- that just kind of hit me. And, you know, it was an epiphany. And I realized, "Okay, we need to do something to ensure that there are safeguards." So, at the time, of course, children were mainly supplying information. There weren't any rules. It was like the Wild West. So they were being asked for all of this stuff. And so we wanted to specify specifically what kinds of information would enable marketers to communicate directly with them. But we were also very aware, at the time, that the so-called "passive" technological mechanisms for identifying children and for collecting information from them. At the time, I remember, one of the terms was "mouse droppings." That one seems to have gone by the way. But it really was a precursor. I know, that's pretty disgusting. But that was really a precursor to what we have now with cookies and other kinds of data-collection and tracking mechanisms. So, what we see now... And also the other thing I just want to add here, that nobody has really brought up, is that one of the goals of the law was to minimize data collection from children. And, often, that gets missed, and people don't realize that that was one of the intentions. So, we're now at a time when the industry has evolved, as everybody has been talking about, and I'm pleased that the language in the law is flexible enough to accommodate many of these new practices. So it's very good that we're having this conversation today.

>> Jessica Rich: So, does anyone... So, we have the lists. Is this one on?

>> Michelle Rosenthal: Yeah.

>> Jessica Rich: Okay? I seem to have trouble with the mike today. Okay.

>> Kathryn C. Montgomery: Oh, I thought we were sharing.

>> Jessica Rich: No, that's okay.

>> Kathryn C. Montgomery: You didn't want mine?

>> Jessica Rich: I'll share with her, too, on 3.

>> Kathryn C. Montgomery: Should I turn mine off?

>> Jessica Rich: Nice community here. So, we have a list of identifiers. Maybe we could...

Without trying to get too abstract here, maybe we could talk a little about why these identifiers are on this list, what characterizes them, which might help us to determine whether there's things left off the list or things that shouldn't be on the list anymore. Jules, do you want to talk a little about what it means to permit the online contacting of a specific individual and why these identifiers are on it. And then maybe we can talking about what else might fit those criteria.

>> Jules Polonetsky: Well, having still been in, I guess, city or state government at the time of COPPA, it's been a great experience to spend time, over the years, with Perry and to hear from Kathryn and some of the others who were so instrumental back with all of you at the commission. So, the history of why and how one picked these in those early days I'll leave to others, other than they, you know, obviously are sort of the most obvious subset of personal information. But I think what has happened over the years that has changed -- and I'm not sure this is something that easily fits into, you know, the COPPA structure. But what I think has dramatically changed over the years, I think, in the time that these identifiers were selected, these were the ways that, "A," you actually reached out and touched somebody and visited them and, you know, called them, visited their house, could contact them. And then the second real interesting thing that comes along with these sorts of things is they were the keys to all the other data that's available about people. And so, by having a name or an address or a phone number, the databases that are available for all the other robust marketing purposes can be brought in and queried. And if you didn't have any of those, it wasn't really easy to bring in all the other data that's out there online and offline. And I think what's happened on both those fronts -- the "Can I maintain a relationship with you and message to you?" or "Can I correlate lots of other information out there about you?" I think that's really dramatically changed. It was always theoretically possible, but today it's par for the course for information to be either de-identified or never actually identified. But given that a user may show up and authenticate somewhere to correlate the other data that's available about them -- appending it, throwing it over the wall, leaving it on a cookie, and being able to maintain that there's never been

any identification -- but yet the PII-connected data -- all the other lifestyle stuff, purchase activity, whatever it is -- can end up being available online. And, indeed, that's, you know, a significant part. Technically, folks don't call it behavioral. It's appending, it's adding data. It's not necessarily your clickstream, but it's adding data. And so, to the extent that that was intended to be the dividing line for PII or not, that's sort of long been crossed. You know, around the world, folks argue, "Well, therefore, it ought to be personal." I don't think we've gone that far in the U.S., but, clearly, the correlation of PII is no longer limited to PII. And then the second thing that's happened that has dramatically changed was, you couldn't easily maintain a relationship with somebody without them identifying themselves in various places online or offline and then correlating that. And, today, whether it's because of cookies, whether it's because of other identifiers, I can maintain that relationship. That wasn't that unique back then, but I think what's happened today is, I would have had to go to lots of places and separately, you know, try to interact with you. Today, because of ad exchanges and data exchanges, I can maintain state with one user across websites, across ad networks, across sometimes even devices and platforms. I don't see how easily, you know, we broaden the COPPA definition, because it breaks down on a lot of these other issues around actual knowledge, around being able to get consent. But it certainly raises a whole host of marketing issues that, you know, Kathryn just kind of put out there as what we wanted to deal with those. There is today a whole host of marketing issues that can happen quite discreetly, as well as maintaining a relationship and messaging the same person over lots of places, because of the way the technology and the data use has developed.

>> Jessica Rich: Okay, well, so, you've put together two basic things, which is maintain a relationship and correlating other data so that you can end up identifying somebody. Keeping those criteria in mind -- and people can add to that or dispute that -- what -- I'd love to hear ideas about other data. I have my own little list that I'm planning to get to. But better for the panelists to toss it out -- other data that might fit that criteria that aren't on this list.

>> Matt Galligan: Sure. So, I see three categories of data -- of identifiers -- and I break them down as exclusive, derivative, and additive. So, an exclusive identifier is something that, on its own, can identify an individual. That would be something like first name, last name, physical address, telephone number, Social Security number. Those are exclusive identifiers because, without any

other information, I can find out the individual. An additive identifier would be something like, with any one of those individual exclusive identifiers, or with multiple additive identifiers, I can find out an identity. So I can take... Let's just take geolocation, for example, which is something that is proposed. On its own, a coordinate doesn't necessarily speak to who somebody is. It might speak to where they are at that given time, but it also doesn't mean home or work. It could mean anything. It could mean the coffee shop down the street that they frequent. It could mean the park that they like to go to. But just a coordinate doesn't necessarily identify a specific individual. However, a coordinate attached to any one of these other categories could better identify an individual than even a physical address, because we're going beyond an address to something far more specific than an address. So, that's what I would consider an additive identifier. A derivative identifier is something we haven't discussed, which is using a third party to identify a person. So, Facebook Connect, for example. So, using Facebook Connect, I can, let's just say, log in using my Facebook identity, and it now generates an I.D. If I was a Web service, using Facebook Connect to identify my users, it generates an I.D. whenever I sign in. That I.D. can be called using something called FQL, Facebook Query Language. And by FQL, I can identify first name, last name, gender, date of birth, address, anything that has been allowed with an FQL. And that's not necessarily something that I own. I only own that I.D. But by using that I.D., I can correlate that with any other information that Facebook has on me. And the same could be said for any API that has personally identifiable information, be it Twitter, be it Google's I.D. service, any of that. But that's what I would consider a derivative identifier.

>> Jessica Rich: So, do all three classes of those fit the COPPA statute definition, which is "an identifier that permits the physical or online contacting of a specific individual" or a subset?

>> Matt Galligan: I think it just depends upon what each one of them is. I think "exclusive personal identifier" means that, without a doubt, it does allow for the contact, because you can find out anything else on that list. "Additive" would mean that you would have to have multiple sources to be able to get to that point, but you could potentially get to that point if you had multiple sources. Actually think derivative probably is almost up there with exclusive, because, most likely, that information exists and resides somewhere else, and you're able to correlate that with something else. But the additional problem with derivative is that you question whose responsibility is it at

that point. Who's falling under the COPPA rule? Is it the person that is collecting that identity, or is it the person that "owns that identity" -- meaning, the original service provider that actually has that information stored in their database.

>> Jessica Rich: Okay, so, does anyone else have comment on the way he's characterizing? Oh, lots. Paul?

>> Paul Ohm: And this is actually a comment on the way you're characterizing things. I mean, when I hear people talk about the COPPA family, I feel like I'm not quite a made man yet, because I'm coming to this with fresh eyes. [ Laughter ] But I think it helps me play the role of a judge looking at that statute without living and eating and sleeping it as a lot of you have. What I see, when I read this statute, is, I'm not sure that the language in "F," which is what you keep citing to, which permits the physical or online contacting, necessarily is the be-all and end-all of what the FTC is supposed to regulate. I mean, I understand that "F" is our guiding light, but the thing I would say is, if you look at the rest of the list and if you look at Social Security number in particular, I think there is a judicial argument that we can get some interpretive use out of why Congress included Social Security numbers in the list. Right? What is it about a Social Security number? I mean, there's obviously a lot of misinformation about how secure it is, how sensitive it is, what it can be used for. But the key attribute of a Social Security numbers is it's the key to linking lots of different databases together. Right? And so Congress, in its infinite wisdom, said, "When we're talking about permitting the physical and online contacting, we want to include Social Security numbers because they're in this list of types of information that are so linkable that we're gonna per se just add them to the list." And so I think linkability has to be part of the commission's charge here. I think the commission has to look at different types of information, and the commission has to ask itself, "How linkable is this particular type of information, given what we know about the state of data in the world, who holds data, the amounts of which they hold data?" And I know one of the reasons I was invited to be here is because I've done a lot of recent research in re-identification. I don't want to monopolize the microphone at this point, but I'm happy to throw out the proposition out there that the computer scientists have recently begun to kind of chip away at this entire construct -- this idea that some pieces of information are really, really, really linkable and some pieces of information are not terribly linkable and we could worry a lot less

about them. And if you're really aggressive about it -- and I've been accused of being aggressive in the past -- there are lots and lots and lots of pieces of information that are much more linkable than we ever realized, and much more linkable than we realized in 1999, certainly. So I'm happy to say lots more about that, but I'm gonna yield.

>> Heidi C. Salow: Jessica, this is Heidi. I'll just add one more thing. I like the way you characterized those three categories. And I think all three are actually encompassed already in the definition. We have -- I'm not sure if I'm gonna use the same terminology -- but the exclusive identifiers are obviously the individual data elements, right? We have additive in "F" and in "G," and then I think we also have -- what's the one, the reverse engineering?

>> Matt Galligan: Derivative.

>> Heidi C. Salow: Derivative. We have that, as well, I think, in "F" and "G," built in. So I would... And I also agree with the linkage issue. I would suggest that the way the definition is written now actually leaves open lots of room for the FTC to decide that there are other data elements out there that can allow a company or a website operator to contact a child without needing to even revisit. I think that you've got the flexibility here to, you know, get in line with technological developments, and I think that was probably intentional.

>> Jessica Rich: Okay, so...

>> Michelle Rosenthal: Jessica?

>> Jessica Rich: Oh.

>> Sheila A. Millar: I think that's right, and I also think that it's important, when we talk about any of these issues, that we keep in mind the greater construct of the statute, because we need to talk about website operators and online service providers and targeted to kids, directed to kids, or actual knowledge about kids. And the gray area, if you will, is in additive derivative area where you don't know. You might have an e-mail address of an individual. You have no idea that it's a child. But

if you've collected that at a kid-oriented website, then you have kids' data and you handle it appropriately. I think, to Kathryn's earlier point, one of the, I think, important things to remember about COPPA is that there was tremendous support by the business community for COPPA, many of whom were active members of CARU, as Phyllis mentioned, and who were living by many of these rules, not, obviously, in the same level of detail or enforceability, for a number of years before COPPA was adopted. And so, for those kids' sites, they've embraced COPPA, they live by COPPA, they understand that they're dealing with kids. And I think it gets harder when you alter the definition, particularly if you're gonna expand the universe and expand the standard of who knows what about you. You exponentially change the burden, which is a very important issue, because a lot of those folks out there, it's not that they don't care about kids. Everybody cares about kids. Everybody wants to protect kids. It's a matter of how do you do it and what's a reasonable way to go about addressing any issues to the extent there are issues.

>> Jessica Rich: Okay, thanks. Well, I wanted to get to sort of some of the concrete examples of which I think people are dying to get to. And the ones that we've certainly heard talked about today and in comments, there's four different examples and I want to know if there's other classes of data we should be talking about. There's behavioral advertising, which has already come up quite a bit today. There's geolocation data, which Matt is dying to talk about. There's... And we are, too. There's, of course, IP address, which is constantly an issue that everyone wants to explore. And there's aggregation of allegedly anonymous data, which is Paul's issue, as well as all of our concern. So why don't we... Are there other obvious categories of data that we should be debating today at this panel?

>> Kathryn C. Montgomery: Can I add one?

>> Jessica Rich: Yes.

>> Kathryn C. Montgomery: I don't know if we have talked about in-game advertising, and avatars?

>> Jessica Rich: No.

>> Kathryn C. Montgomery: But to the extent that avatars are individually identifiable -- I mean, we would have to look more closely, but they do permit the kinds of relationships and interactions and targeted personalized marketing that this law was intended to address.

>> Jessica Rich: Okay, that's a great addition. So, why don't we take these one at a time and see where we go with this. So, why don't we start with IP address, since it's the most basic, understanding that IP address is actually collected far more than -- I mean, it's collected immediately, so you've got a real issue about IP address. And if somebody would like to just give us the basics on the theory as to why IP address should and shouldn't be considered personally identifiable information.

>> Kathryn C. Montgomery: Shouldn't Paul talk about this?

>> Jessica Rich: Paul.

>> Paul Ohm: I mean, I can.

>> Kathryn C. Montgomery: He's done all the writing.

>> Paul Ohm: I'm... And by the way, I classify my research as I'm an import-export specialist. I was a computer-science undergrad and a network systems administrator for a few years and, in that job, spent a lot of time living in the Apache log files and trying to figure out who was visiting the website, for what purposes. And I promise you, they were all noble.

>> Maureen Cooney: [ Laughs ]

>> Paul Ohm: But the point -- and I think this is commonplace to everyone in this room -- is that there once was this belief that IP addresses were these evanescent little fragile bubbles that disappeared every time you hit "Reload" on your browser. And, of course, many, many, many technological and organizational decisions have conspired to make that really no longer true. And

that we all know this, right? Your cable modem is always on. Your DSL is always on. Your computer, with its DHCP settings, is not getting a dynamic IP address that frequently. And I'm at the point now where my home computer has the same IP address probably for months on end -- at least, the last time I looked at it. And at work, it's even more ridiculous. I'm basically always attached to a single IP address. And so the idea now is there's this very persistent piece of information about your computer -- that's an important caveat -- not necessarily you, but your computer -- that, as you say, is promiscuously handed out to everybody. And so the idea is that once you have this IP address, you now have this fulcrum upon which re-identification can occur. And if we attach it to a home address in this one instance and if we attach it to a credit-car number in this instance and what you did on Facebook last night in this instance, if you're a savvy enough data aggregator, you're gonna be able to use that one piece of information to correlate lots of pieces of information. So, what does this start to sound like? It starts to sound like the modern Social Security number. And what animated Congress to include Social Security number in 1999, I'd submit, probably brings IP addresses into a similar category. But let me have one important caveat -- and Sheila kind of made this point -- which is, we can't break the Internet. Right? And so -- you're right -- the Apache log, for no pernicious reason, saves IP addresses as soon as you install it. It seems like it would be an unwise regulatory decision to then say that anyone who collects IP addresses automatically has to start worrying about COPPA. But my argument would be, that's a matter for regulatory discretion and restraint more than it is a hard question under the statute. You know, I like to tell my students, when I see a legal battle, "Which side would I rather represent? Oh, yeah, I'll represent the side that argues that IP addresses fit comfortably and squarely within this list." So then the question is, should we really be putting this onerous burden on every website. And I would say, "Problem not."

>> Jessica Rich: Let's get that answer. Should we be putting this burden on every website?

>> Heidi C. Salow: I'm dying here, but I'll wait for Jules. [ Laughter ]

>> Michelle Rosenthal: Jules?

>> Heidi C. Salow: Go ahead.

>> Jessica Rich: Let's go to Kathryn first. Kathryn first.

>> Kathryn C. Montgomery: Age. Age comes first. [ Laughter ]

>> Jules Polonetsky: Age and beauty.

>> Kathryn C. Montgomery: Well, I think we need to always get back to the goal of addressing marketing. So if you look at how... And you have to then look at contemporary business models and the extent to which IP addresses and the other things... I think it's hard to talk about them in isolation, really, because that's not, in reality, how they work. It's a system of marketing that is designed to identify individual consumers. And in the case of children, then I think there is a burden. And I understand, as well, that, you know, we did negotiate with industry on a certain set of rules, but there has been an understanding that the business evolves. And those rules have to be updated, in response to your comment, in ways that will really meaningfully address what's going on. So, for example, I've looked at some children's websites. We're going to be submitting comments through with the Center for Digital Democracy and a coalition of children's groups and consumer groups, where we can see that children under 13 are on the sites that are designed for them. Parents may give permission, and the privacy policy says we only do this and this and this. But there's other evidence that suggests there's a lot more going on there that may be enabling marketers to personally market to individual children. And I'm not certain that all of that is being disclosed.

>> Jessica Rich: Jules?

>> Jules Polonetsky: Yeah. So, I mean, I guess one point before we just touch the IP address, which relates to it. You know, it would be really interesting if what was here was, you know, an identifier that's widely and globally used, because that would include a lot of interesting things -- frequent-flier numbers and so forth. Social Security number kind of comes with the government-backed, you can't get rid of it, this, you know, special category. "This is your passport number," and so forth. So I'm not sure I would look to it, you know, to make Paul's point. I think, you know,

"F" perhaps faints in that direction, although, again, it ends up being linked back to that, tied with, you know, PII. So I think the statute and rule kind of push a little bit away from drawing the broad conclusion there. And I think the second thing is, you know, Paul, in his paper, does a great job kind of looking at the scope of research out there. And I think it's conventional wisdom in one part of the community that just about anything, when you've got a lot of data, or even not that much data, can become identifiable with enough rocket scientists or even maybe with just enough smart people doing some work. And if that's gonna be the screen of, like, whether something starts becoming, you know, verboten, we're screwed, right? Because the reality is, that just about covers -- wow -- everything that is out there. And to the extent that we want to recognize that, but yet give people credit for not going ahead and trying to be rocket scientists and come up with technologies... And, obviously, there are people doing it. There are people fingerprinting browsers. There are actors around that edge who are seeking to do so. And so it's one thing, I think, to say, "Well, yeah, if you're able to," if you're somehow managing to accomplish this, or you create a great likelihood or you're going to publicly expose it, in a Netflix circumstance, where there's reason to say, "Well, wait a second, there's some risk or some issue created." But if everyone falls under the rule because of what is theoretically possible, I think it really breaks the practical process. To bring that over to the IP address for a second, look at IP addresses in a number of ways. I don't know that anybody would argue that if someone is using an IP address to get your name and have it available next to it, just using it as a substitute identifier to hand around, that it isn't directly linked. But, in the reality of most circumstances -- right? -- it is either an item that, with law enforcement or with perhaps cooperation, is sometimes, maybe even often, linkable to a person. And so I think, let's take that over there for a second and try to figure out whether or not people are using it in a way that links it to a person and pulls it into that category. I think the second piece about it is, it might be a way that you can maintain state with users, so it might be kind of a really good cookie. Right? It, frankly, isn't as good as a cookie yet, or you'd find most people using it. The industry is still using cookies, "A," because their technology is set up to do that, and, second, despite the messy frailty of the cookie, it still is a bit more stable, it appears. And I check this every so often, because, one assumes, with increasing stability of IP addresses and IP 6's and so forth, but yet the most recent research, which isn't that fresh, that I saw, still shows that the average user can have 10 or 12 IP addresses, for whatever reason, in a month, and cookies end up being a little bit more stable than that, although, frankly, probably not very reliably good for more than a number of

months. So, as a tracking device. And then I think the third cut to think about, when we talk about IP address, is, does it allow that correlation of non-PII, given that in the hands of some folks, they do have a name behind it. And just like we described the situation of a user coming to a site, you know, registering, and the appended data being put over on the cookie but no identification, clearly, by working with parties who have access, it can be a correlator of appended data. And so I think when we look at these aspects of it, it fits into those buckets just because it has this, you know, IP, IP. We spend so much time, I think we ought to take a look at how is it being used, how is it possibly gonna be used in practice, and then do these things fit into any of the rules. I'd argue. it's hard to fit easily fit it into the rules unless you're doing the more explicit PII, link things to it.

>> Jessica Rich: Heidi?

>> Heidi C. Salow: Oh, gosh. I have so many things that I'll try to cut it down. So, going back to what Paul said, I don't know if I agree that the IP address is... I don't know the word you used, but pervasively shared in way that...

>> Michelle Rosenthal: Promiscuous.

>> Heidi C. Salow: Thank you. Promiscuously share in the way that you described.

>> Paul Ohm: Oh, I just meant between computer and website. I didn't mean among websites.

>> Heidi C. Salow: Okay. I just wanted to make sure we...

>> Paul Ohm: Oh, no, the [inaudible] protocol, you're giving it to every single -- on every single packet, that's all.

>> Heidi C. Salow: Okay. So I think there's a perception maybe that that's happening, but I don't think it is, from what I know. So that's one point. The other point -- or two other points. I'll go back to what I said before, which is... I'm too much of a lawyer, I guess, but I keep looking at this definition, and I do think that what we're contemplating -- I agree, that an IP address, when

combined with other information, can make it personally identifiable. I mean, I think it would be really hard to argue otherwise. You can certainly attach a computer to a person. Okay? And I think this definition is broad enough to encompass that. It says, "a persistent identifier." And especially when we're talking about IPv6. Okay? And then it says, "such as." Well, the "such as" is just an example, right? So, and then if you combine that with "G" and then if you look at the statute, which gives the FTC authority to expand, I think you can still stay within the confines of this idea that it needs to be linked. Because what I get concerned about -- and I know a lot of companies are concerned about it -- if you start calling an IP address, in and of itself, personally identifiable, the ramifications are going to be huge. And it goes well beyond COPPA. Well. It's really important to think about that. It's gonna have huge implications for COPPA. For example, if you want to talk about real-world samples, what that would mean is that the second that a child goes to a website -- the second they go there and look at content -- if the server is automatically collecting the IP address, which is a normal function -- okay? -- of servers, at that point, does that mean that the site has already started collecting personal information and it has to then obtain verifiable parental consent? What if the child is just, you know, browsing? What if the child, you know, does not intend to go on a blog or a chat room or any of the above, and they're just looking at a picture, a game, or, you know, whatever, educational content, free content? There's a ton of these sites out there. And I've polled people. And it'll shut those sites down. It's gonna shut down the mom-and-pop sites. It's gonna shut down the not-for-profit educational sites if they suddenly have to start worrying about COPPA when they've never had to worry about it. So I really want to make sure that we can talk about sort of black-letter law, which is one thing, and we can debate about whether an IP address, in and of itself, is black-letter law PI. But then, of course, we do have to talk about... Let's talk about what that means in the context of not only this set of rules but in the context of other privacy laws, as well, that could potentially be expanded down the road. So...

>> Jessica Rich: Relative to your point, it's clear that everyone thinks, when there's linking, that it's, frankly, already covered and should be covered.

>> Heidi C. Salow: Mm-hmm.

>> Jessica Rich: But what about, is there some sort of distinction -- this is relevant to your point -- beyond linking, about use? I mean, Jules was suggesting that there's a use component here that changes its nature. So the difference between the automatic transmission that happens, and retention, the use, the sharing, is there something around that that could make IP address a reasonable item for this list?

>> Heidi C. Salow: Well, yeah. The collection versus the use.

>> Jessica Rich: Maureen. Maureen hasn't spoken.

>> Heidi C. Salow: Sorry. Go ahead.

>> Jessica Rich: Maureen.

>> Maureen Cooney: Thank you. I think you've hit exactly on the point that we're concerned about as a safe harbor. And I think probably the other safe harbors would share that same concern. As Jules, I think, did a lovely job explaining, it is the linkability, but it is the use. How do you do or design a compliance program that keeps people attentive to what the purpose of the statute was, which is to protect a very vulnerable class -- children -- and really protect their privacy? And it is about how that information is used. So where does that IP address get you? What other information is linked to it? And is the notice being given in a vibrant enough way to tell the parent exactly what is happening with that distinct identifier? I think we looked at IP address and didn't initially think that that should be necessarily be included, you know, as a rote or a default PII identifier, because, still, while you can attach it to some individual children, there may be other members of the family that are being served. If it's for behavioral advertising that the IP address is facilitating marketing to a particular IP address, it isn't necessarily a particular child. It could be other members of the family, could be other children. So I think it is a matter, as Paul said, of seeing how sophisticated are we. As the technologies evolve, what can we monitor? That's what we look at. Can we monitor what the use is, attached to that IP address?

>> Jessica Rich: Okay, so, we need to move on to behavioral advertising. But I think we'd be particularly interested in comments on IP address and how one could get at a standard, you know, if people think that's a good idea that somehow links up to use, that doesn't just say, "Trust me."

>> Maureen Cooney: Mm-hmm.

>> Jessica Rich: You know, because it has to be something that can be objectively measured and it doesn't just have the FTC and parents relying on how the company decides to use the information, because that's not protective enough. So let's move on to behavioral advertising. So, behavioral advertising is an example of IP-address-plus. And the question is, "Is data that may not be personally identifiable in the traditional sense, but is used to target ads, should that be covered by COPPA?" And, Jules, Kathryn, anyone else?

>> Kathryn C. Montgomery: I'll jump in.

>> Jessica Rich: I thought you would.

>> Kathryn C. Montgomery: Okay. [ Laughter ] I would say "yes." I mean, my immediate response is, the very nature of behavioral advertising and certainly the direction it is taking toward personalized advertising, if you look and monitor the literature in the industry, this is how the marketers are promoting what they're able to do to deliver communications and establish relationships with individual consumers. To the extent that that's happening with children under the age of 13, I would argue it fits under COPPA. And I think, again, one of the problems for -- especially, I think, with behavioral advertising -- behavioral targeting -- is that there really is not sufficient transparency as to what's going on. You know, it's not something that parents are necessarily gonna be able to tell. And I'm not even certain how the FTC monitors this kind of thing. Because you really do sort of have to trust that you are being told what's actually happening, because where I'm finding most of the information is from all of the other literature in the field that describes what goes on in many of these places, as well as promotional materials for specific websites and content areas designed for children.

>> Jessica Rich: Jules, is the targeting of an ad contacting a specific individual? And can it be correlated with other data, which is your other test?

>> Jules Polonetsky: So, look, I mean, I think that there's a problem that everyone wants to solve, and whether squeezing it into the COPPA framework is the best way to do it. I agree with Kathryn that we shouldn't have, you know, kids being tailored with ads that are gonna be persuasive to them based on the previous websites that they've been to. Generally, that's not happening in the industry, with the caveat that, very often -- well, in 10 years of my experience, I've come across a couple -- and, usually, the reason it was there wasn't because somebody was intentionally looking to create a profile of, you know, "Here's this 6-year-old's surfing habits. He'll click and he'll buy stuff." It's just not an appealing audience. And at least, most sites kind of got the sense that tykes -- you know, junior -- ought not to be there. But what ends up happening often is you do deal with an ad network and you put in your 32 sites as one big bulk. And nobody says, "Oh, it's nonpersonal, so nobody is gonna talk about, you know, kids' privacy." And so this small, underage site ends up being lumped in, because the ad network doesn't have a way to serve ads and not take the data. And so, over the years, I've certainly seen sites, inadvertently or just because nobody had the interest or capability of carving it out, throwing in kids' sites. But, generally, there isn't a big market in most of the leading ads network. You can't go ahead and buy the underage audience. Where there's obviously gray around the edges is that tween audience, where there isn't clear personal information being collected. The only information they have about the age ranges of the services are based on their marketing information. They've got some big chunk of parents, and -- boom -- there's a site in there, and there are obviously some kids. And, again, they're not collecting personal information, how you would appropriately carve out the necessary audiences. And so I think this is an area where industry, when it did, I think, a fairly reasonable job at putting together behavioral-advertising self-reg rules, didn't nail it, because on the kids-related marketing piece, they kind of stop with both, "It's covered by COPPA, good, and, if not, not." When reality is most folks aren't doing it, they could have and should have taken off the table treating a site that has a large audience of kids as a profile that ought not to be created, just like other sensitive information was excluded. And so I think that would be an easy win for kind of the industry to do for the kind of marketing practices to kind of get to. I don't see how it fits easily into the COPPA bucket. It's just a marketing thing that easily should stop. Most people aren't doing it. It just ends up being,

"Let's debate the tween piece," where I think there's disagreement, or the teen piece, where I think Kathryn and others have said, "Well, I don't even want behavioral advertising to teens." So that's where there's a debate. There ought not to be a huge debate, but yet it's not off the table, technically, under anybody's practices. So...

>> Jessica Rich: Well, why doesn't it fit into the COPPA bucket? I mean, first, does it enable you to contact a specific individual? And does it satisfy the goals of COPPA? So, we talked about the goals all day, which is to give parents more control to protect kids and, you know, to reduce information collection from kids. I mean, does... Would covering this targeted advertising serve those goals?

>> Matt Galligan: So the question, I think, that was originally posted was, does this constitute contact? So, is simply delivering an ad to a child -- knowingly delivering an ad to a child -- constituting contact? And, specifically, as it relates to behavior, I think part of what was discussed earlier was the transparency as to whether or not it is behavioral or contextual advertising.

>> Heidi C. Salow: Mm-hmm.

>> Matt Galligan: And, you know, look at... Contextual advertising is no different than a marketer wanting to advertise on Disney. You know, so I know exactly who the audience is. I know that when I'm getting ready for putting an ad buy out, and I want to do an ad buy on Sunday-morning cartoons, I know exactly who I am marketing to. And if I'm doing the same thing on a website, I'm specifically targeting a specific group of individuals based on the context. Now, understanding that, how do you define the differences between the kinds of ads that are delivered based on behavior versus context? Because, presumably, they may be the same thing. And then, as an outside party, how do I determine whether or not that was through behavior or context? So, as a website serving up those ads, does the responsibility lie that if I am providing contextual ads, that I'm not contacting an individual, but if I'm targeting those ads, that I am contacting an individual? And, actually, I think the line is so blurred there that to define serving an advertisement as contact that that is a disingenuous thing.

>> Jessica Rich: Well, except that there may be a difference in what's collected from kids.

>> Heidi C. Salow: That's what I was actually gonna say. I was gonna say, to add to what both of you are saying, there's a distinction between contextual and behavioral. Right? So we can make a line there. Contextual, I think of as being sort of like a push versus a pull. Right? So you're pushing out content to everybody equally, just like you said, based on where they are -- what website the computer is visiting at that particular moment. Pull is you are... I think you can make a distinction. Are you pulling personal information, however you define that, to determine what ad gets delivered? In my mind, I think that does very clearly already fall under COPPA. I think that that's already, or should already be, governed by the COPPA rules, because you're collecting the personal information from a child. Then we get into the actual knowledge standard. But you know it's a child, and then you decide to send an ad. Why wouldn't that already be covered by COPPA? I think where it gets much grayer is the contextual-advertising scenario where you're not pulling personal information from the child.

>> Jessica Rich: Let me just ask Maureen, who's probably addressed this in her self-regulatory standards, to comment on that.

>> Maureen Cooney: Yeah. I think we think it could already be covered by COPPA, not just under "F," which is what we've been talking about, but under "G," which is so broad. You know, information concerning the child or the parents that's collected. So I think it could be there. In the area of behavioral advertising versus contextual, I think we find, in programs that we're developing around behavioral advertising, that there are ways of monitoring, you know, whether or not advertising was delivered in a behavioral targeted means, rather than contextually. And there may be additional ways that industry will be adopting, through metadata tagging and other mechanisms, that programs like ours and others will be able to monitor. So we think it's important. And then, to the underlying issue of what's the impact on a child, the fact that profiles can be built about children, delivered to them at a young age, and then built upon as they're maturing, is that fair? Isn't that fair? How does that impact them? We think that's very important, privacy-sensitive information that should be protected, and can be, under COPPA.

>> Jules Polonetsky: So, let me just note, though, that it's not necessarily a behavioral distinguisher that we're kind of really talking about, as well. Right? The behavioral is where and how I come up with the assumption that this is a kid. So that could be because I'm at this kid's site or I've been at many kids' sites, or it could be because I've registered somewhere else and this fact is now appended. What we're really talking about is that the cookie, the IP, the identifier, once we've decided this is a kid and we've attached it to this identifier, this identifier is something now can be presented when the user shows up in lots of other places where they don't necessarily present their name. And so I think that's kind of the real question that's, you know... The reason contextual is different is because I'm not in any way doing anything about a specific user. I'm saying, "Put this here," as opposed to, "I can reach you and continue to market to you as you go elsewhere." Right?

>> Kathryn C. Montgomery: Right, and retarget you and tailor the advertising to you as a specific child. And that's precisely the kind of thing we're concerned about. As to the monitoring issue, I am glad that you are monitoring. I would hope that this information could be made widely available. I know you can't always do that. Some of it's proprietary. But, you know, I don't have a whole lot of confidence sometimes, when I'm just looking at a website and a privacy policy, that the marketer is engaging in practices that are completely free and clear of COPPA. So, I mean, I'm glad you guys are around. That's, I think, one of the really good things about COPPA, is the safe-harbor provision and the combination of the government regulation and the self-regulation and the education that has to go on. I don't see why we... Seems to me, behavioral -- I'll get back to it again -- behavioral targeting is included. I don't believe it's being done in a widespread way -- you're right, Jules -- I think that's true -- with kids under 13. But I don't see why it can't be clarified, at this point, in the rules and just have us reach an understanding. There are some areas that we're talking about now where you'll have to kind of spell out when it applies and when it doesn't. But I just think it's a really important... If there's one important message I would like to make today, it's that these kinds of business practices need to be effectively addressed by the current law that we have on the books.

>> Jessica Rich: Okay, so let me take this one question, and then we're gonna move to aggregation.

>> Male Speaker: It feels like we're putting the cart before the horse a little bit here, because we haven't really... As, you know, the FTC has addressed on a number of occasions, we haven't really come to a conclusion about behavioral advertising in toto and how it's going to be regulated and how it's going to be governed. And in the absence of that overarching framework, it seems kind of premature to say, "Okay, we think behavioral advertising is an issue, let's address it under COPPA," when we haven't looked at how it's going to be addressed overall. If we look at how it's gonna be addressed overall, then we can look at that and say, "Is there something about that overarching framework that is insufficient as it's addressed to COPPA, but not the other way around?"

>> Jessica Rich: Your point is well taken except that, here, we're dealing with a statute and a Congressional intent, whereas, in the behavioral-advertising context, it is still a policy work that we're encouraging self-regulation, so there is a distinct there. But I understand the relationship. Sheila wanted to make one quick comment, and then we need to move on.

>> Sheila A. Millar: Yeah. And I think, when we talk about online behavioral advertising, it's important to make not only the distinction with contextual advertising, but the underlying concept of OBA is across unaffiliated websites. And I think there is a vast difference between information-collection practices by what we'll call "first-party websites" and those unaffiliated website or ad networks that are serving targeted advertising. So I think, when we think about the framework of the statute, we not only have to think about definitionally whether or not, whether it's an IP address or linked information, aggregated information, and whether it fits under "F" or "G." I tend to agree with Maureen. I think it's more likely under "G." But we need to keep these distinctions between the entities involved, because depending on how we define these issues, I think a number of us have said, you're gonna break the Internet. We don't want to do that. We need to find what we agree on, what's potentially harmful to kids, what's appropriate business practices in order to maintain a vibrant Internet, and then figure out how to manage it in a rules setting within the framework of the statute.

>> Michelle Rosenthal: Okay. Okay, I think we're gonna move on to what I like to call Paul Ohm section of the panel.

>> Jessica Rich: But others can talk.

>> Michelle Rosenthal: No, just kidding. So, we talked a little bit before about the aggregation of allegedly anonymous data. And here we're talking about data points that, in and of themselves, are not identifiers or not -- what was the term we used previously? -- exclusive... What was your term, Matt?

>> Matt Galligan: Exclusive identifiers.

>> Michelle Rosenthal: Just "exclusive identifiers." Okay. But that, together, when combined, could identify an individual. And, you know, Jessica talked a little bit about Netflix as an example. And there has been concern in the past about AOL, when they released data, that each data point, in and of itself, was not identifiable, but, together, they were. So I want to make a quick distinction. In the behavioral-advertising report that Jessica mentioned earlier, we did away with the PII-versus-non-PII distinction, and we said, "Data that reasonably could be associated with a particular consumer." Here, in part "F," we have the word "permit." And so the question is, is that different? Is there a different threshold here? Because "permit" means to make possible. Paul?

>> Paul Ohm: Yeah, so, "permit" is a fascinating word, and I think we should spend a little time on it. I wanted to start by clarifying a point, for those of you who haven't encountered all this research, that I think is really critical, which is, Jules used the phrase "rocket science," and what we are learning is, this is anything but. And so what I think astounds me most about the research coming out of computer science is, every time a supposedly anonymized database is re-identified, experts -- I don't mean casual observers -- experts in the field -- seem surprised by how quickly it's done, how cheaply it's done, with what rudimentary tools and techniques, the slowness of the computers that are used. So, Latanya Sweeney, who had a landmark study used Visual Basic, I think, which, if you know anything about coding, you know, is cause for derision. We're not talking about rocket science. And more to the point, I think that, over the next five years, we're gonna see that this trend accelerates, that as computers get faster, outside information gets richer -- and one thing you have to understand, it's all about the outside information -- that we're going to slowly but surely

recalibrate our intuitions, and we're going to slowly but surely just lose the faith that we have in anonymization today. Okay? So, what does this mean? This means that, in today's conversation that we're having on the panel, I think we keep really bouncing back and forth between two questions which are different. Question one is, "Does the FTC have power underneath the definition in "F," to extend the regulations to things like IP addresses?" And I think, unequivocally, the answer to that is "yes." I absolutely think it is. And you will have an amicus brief written by me and my students when this gets litigated someday in federal court. [ Laughter ] But if the question is, "Should we include things like IP addresses?" then I'm right on board with Jules and Heidi and everyone else. You know, it's the classic "With great power comes great responsibility" meme, right? So the idea here, I think, is it's a really dangerous thing to tell a federal regulator, which is, "You now have the power of God. Any piece of information out there that you want to deem, suddenly, within this regulation, you have a very colorful argument based on lots of recent computer science, that you have the power to do it." And so then it gets to questions like, "well, then should you?" and "How are you gonna break the Internet?" So, Heidi's point was, we can't include IP addresses on the list, because then every website will be covered. Of course not, because we still have the knowledge requirement. Right?

>> Heidi C. Salow: Right, but that's a whole nother...

>> Paul Ohm: Which doesn't have to turn necessarily on how we define "personal information" -- at least, as I read the statute. So we can have an expanse of definition of personal information and interpretation of the knowledge requirement that still excludes most websites.

>> Heidi C. Salow: No, but they tie together, correct? I mean, they tie together.

>> Paul Ohm: Not necessarily. I've been looking at the language. I'm not sure they are tied together.

>> Sheila A. Millar: Well, you also have the exclusions.

>> Paul Ohm: Right.

>> Sheila A. Millar: And so I think the task is that, if, for certain policy reasons, we want to expand the definition and that there is a, for the sake of argument, a legal, colorable basis to do that, then I think the response is, "Does it make sense? Should there be exclusions?" Let me give you one good example. You collect, as many of us have noted, IP addresses. They're immediately logged when the visitor hits the page, regardless of who that visitor is. Now, for many kids' sites, their sites are structured to following the COPPA FAQs and the guidance of CARU and others to promote an anonymous experience. So many, many children's websites will allow that child to participate by signing in with a user name and password. If, suddenly, those items are personal information, plus the IP address, you undercut this assumption of how you provide a pretty anonymous experience to a child, and you force the websites to turn to a more privacy-invasive model, perhaps, because you have to collect more personal information. The IP address alone will not allow that website to contact the parent to get parental consent, and so you have to really think through, with all of the elements of the statute and the regulations, how would such a universe look if we redefine these terms in a different way, and then how you practically offer appropriate content intended for kids and get meaningful parental consent. I would say that an IP address, user name, and password won't allow you to do that. And if you define that as personal information, you then would force the website operator into a different data-collections construct.

>> Michelle Rosenthal: Okay, so, Sheila, you're offering an example where the website is not... You know, they're getting this information, they're not using it. They're promoting anonymity on the site. What about an example where the website has access to a large database is appending data? Should there be a difference if the website is actually getting information elsewhere?

>> Paul Ohm: So, let me just summarize really quickly. And I think this is response to your question. I think our conversation should be about policy and not power. I think the question of power is actually one where you've got angels on your side because of the way computer science has been evolving. And so the question is, "What are our guiding principles that..." Because I don't think anyone is making the argument -- and I'm not an admin-law expert -- that you need to regulate anything that could colorably be called personal information. I think the FTC is free to make choices based on lots of policy. So, I've heard lots of different policy proposals thrown out.

So, Jules said, "Are you actively re-identifying?" That's a wonderful principle on which to build a rule. The second is, think about the policies behind COPPA. Why are we having this? So, let me add one more to the mix -- quantity. So, the one thing I say is, the research has suggested that the more data you warehouse, the easier it's going to be to do the kind of re-identification I'm talking about. And so... And I might even write a comment to this, respecting this proceeding. I would argue that, once you get past a certain amount of data living somewhere in your company, and then you have actual knowledge that you're reaching out to children, yeah, you probably fall within COPPA. You probably should fall within COPPA. It may be clear.

>> Jules Polonetsky: And to stay at a policy level for a second, because we don't really have parental-verification accessing methods, but what we're really sort of doing here is we're saying that there is this kind of identity that's out there that can be achieved that other people can create about you. And just one thing is that, if we want a solution here, whether we would maybe push the focus more towards "how do we advance the identity solutions that come along with the full package" -- and, obviously, they come with the privacy challenges, but they also come with the solution, instead of sort of deeming identity to have been created -- I think, until recently, it probably just wasn't really right. But when you take a look at, you know, Facebook as a social-media lair, when people kind of got some use of websites, thought it was useful -- boom -- you know, hundreds of thousands of sites kind of adopting the various tools, the government making progress with access to various government services -- we're probably at a more ripe time today and maybe the NTIA Task Force will come out with some progress. And there are companies all throughout the room here, from Makeshore and Privo and others. And if we start looking at them not solely as verification but as ways to solve identity, that's obviously the most attractive privacy solution that could come along.

>> Sheila A. Millar: Well, and I think retention also has a role when you're talking about aggregated data. Some of these issues potentially could be solved by limited retention, as well. And so the question again, from a policy standpoint, is, "what is the problem that we're trying to solve? What are the benefits that kids have from accessing the Internet? How do we address this potential?" But according to Jules and others, is apparently not reality of a lot of data aggregation and online behavioral advertising targeted to teens, but we want to be proactive in trying to

anticipate how do we address issues that might affect children's privacy. I think we're all here to try to solve some of those issues and be creative about looking at ways to do that. And it may be that, you know, retention and other approaches would be one way to look at the issue and solve the problem.

>> Kathryn C. Montgomery: Can I just respond to several of these...

>> Michelle Rosenthal: You can respond. And then we're gonna get to one more question and move on.

>> Kathryn C. Montgomery: Okay, fine. Well, I think these are all really important questions. And it isn't a black-and-white issue. But I do think, what is suggests to me is that we need more information on what the actual practices are, and we need independent information. And I would hope that there would be some way that the FTC could do an audit. I mean, one of the most useful things -- and not just an audit of what you can see on the website, but an audit that looks really at what the contemporary practices are and what the best practices are. One of the most useful things that led to COPPA was the study that David Vladeck talked about earlier today, that the FTC did. So I think we're talking somewhat hypothetically here, and it would be really useful if we could have more information. And I also just want to say that I agree that there is a need to be able to create an accessible experience for kids online. It's a terrific tool. I want them to be able to go online and have a personalized experience, but to do it in a way where they're not being targeted with personalized advertising, and to do it in a way where the minimum amount of data are collected. So those are the goals. You know, and I think there are ways to do it. But we do need to take into account what the current capabilities are with the contemporary business models and make sure they're covered.

>> Michelle Rosenthal: Thank you, Kathryn. So, I wanted to get to one more question sort of in this category, before we move on to geolocation, which I know Matt is itching to talk about. Part "G" of the rule says, "Information concerning the child or the parents of that child, that the website collects online from the child and combines with an identifier described in this definition." So, Maureen, you mentioned earlier that behavioral advertising might actually fit under "G." If there's

no specific identifier involved, how would that fit under "G"? You know, does "G" contemplate that type of information?

>> Maureen Cooney: Okay. So, I think we would look at that in a couple of ways. One is the identifier may, in some cases, be an IP address. Or it may be a cookie that's been dropped. But what we would be looking at -- and in fact, so far, we've been talking about pretty sophisticated collections from children online -- and they're not really the types of experiences that we're seeing at TRUSTe in our COPPA program -- but what we are seeing are some types of information about children's interests, that are so vibrant in the ways that they're doing them now, through videos, where there's no name attached to a picture but plenty of other identifying information, including not necessarily what we've talked about as geolocation, but basic address kinds of identifiers that you could pick up a lot of information about children's interests through photos that are being put on services or through videos. Those are the two main areas that our clients are dealing with. And then, from those interests, it would be possible to do some targeted advertising. But that's not what we're seeing as the present-day issue. It's safety concerns for children and really reputational risks about building a profile, about their interests, that they're a little bit naive in putting information out there that may not be appropriate if it were tracked.

>> Michelle Rosenthal: Okay. I'm going to move on to geolocation. And I think it would be helpful to sort of state, to note, that we're starting with the premise that what's already covered is Part "B." So a home or other physical address, including street name, and name of a city or town. So the big-picture question is whether that language is adequate, given current business models, or whether we need to move beyond that. So maybe, Matt, maybe you can talk about what "geolocation" means.

>> Matt Galligan: Sure. So, first, start off to answer that question. It absolutely is not adequate in the current language. If I were to give anybody in the room my current coordinates, which would be, you know, whatever, negative-37-dot-zero-blank and then, you know, 105-blanks, that would mean absolutely nothing to anybody in this room. You know, and it, on face value, means absolutely nothing. Sure, you might be able to plug it into Google Maps or any of these other services, but, at face value, it means nothing. However, you can take that and make a much more

accurate reading of where something has happened -- an event, a physical address of where somebody is standing. Under the current ruling, it says... Or, under the current rule, it says, "a home or other physical address, including street name, name of city or town." which means that "coordinate" is not defined in that rule. Now, I can correlate the coordinate to come up with that. But coordinate itself is not specifically called out in that rule. Coordinate may or may not be able to be included in "B," because it is -- because the information that you get from the coordinate is derivative. So it's not necessarily identifying at face value, but as soon as I plug it into a service that can identify that, then I get some information back about the street name, city, town, things like that.

>> Michelle Rosenthal: Okay, so... Yes. [ Laughs ] Sorry. So, how specific should geolocation be, in order to trigger COPPA, if we were to say geolocation is personal information?

>> Matt Galligan: You know, I think that it actually falls under the "F" or the "G." I'm not... Probably the "G," or at least somewhat falls under that. I don't know if the language itself needs to be specifically called out. But, on its own, it would need to be combined with any of this other information for it to become effective, because, you know, for instance, an iPhone, as soon as you open the camera app for the very first time, it says, "Would you like to allow this app to use location?" And you never see that prompt ever again. And every single picture that's then taken with the iPhone stores the metadata of where that picture was taken. And, on its own, each one of those coordinates may be an identifier of where somebody is. But it's ethereal. It's where they were at that given time. Now, if you have enough information collected -- and this goes back to aggregate knowledge -- if you have enough information collected and you can start seeing trends about where that person is, you might see two locations, which might be school or work and home. And you might see those things happening over and over and over again now. I think that it absolutely goes back to aggregate knowledge, that, with all of that information put together, then you can start building a profile about somebody. But without any one of these other identifiers, I don't think that it is an exclusive identifier.

>> Michelle Rosenthal: So, Jules, should geolocation be included in the definition of personal information? And if so, what would that look like?

>> Jules Polonetsky: So, maybe let me again cop out by saying, what should the question be? Right? So, if there's a precise geo-information that, frankly, acts as a substitute for home address -- if I actually have a coordinate that can identify that precisely, that these are his home address -- how is it not different than that user's home address, whether or not you got to go look it up or not? It's just a coded term for a particular address. I think the trickier issue is, what about when it's not your home address or, you know, this identifying address -- your place of work, your home, whatever the category that one captures? What is it... What about when it's just, "This body is here now?" Is that just another interesting data point which, you know, is no different than, "Okay, here's what we now know about this person," and whether I have a lot of data points and I know a lot about your activity, it's no different than having lots of specific marketing or interesting points? Or is there something about the fact that, at some time, we could walk over and find you because of the geo that makes it interesting? So I think, the latter example, I disagree with Matt, in that, in some cases, it may just be a substitute for a very precise coordinate that indicates your permanent PII home address. In the other case, I think it's a little trickier to figure out whether what we -- is there a contact here? You know, what is it that we're capturing about this moving set of information?

>> Michelle Rosenthal: Okay, so Kathryn, and then we have a question in the audience.

>> Kathryn C. Montgomery: I think, first of all, when we talk about geolocation, generally, the technology we're talking about now is the mobile phone. I mean, there may be others, but, right now, that's what the issue is. And I think you have to look at this in the context of emerging practices with mobile marketing. So, what can happen by having the location, you're also going to know who the phone belongs to, or you'll know more information by the very nature that that's the device that's being used. You will know more than just where that person is. You'll know that that is the user of that telephone, right? And then let me just --

>> Matt Galligan: Not necessarily.

>> Heidi C. Salow: That's not necessarily true.

>> Sheila A. Millar: And you may not know it's a child.

>> Kathryn C. Montgomery: All right, so, you'll know things about who's been on that phone, too, which you might also because you may be collecting all kinds of other information about how that phone is used. So it would make it possible to be able to identify when a child is near a particular business, like a McDonald's, and send a coupon. And, again, those are the kinds of things that we're concerned about.

>> Matt Galligan: So, knowing that it is a child is the important component there. And the phone...

>> Kathryn C. Montgomery: Well, under COPPA, it is, yeah.

>> Matt Galligan: Under COPPA, absolutely. But that's what we're talking about, right?

>> Kathryn C. Montgomery: That's what we're talking about today.

>> Matt Galligan: So, under COPPA, you have to know that it's a child to have that defined that way. Now, I certainly agree with, actually, both of you in the regard that --

>> Kathryn C. Montgomery: You just said "no." [ Laughs ]

>> Michelle: You said it's not true.

>> Kathryn C. Montgomery: "Not true."

>> Matt Galligan: I agree to an extent that the -- that you can -- or that the targeting based on geolocation should be covered. But going back to his point, which is, "What is this distinction between home and some other point that you exist?" And, first off, the home question, yes, you can determine that a coordinate is home, but you require aggregate knowledge before you can

determine that that is home, because it's just a number. But with enough numbers that is all within a similar area, you might be able to determine that that is home. But another point, without any other information, say, other than what Apple considers device data -- they actually specifically call it in their TOS -- device data is defined as IMEI, which is the specific device identifier, your SIM card number, your phone number, and a couple other things that Apple just has available in their API. They specifically have called out, in the TOS -- now, this is just Apple, it's not across everybody else, and it probably could just be a best practice -- it specifically called out that you cannot use that data to market.

>> Kathryn C. Montgomery: Oh, Apple. Yeah, I think that is... That's different, and that could be a best practice.

>> Matt Galligan: So now I'm saying that could be a best practice, but it could also mean that it could be a baseline for a rule.

>> Kathryn C. Montgomery: Mm-hmm. Now I'm not proposing that, but I'm just saying that that could potentially be that. Now, I don't necessarily think that with device data that you can still identify that it is a child, because you also don't get access to what other apps are included or are on that device. You don't know through behavior necessarily, except for maybe through your own line.

>> Michelle Rosenthal: And we're assuming, though, for purposes of this discussion, that they know that it's a child or that it's directed at a child, just for this.

>> Kathryn C. Montgomery: And there are a lot of ways.

>> Matt Galligan: Sure.

>> Michelle Rosenthal: Right.

>> Kathryn C. Montgomery: Because of the cross-platform content areas, for example, whether it's social networks or something else, you may very well know.

>> Matt Galligan: Sure.

>> Michelle Rosenthal: So, John, did you still have a question? I don't want to...

>> John: No, Matt largely...

>> Michelle Rosenthal: Oh, take the mike, yeah.

>> John: Matt eventually got to it. But just to make very clear that two location points really can be a unique identifier, I mean, there is only one person on the earth who regularly travels from my home to her high school, and that's my daughter. And...

>> Michelle Rosenthal: So if we were to include geolocation in the identification of personal information, should there be a requirement that it is collected over time, that it's not just one piece of geolocation data, that it's aggravated in some way? Or can we, you know...

>> John: Well, to some extent, in "G," you have kind of a catch-all, but the catch-all correlates back in something in "A" through "F."

>> Michelle Rosenthal: Right.

>> John: And I think the point is that you can have some "G"-type data points that, taken with other "G"-type data points, could be a unique identifier. And so, I mean, it gets a little harder. And all you guys have been talking about, can you go back to a use idea of, you know, well, how do you use the IP address or how do you use these data points, and do you use it as a unique identifier. And that's a possible approach.

>> Michelle Rosenthal: Heidi, you have some clients that are here.

>> Heidi C. Salow: Oh, yeah. I was gonna say, not even just on behalf of clients, but I think, to can assume that because it's a mobile device, that suddenly you -- whoever the "you" might be -- because I think that's another thing we're talking a lot, sort of very generally about -- one or you having this information, I think it really depends on who are we talking about, right? To assume that because a person has a mobile device, the world then knows I'm the owner of this mobile device, I was in the Starbucks this morning, I bought a latte, that's not really the case at all. And in fact, you can't even get -- Mike will know this -- you can't even get a cellphone number. I can't look up a cellphone number. Okay? I can't find your cellphone number. You have to give it to me. It's not publicly available. So, no, I don't know who you are, meaning...

>> Michelle Rosenthal: So, let me just offer... Okay, so, it's not about necessarily knowing who you are. If I have your e-mail address, I don't necessarily know who you are.

>> Heidi C. Salow: Right.

>> Michelle Rosenthal: But I can contact you online. And if I have your geolocation, maybe I don't know who you are, but I might be able to physically contact you. So, let's just make sure we phrase it that way. In that case, do you think...

>> Heidi C. Salow: So, now we're going -- So now I think we're going to the device versus individual, right? Because you're contacting my device, right? And I'm just trying to clarify.

>> Michelle Rosenthal: Okay. Yeah, right.

>> Heidi C. Salow: You don't know that I'm... I know, I realize I'm...

>> Michelle Rosenthal: No, I just want to to...

>> Heidi C. Salow: I feel like I'm the bad guy, but I'm just trying to be practical here.

>> Michelle Rosenthal: I don't mean to put you on the spot. I want to make sure that we explore this.

>> Heidi C. Salow: Just to be practical, because I think we need to really think, practically speaking, what's happening and who are we talking about has this information. The wireless carrier knows who I am, because I subscribe to the service. And when I signed up for the service, I told them who I am. And, by the way, I know we talked about this earlier, Michelle, but when you go back to IP addresses, an IP address alone is not going to be the only mechanism by which you can identify a mobile device. This already exists. The SIM card identifies the mobile device already today. Everybody has a SIM card in your device that's unique. So we get worried when we talk about it. Again, I'm not saying it's not something we should be concerned about. But it's already identifiable. But anyway, going back to that. So, I think the carrier knows a lot about me as a subscriber, and the carrier is subject to very strict rules, both under the CP&I regime and under ECPA, the Electronic Communications Privacy Act, as to who that information can be shared with and for what purposes. So I just wanted to make sure we were talking about -- who we're talking about here.

>> Jules Polonetsky: I think there's a simpler example that maybe highlights this a little easier, because the mobile thing starts bringing in all these other factors that are not... So, here's a more real-world example. Today, I'm at a website. A website obviously can geo in a general way because of IP address. But, today, many computers that don't have built-in GPS, however, can download a little plug-in that relies on your Wi-Fi antenna. You know, great attention in recent weeks to the kind of Google Wi-Fi, but obviously there's Skyhook, there are other companies. Wi-Fi networks are mapped. And so do we want to say, for instance, that if you're -- what we would be saying, if we extend to geo, is that if I'm a kids' site and it said, "Click here so that you can get your precise whatever" -- right? -- "Click here to allow us to use --" most of the browsers require this on some sort of an opt-in basis -- Firefox actually is launching a little icon that's gonna let you know when their next version -- IE may do that. I haven't checked. So, do we want to say that a child site could not collect -- right? -- that's not collecting any other explicit personal information - - that it couldn't use this Wi-Fi geo thing to precisely take the location? That's kind of a clear, clean shot at this question.

>> Michelle Rosenthal: So, do we want to say that? Paul?

>> Paul Ohm: So, I see why you're all COPPA experts, because it's like a beautiful matryoshka doll, and every time you read this, you see a different layer you didn't notice before. [ Laughter ] I might become a COPPA expert after this. [ Laughter ] So, look at "B." First of all, "B" is not restricted to homes. Right? It's any physical address. But aren't you intrigued by the fact that Congress did not care about the street number? All you need is the name and the city. So, what is this, the megaphone rule? If I drive to your street and yell an advertisement at you?

>> Kathryn C. Montgomery: "Including."

>> Paul Ohm: But it does suggest to me that when you ask a question about one coordinate at one moment in time, why isn't that exactly the kind of interest that Congress had in mind? Right? I don't know what Congress was thinking there. Maybe they were worried about megaphones. [ Light laughter ] But, again -- I hate to be a broken record -- I don't think this is about power. I mean, Congress was writing lots of blank checks here. [ Laughter ] I think this is about, is it a good idea or is it a bad idea.

>> Michelle Rosenthal: All right, so let me attempt to wrap up on the geolocation so we can get to a couple more questions before we finish the panel. Is there a way to articulate a clear standard on geolocation? If we were to include it in the definition, how would we do that? What would it look like?

>> Sheila A. Millar: Well, I think that we've talked a little bit -- and Paul's made a good point here -- that, under "B," how different is precise geolocation, where you either have actual knowledge that you're dealing with a child or on a kid-directed website or online service, that your kid-targeted, then potentially it's already covered? I think the issue is whether or not there is any reason to exclude it, as Paul suggested. You know, are there beneficial reasons to include that sort of information. Otherwise, currently, under COPPA, beyond the exceptions, you're required to get parental consent. And if you're getting the home address for purposes of internal marketing to a

child, you have the e-mail-plus option. So maybe geolocation fits in the e-mail-plus construct. Maybe it doesn't. But I think that for the geolocation information, if you're either kid-directed or have actual knowledge -- and I think the actual knowledge is the tough one, because I think, in most circumstances, you don't know. If somebody is going between school and home, you know, Dad may know that it's my daughter, but service provider, assuming there's a website or an online service involved, they may have no idea. They've got a number and a location, so they don't know. So, again, I think you have to put the pieces together to determine what's the right rule. But if you have a kid-directed website or online service or somebody with actual knowledge, I think geolocation probably fits right within "B."

>> Michelle Rosenthal: Okay.

>> Matt Galligan: I think it actually fits better within "G."

>> Kathryn C. Montgomery: [ Laughs ] I love this discussion.

>> Matt Galligan: Just saying that.

>> Kathryn C. Montgomery: Any other letters? Like "Sesame Street."

>> Matt Galligan: Just because, like I said earlier, exclusively, a single point does not constitute -- Well, I guess it says, "or other physical address." I'm going to agree with her. It's "B." [ Laughter ]

>> Michelle Rosenthal: Final answer? [ Laughter ] Is that your final answer, Matt?

>> Matt Galligan: You know, in terms of calling it any other physical address, I mean, if just any coordinate defines any other physical address.

>> Michelle Rosenthal: Okay.

>> Kathryn C. Montgomery: I just want to make sure COPPA covers mobile marketing. [ Laughter ]

>> Michelle Rosenthal: Kathryn. [ Laughs ]

>> Matt Galligan: But the one thing I will say about coordinate and "B" is that coordinate will likely need to be spelled out.

>> Heidi C. Salow: I was just gonna say the same thing. I don't disagree that it falls within "B," but if you're gonna add geolocation, please make it clear.

>> Michelle Rosenthal: Sure, we'll do that.

>> Jules Polonetsky: And I just want to throw in the complication that your wireless carrier usually knows who the account holder is, not who has the phone. So if the iPhone was in my family, I haven't told anybody who has which one of them, and...

>> Sheila A. Millar: Well, and that goes back to the fundamental point that it's directed to children or it's actual knowledge. And if you... And I can go as a small business and buy six phones and give them to my employees. There's no automatic assumption that just because there's multiple cellphones attached to a single subscriber, that there are some kids in there. And even if there were, you wouldn't know how old they were, because they would be minors perhaps. But they may not be. So I think we really need to keep coming back to the required statutory language and understand that there are some limits to what people actually know about you.

>> Michelle Rosenthal: Okay, so, yeah, we're just going to wrap up, because I don't want to deprive you all of your break. But we, again, urge you to submit comments on all of these topics and anything else that you think we should cover.

>> Kathryn C. Montgomery: We didn't cover "H."

>> Michelle Rosenthal: And we didn't... [ Light laughter ] There is no "H."

>> Kathryn C. Montgomery: [ Laughs ]

>> Michelle Rosenthal: Oh, yeah, we're back at 3:00. Thank you, all.