JIM TRILLING: Good morning. My name is Jim Trilling. I am an attorney in the Federal Trade Commission's Division of Privacy and Identity Protection. On behalf of the FTC, welcome to today's FTC workshop on the future of the COPPA rule.

Before we get started with our substantive program, I need to review some logistical details, and the first one is going to make me very unpopular. If you do have coffee or other refreshments with you, I do need to ask that you please discard them. We're not permitted to have those items in the auditorium. Please silence your mobile phones and other electronic devices. If you leave the Constitution Center Building during the workshop and will want to re-enter, please allocate time to go through security screening again. If you notice any suspicious activity today, please alert building security.

If an emergency occurs that requires you to leave the auditorium, but remain in the building, please follow the instructions provided over the building PA system. If an emergency requires evacuation of the building, an alarm will sound. Please leave the building through the 7th Street exit. After leaving the building, turn left and proceed down 7th Street and across E Street to the FTC Emergency Assembly Area. And please remain in that assembly area until you receive further instructions.

This workshop is being photographed, webcast, and recorded. By participating, you are agreeing that your image, and anything that you say or submit, may be posted indefinitely at ftc.gov or on one of the commission's publicly available social media sites. The webcast recording and transcript of the workshop will be available on the FTC's website shortly after the workshop concludes.

Attempts to address the speakers while the workshop is in progress, and other actions that interfere, or attempt to interfere, with the conduct of this workshop are prohibited. Any persons engaging in such actions will be asked to leave.

During the panel discussions, the audience is invited to propose questions via the question cards that are available from FTC staff. If you would like to submit a question, please write the question on a card and raise your hand to signal for FTC staff to collect the question from you. If you are watching our live webcast, you can propose panelists questions by tweeting them to @FTC using the hashtag #COPPAworkshop or emailing them to COPPAworkshop@ftc.gov.

Please understand that we likely will not be able to get to all proposed questions.

Restrooms are located in the hallway just outside the auditorium. And the Constitution Center cafeteria is located around the corner from the auditorium. The cafeteria will be open during our morning break and during our lunch break. The cafeteria does closed for the day at 3:00 PM, so it will be closed during our afternoon break. When you leave the building for the day, please return your visitors badges and lanyards to the security staff so that we can reuse them.

And with those logistics out of the way, it is my pleasure to turn the podium over to FTC Commissioner Christine Wilson who will provide opening remarks.

[APPLAUSE]

CHRISTINE WILSON: Good morning, everyone. Thank you so much for coming today. Obviously, this is an incredibly important topic. And so we greatly appreciate your participation, your perspectives, and your thoughts. So my name is Christine Wilson. And I'm honored to serve as a Commissioner at the FTC, but I am also honored to serve other important roles in my life, including that of wife and mother.

My children are now young adults, but I remember vividly the online privacy issues with which my husband and I grappled as our children were growing up. Let our pre-teen play interactive video games with other players around the world, complete with private chat rooms? No, honey, you need to wait until you're older. Allow our high schooler to join Facebook to access homework assignments. Of course, but you also need to understand your grandparents are going to stuff your timeline with cute puppy videos. And agree to our young teenager's request to launch a vlog in the hopes of attracting thousands of followers and becoming a paid online influencer? Uh, no, my love. But to the backup request to launch a fashion and makeup blog? Yes, with some parental oversight.

So we had countless discussions with our children about these and other issues, including parental controls, Snapchat, other apps, geolocation data, and the potential pitfalls of an online presence, generally. One of my children did endure cyber bullying, but neither dealt with being stalked or lured into a sex trafficking ring. But my husband and I were always alert to these very real and dangerous possibilities.

So I share this background with you to provide context for my remarks this morning. I

understand the struggles that parents face in allowing their children to take advantage of online educational and recreational content, while preserving their privacy. And I'm honored to serve in an agency that has a rich history of working to preserve children's privacy. In fact, the commission's focus on privacy, and children's privacy, dates back more than two decades to the FTC's 1998 report to Congress on consumer privacy.

There, the FTC called on Congress to enact legislation that would put parents in control of the online collection and use of personal information from their children. And Congress enacted COPPA, the Children's Online Privacy Protection Act, later that year. In passing this law, Congress determined it was important for websites targeted to children to obtain verifiable parental consent, or VPC, prior to any collection, use, or disclosure of personal information from children. The FTC was, then, empowered, through rulemaking, to outline the mechanics of how websites or online services could get VPC. And we issued the COPPA Rule in 2000.

So the FTC seeks to ensure that the COPPA Rule keeps pace with changes in technology, the development of new business models that involve data collection, and the evolving ways that children interact with online services. This imperative prompted amendments to the rule in 2013. Relevant changes we were dealing with then included the rise in social media platforms allowing children to upload photos and videos, the explosion of smartphone technology permitting the collection of precise geolocation information, and the use of behavioral advertising for children. The 2013 rule addressed these changes and facilitated many enforcement actions in the intervening years.

And we approach the current rule review with the same goal. Today, we have the growth of education technologies, the use of voice-activated connected devices, and the prevalence of platforms that host third-party content. We're accepting public comments on a range of topics, including how the rule should apply to these new technologies. We also want to make sure that the changes we made to the rule in 2013 have accomplished their goal of protecting children. To be clear, this rule review is not an attempt to rollback any of the 2013 changes, but instead to make sure that the rule continues to serve the congressional goals articulated in 1998. Personally, I look forward to hearing from all stakeholders to be sure that while we are alert and cognizant of the issues of innovation and competition, those goals are not served at the expense of children's privacy.

Obviously, I wasn't a commissioner when the FTC recommended that Congress enact COPPA, but I agree wholeheartedly with the goal of putting parents in control of the online

collection and use of personal information from their children. At the same time, it's important for parents to use the tools that Congress and the FTC have created. I also commend to parents helpful materials, like Protecting Kids Online, available on the FTC website. As my children were growing up, I read those materials, and I shared them with my children, and I would commend them to other parents, as well.

Let me focus, for a minute, on COPPA enforcement. To date, the FTC has brought more than 30 COPPA cases against a variety of entities. With your indulgence, I'm going to highlight two recent cases. The first is Google YouTube, which puts online platform operators on notice regarding their obligations under COPPA. If operators know user-generated content on their platforms is directed at children, they must comply with COPPA, if they collect personal information from viewers of that content. Our complaint alleged that YouTube had actual knowledge that it was collecting personal information from viewers of child-directed videos on its platform, but failed to comply with COPPA obligations.

The settlement requires YouTube and Google to pay $170 million in monetary penalties. YouTube must also develop a system for third-party content creators to self-designate child-directed content that they upload to the platform. If content is directed to children, in other words, if content creators couldn't conduct behavioral advertising on their own website or app without parental consent, they can't do it on a third-party platform either. And we will conduct a sweep of YouTube channels soon to determine whether there are other violations of the COPPA rule we need to address.

A second case I wanted to highlight is one against Musical.ly, which is now known as TikTok. This case made clear an operator may be subject to COPPA obligations, even if its target demographic is not children under 13. Here we alleged large numbers of children had TikTok accounts that allowed strangers to directly message them without providing notice or obtaining parental consent. As our complaint alleged, TikTok knew that children were using the app. In addition to the $5.7 million civil penalty, the operators are required to comply with COPPA going forward and to remove all videos made by children under the age of 13.

Given our scarce prosecutorial resources, it is reassuring to remember that the impact of these cases extends far beyond the specific companies at issue. For example, following the TikTok settlement, I spoke with a company that offers third-party age verification services. In the weeks following the TikTok announcement, this company received a substantial increase

in requests for their services from companies seeking to ensure COPPA compliance and avoid FTC enforcement action. The company directly attributes the rapid growth in demand for its services to recent FTC enforcement actions.

So the cases I've just described demonstrate the commission takes its COPPA enforcement very seriously. But our enforcement actions are only part of the commission's COPPA program. We also help companies comply with COPPA on the front end. FTC staff speaks frequently at public events about how the rule operates and responds to thousands of questions submitted through the so-called COPPA hotline. In the past year, our COPPA FAQs page has received over 125,000 views and our page on how to build a compliance program has received over 48,000 views.

But today is primarily hearing from you. Today's workshop will feature four panel discussions reflecting a variety of perspectives, consumer groups, academics, practitioners, industry, and the UK government. The first panel will explore the state of the world in children's privacy, including CCPA, GDPR, and the UK's age appropriate design code. The second panel will examine the scope of the COPPA Rule. Among other things, panelists will consider what it means to be a mixed audience site that appeals to both children and teens.

Our third panel will discuss whether we need to revise any definitions in the rule, including the definition of personal information. It will also examine current and potentially new exceptions under the rule to parental consent, including for internal operations, EdTech, and audio files containing a child's voice. The final panel of the day will address persistent identifiers.

The workshop will also include presentations from Dr. Jenny Radesky of the University of Michigan, Morgan Reed of the App Association, and Jonathan Mayer of Princeton University. And my colleague, Commissioner Phillips, will give remarks prior to the second panel.

Before concluding, I want to say a few words about privacy legislation. Along with my fellow commissioners, I have urged Congress to enact federal privacy legislation to be enforced by the FTC. I believe COPPA is a good model for Congress to consider, as it drafts comprehensive privacy legislation. Congress made value judgments about the potential harm to children from online activity and determined it was important for websites targeted to children to obtain VPC before collecting, using, or disclosing personal information from children. Congress then empowered the FTC, through APA rulemaking, to outline the mechanics of how websites or online services could obtain VPC.

So this division of labor, Congress weighs societal values, makes value judgments, and identifies the harms to be addressed, while the FTC exercises narrow APA rulemaking authority to implement the statute, is an effective allocation that appropriately cabins the FTC's role. COPPA also gave the FTC civil penalty authority, which it has employed in dozens of enforcement actions. And I believe this authority has a beneficial deterrent effect and should be included in forthcoming federal privacy legislation.

In closing, I would like to emphasize my deep concern for protecting children's privacy online. I look forward to working with my colleagues and with the agency's stakeholders to continue preserving children's privacy as technologies evolve and as new generations of parents grapple with ever more complex issues. I thank you, once again, for joining us today, whether here in person or online. And I now turn the podium over to Dr. Radesky.

[APPLAUSE]

JENNY RADESKY: Good morning. Hi, everyone. I'm Jenny Radesky. I'm an Assistant Professor in the Division of Developmental Behavioral Pediatrics at the University of Michigan Medical School. I'm also an NIH-funded researcher about young kids and digital media.

--and digital media. I called my talk "The Digital Playground Today," because I really like this idea-- Marina Bers, who is a human computer interaction researcher out of the MIT Media Lab and Tufts-- I love this idea because it conveys the fact that this is an environment. This isn't just an exposure, or a game, or a substance that children are using. It's an immersive place of which the design can really influence children's behavior and shape what they're doing.

So, you'll see over and over today in my talk, I'll be referencing this idea of how the design of the environment can improve children's well-being. Now, let's see where I advance. Here we go.

So my goal is really to set the stage for a discussion about COPPA today by reviewing research about what kids are actually doing in this rapidly changing digital environment. So I'm going to review some of the Common Sense Media statistics from their latest census. I'm also going to be reviewing some of my really current research where we've been tracking the app usage of preschool-age children and finding that many of them are using general audience apps.

We've also been looking at what sort of data transmissions are happening from the apps that they're playing. I'm also going to review some of our priorities from the American Academy of Pediatrics. I'm a policy author at the AAP. And so I really want to highlight how we and why we think children deserve special protections because of their own strengths and vulnerabilities.

This graph is probably well known to a lot of you. This is the Common Sense Media data about the rise in adoption and access to smartphones and tablets since 2011 through 2017. It may be taken for granted to a lot of you because you are-- you work in the industry or you've kind of been behind a lot of these trends.

But for pediatricians, for parents, this feels like a tidal wave. This has been such a dramatic and game-changing evolution of technology in their homes, in our offices, that parents really don't feel like they can manage it or keep up with all the knowledge they need. Researchers can't keep up in terms of our funding cycle or getting publications out in time just because it's such a moving target.

And it's not just the number of little hands that can get on mobile devices. It's also the amount of time that they otherwise might have been watching TV, or a DVD, or something else that was a uni-directional information exchange and now is a bi-directional exchange and has a lot more interactive design features. I mean, this figure shows an almost 900% increase in the amount of time that children spend with mobile or interactive platforms. And that is such a dramatic change, both in terms of families' everyday lives and the research we do.

I also see this as a huge opportunity that things have been changing so rapidly. That we have the power now to change the design of the technology kids are using, to make it healthier. If any of you have read my op-ed in *The Hill* from April. I really think that designing changes in the environment are the way we'll get much more impact, instead of asking each individual user or parent to change their each individual behavior.

I cited Tom Frieden's work. He was the CDC head a couple of years ago. He was the one who went to West Africa and saw Ebola patients. Like he's really legit. And he had this really great publication in 2009 talking about how there's this pyramid of things that we can do to improve Americans' well-being.

And if you're changing the environment through this really just changing the structures, and the everyday nudges that they get, and you're making the healthy decisions, the easiest default decisions. You're going to have so much more impact on children and families than by

at the very tip of that pyramid was me counseling a parent in clinic to try to change what app their child is using. So that's why I'm here. That's why I really believe in design change as a way to make this better.

So Common Sense Media has been serving how parents are engaging with media and mobile and interactive devices with kids. These data show that as of 2017 the majority of children under 8 had used a smartphone or tablet to play games, to use apps, or to watch videos. And parents are generally involved in this. That they had down-- 72% had downloaded an app for their child to use.

But a really important point here is that 37% of parents reported never or hardly ever playing or using mobile games or apps with their kids. This is much less compared to TV where the TV is this big screen in the living room with us, where we can all share it and watch it together and talk about it. Some of my research has looked at how kids just huddle around their tablets and exclude the parent from the interaction around it. It's much harder to sit and interact and know what your child is doing on a handheld device that they can take from room to room.

We did a study where we put audio recorders on kids up to the tween ages-- from toddlers to tweens. And we listened in basically on how they were talking about media with their parents. And it was very little. They were talking about things like turn that down, plug that in, that needs to be recharged, where's the charger. They were talking about things like, oh, there's so many things to watch, what should I watch? But they weren't really talking about any of the instructional mediation that we want parents to be doing to teach their kids about this digital environment.

Many times we heard kids on their devices and parents on their devices. So the takeaway from this is it's important not to assume that there's a parent by that child's side every time they are on their device, installing a new app, or making some sort of decision about the content that they're using. And I think that as of 2017, Common Sense Media reported that 20% of children find apps or games themselves.

I definitely see this plenty in clinic where I will often sidle up to a little kit and say what are you playing? And they'll say something like Zombie Kill Breaker or something like that. And the parent will be like what? What? How did you-- you're not supposed to install stuff like that. So there's a big disconnect happening between children's ease of access of what they can install and what their parents really want them to be playing.

So my research has really tried to describe the design of mobile apps to really try to highlight mismatches between the assumptions some of the designers might make and who little kids are and the way little kids think. So we did this content analysis of 135 apps that were marketed to-- meaning, they were in the five and under category, or in the app store or played by children under five years of age in some of our mobile sampling that we had done.

So there are a lot of mismatches we found. Here's a hidden ad in a sparkling present. I know it says sponsored, but if you're under five, most likely you can't read. So there's things here that are not really a fair way to be advertising to young kids. We also found plenty of banner ads that had adult appropriate content. This is bipolar facts. If you click that, you get to a website that's assuming you're an adult looking for information about mental illness.

We found lots of pop-up or interstitial ads that come up out of nowhere during gameplay and might have some violent themes, might have some guns, knives, sexy content. So it appeared that some of the ad networks were not really filtering out the ads that were appropriate for this five and under group. And we found lots of rewards to watch ads or in-app purchases.

And really, I highlight-- I know this conference is not about advertising, but I highlight this study because number one, it's showing this could be a source of inappropriate installs of age inappropriate apps for young kids. If you're sitting there playing a little toddler ABC game and you get a pop-up ad for something that's not really appropriate for young kids, a little immature brain and fingers might click that and depending on the settings that you have on your device, it might be pretty easy to install.

It also just highlights the fact that when you take adult-centered design, whether it's about monetization or ad networks or other things, and you just try to apply it wholesale to kids' media content, it's not appropriate. It's not taking into account children's unique needs. I mean, if you think about it, if you took-- think of a three to four-year-old that you know and think of a 30 to 40-year-old that you know. And think of how you might describe an advertising ID to them. It's totally different.

You wouldn't even know where to start with a three to four-year-old to help them understand what persistent identifiers even are. I mean, when I talk to a 3 to four-year-old in clinic, I'm like on the floor with them, playing with toys, drawing pictures. Their minds are magical. Their minds are expansive. They don't understand these abstractions that we as adults now cling to as rules. So it's really important not to make assumptions about what they might understand

based on what we understand.

So with that in mind, I want to talk a little bit about our ongoing study of preschool-aged kids in Michigan. We've recruited about 365 of them and we're following them over six months. We're almost done with data collection. I'm going to be presenting just our baseline data today.

And this is a really fun study because we are tracking what kids are doing on their mobile devices. We have about a third Android users. We have about 2/3 iOS users, 19 who never used mobile devices. And in our sample, about 35% have their own smartphone or tablet. So it's only that child exclusively using it. And the rest of them are shared with a parent usually or sometimes with a sibling.

So we're using this novel method that we've developed. For Android devices, we have an app called Chronicle and it queries the Google usage stats manager API and it sends a continuous stream of apps foreground-- which apps are in the foreground with a timestamp. And from this we can see what apps a child is playing, what time, how long. It's really fascinating.

And then from iOS devices, which don't allow this sort of tracking of the screen-time API, we do battery screenshots. So we have parents after a week, bring up their battery thing that shows how many minutes each app has been played that week. And then we took-- we've generated a list of different apps that each child has played.

We made sure it was truly the child playing those apps basically by asking the parents. At the end of a week, saying what apps did your child play this week if it was shared devices. If it was an unshared device that was just the child's tablet, we made sure that no one else had used the tablet that week.

And then I'm collaborating with Serge Egelman from Berkeley to use his method for analyzing data transmissions. I'm going to have to read this because I don't fully totally remember the language. But basically, he's using an instrumented Android environment using an app exerciser monkey tool and that allows them to capture apps' network traffic. So that's been really interesting because then we get to see what apps are actually transmitting in terms of data.

So this is our baseline data wave of what the most popular apps played. I've taken out things like settings or other kind of utility apps that we don't care as much about. But as far as Android devices, about 50% are using the YouTube main. So thank goodness YouTube is

making some of the changes that they are to really acknowledge that child users are using their platform and trying to clean out what is the child-directed content and what is not.

YouTube Kids was the most popular on iOS devices. But YouTube came in with a quarter of kids using YouTube. Browsers, quick search boxes-- those are also really popular. So about 15% to 20% of kids in our study are using Siri or the voice quick search box which also has privacy implications.

There's a lot of streaming video and then a bunch of-- lots and lots of games. So we have generated a list of over 500 apps played by all of our Android participants only. And it's probably double that for the amount of different apps that kids have downloaded and playing on their tablets or smartphones.

I want to highlight-- this is not to pick on any particular app or developer-- because we have a whole list of the different ones that are transmitting data. But I want to highlight the fact that lots of kids love Subway Surfers. I hear about it in clinic. I hear about it from my own kids. So there is-- it's listed as an everyone app. But from what we found, it had Android ID and advertising ID shared with different domains.

We also found that Children's Doctor Dentist, even though it is rated as an E-plus for everyone, but has children in the name, also was sharing the advertising ID with five different domains. So this is just information about the fact that a lot of these apps themselves probably yet are not really sure how to designate themselves as a general audience app or really identify when it's a child using them.

We also identified a lot of adult or mature apps played by kids. These are preschoolers who are three to four years old and we were finding a lot of things with guns. The Walking Dead Dead Yourself, Grandson, Granny, Kick the Buddy, Zombie Tsunami, Terrorist Shooter, 3D Knife Challenge. So kids are really getting their hands on a lot of age-inappropriate content. This is on Android devices. This is on iOS devices.

So some of these aren't necessarily too violent. I mean, Roblox is a very common app. But the kids love Jumpscare apps. They are really seeking that forbidden fruit. And if it's easy for them to access either through the app stores or through apps that are popping up as ads, as interstitial ads in their gameplay. We have to be aware that this is one avenue that they're getting access to it.

So just some examples-- these are ones that we ran through our data transmission protocol. That Gun Fu, Stickman is sharing advertising ID. Granny-- do you guys know Granny? She locks you in her house and you have to try and escape. And there are booby traps set everywhere. And it is-- I mean, my patients tell me they have nightmares about apps like this. And so yeah, but kids still access them. They're fascinated by them. And she shares your advertising ID and Android ID with two different domains.

Kick the Buddy is also a very common app that we've been seeing in our output. It's kind of like a voodoo doll that you can explode and kick and be violent with. So other than the content issues going on here, where I need to care about what preschoolers are doing with regard to exposure to violent content-- that's been associated with sleep problems or behavior problems-- I mostly also care about the fact that they're attracted to more mature apps and that these apps are more likely to have data trackers.

So some of the reasons I care about this mismatch between what children are accessing online and what they can actually understand there's a little bit of research that's been published about this. And there's a great review by Sonia Livingstone. She has an executive summary too. If you're interested, just search for her children's data and privacy online. I think that there's pretty good evidence that school-aged children through teens do not understand the complex ways that data are collected, analyzed, and used for commercial purposes.

In all the studies that Dr. Livingstone reviewed, children describe having a more personal or interpersonal conceptualization of privacy. Meaning, oh, someone might steal my password. Someone might share a private photo that I didn't want them to share. They don't understand the idea of an institution, like a school, having their data, or a social media platform having their data. So this is very important because we may be misleading them based on our current ways that we describe our privacy policies to them.

And there's been research also showing that, especially younger kids are more trusting of anthropomorphized technology. So their home assistants, little robots, and internet-connected toys, they treat them as more alive, and especially if it's convenient. Susan Gelman did this interesting study where they put a location tracker on kids' backpacks. Parents thought it was creepy and kids thought it was convenient. Great, I'm not going to lose my backpack anymore. So it's really important that we think about things from the child's perspective.

So there's also been some nice work done by the Information Commissioner's Office in

preparation for their age-appropriate design code where they've interviewed kids about what they think about their online data. Children report being uncomfortable with their data being used for targeted ads. And preschool children through teens believe they should have the right to erase or limit the use of their digital data. And this makes sense.

Your digital footprint is not just what app you downloaded that day. It can be linked with your school progress or your class Dojo behavioral progress. That apps can even capture our psychological profile. It can tell how impulsive we are, how hard workers or critical thinkers we are. I don't want my patients who have impulse control issues, who have immature frontal cortexes to be up against a really powerful ad network that has been able to collect data about them.

As far as the American Academy of Pediatrics, I wasn't going to discuss our upcoming advertising policy and privacy policy statement recommendations yet because they haven't yet been fully authorized. They're coming out in 2020. But these are the general principles. It's really important for industry, policymakers and parents to understand children's vulnerabilities to persuasion and the developmental limits of kids' critical reasoning about digital privacy. It's just much harder for them to get.

We also want to protect children from either manipulative or deceptive practices or just sloppy design that hasn't really taken into account who the users are. We want to help parents become more informed about the methods used to advertise to children and to collect data from children. And we also want there to be just improved design of the digital environment for kids, increased funding for PBS as a gold standard for privacy protections as well as non-commercial high quality programming for children.

And so I'm going to sum up by just taking together these ideas that we talked about with-- there's been this rapid change into children's digital environments. They've evolved so rapidly that research can't keep up, but also I'm sure privacy protections feels like you're constantly chasing this moving target. Our research shows that many young children use general audience apps and platforms which pose both the content-related and privacy concerns.

We're also finding that many child directed apps contain similar advertising and monetization and data sharing practices as adults and general audience apps. And so I'd really love for there to be more of a discussion about a children's design code that can be put towards the types of apps that we're hoping get into the hands of young children.

And I often when I'm talking to either regulators or folks from industry, I often hear, OK, so just parents need to just download this thing, so they can monitor what their kids are doing. Parents just need to be more on top of their kids. I do not want to put anything more on the shoulders of parents. American parents have the hardest job in the world. They have a lot more income inequality, housing insecurity, food insecurity than a lot of other parents in wealthy nations.

They already feel a lot of stress and pressure from the press or just our culture to make sure that they're raising really productive kids. So the best thing we can do is to design an environment that makes their children's digital choices and their own digital choices much more of a healthier design by default. I think we'll have a much more resilient set of children and society if we do that. Thank you.

[APPLAUSE]

PEDER MAGEE: Good morning. My name is Peder Magee. I'm an attorney in the FTC's Division of Privacy and Identity Protection. And with me is my colleague Jim Trilling, also from DPIP. We're going to be moderating today's first panel entitled, "State of the World of Children's Privacy." First, I'd like to thank Dr. Radesky for her presentation. It's very interesting.

And next I'd like to introduce our panelists. Their bios are included in the workshop materials so I'll be brief. We have Phyllis Marcus, who's a partner at Hunton, Andrews and Kurth. Phyllis is a former FTC attorney who worked on the 2013 COPPA rule amendments. Next we have Laura Moy, an Associate Professor and Associate Director of the Center on Privacy and Technology at Georgetown University Law Center.

We have Jo Pedder, who is Head of Regulatory Strategy at the United Kingdom Information Commissioner's Office. Next, Claire Quinn, Vice President of Compliance at PRIVO, which is one of the FTC approved safe harbor programs. Dr. Jenny Radesky, from whom we've just heard. And Janne Salminen, Senior Legal Counsel at Rovio Entertainment Corporation.

Jim and I will be guiding the discussion and directing questions, but I'm hoping that this will be a very interactive dialogue between the panelists. To kick off the discussion, Phyllis is going to provide an overview of COPPA and the California Consumer Privacy Act. And then Joe will talk about the European Union's General Data Protection Regulation and the UK's Age Appropriate Design Code. So with that, Phyllis.

PHYLLIS MARCUS: Thank you. Do I advance this way? So Commissioner Wilson did a wonderful job of setting up for all of us today the background that led to the enactment of the children's privacy laws. I won't go back and completely reinvent that. But I did just want to provide a slight scene setting for us for today so that we can see how we got here.

So as the commissioner said, in 1998, worried about the widespread collection of personal information from children-- and we'll talk about what a child actually is-- in a very rapid series of developments, the FTC recommended that legislation be enacted. And Congress and those of you in the room who were very involved at the time-- I'm looking at Parry right now-- no-- in almost an unheard of lightning speed round, Congress took it up and enacted the Children's Online Privacy Protection Act. I think there were four months between introduction and enactment.

And as the commissioner urged those who might be listening from afar here today, would that pace continue today. The statute is primarily enforced by the FTC and for a long time that's the way it was. And more recently, we've seen states come into the game in very big ways, including the most recent YouTube settlement which also involved the State of New York.

At the time that COPPA was enacted, there was a small debate about who would be covered. That is, who is a child? The statute settled on a cutoff at age 13. That is, a child is defined as someone who's under age 13. And it stayed that way since 1998 with some discussion as to whether that would change, but that's the way the line was drawn. As we'll hear today from Jo, there are other determinations around the world that have made different cutoffs. And California has made a slightly different decision as well. But for COPPA, the child is defined as under age 13.

So why is this important? The flip side of that is that it does not by its terms cover teens. And I know the FTC has been careful in its FAQs. There is an FDA very specifically that targets what about my teenagers-- what protections are there for them? Not necessarily any under COPPA, but there's a lot of room, as we'll talk about today, for sites that are directed to teens and that may have a great number of younger children engaged.

One of the open questions-- I'll just throw it out there-- and [? Jana ?] and I were talking about this in the green room-- is how this interacts with website's terms of service which visitors to websites are required to accept in most cases and form a contract. If you have a teen who can consent to her own data collection but can't consent to the terms of a website, it's always been

an interesting question about the interplay there.

Another big question that we will discuss today is what is covered? The body of sites that are covered are those that are directed to children that are under age 13. And there's some widening or contracting of those categories or sites that have actual knowledge that they're collecting personal information from children. So perhaps it used to be that there was a bright line world. Now that world is changing a little bit. And I'm sure we'll talk today about what kind of certainty website operators are seeking as they look to comply with COPPA in the current age.

Another thing going off of what was said today by Dr. Radesky is that COPPA does not prohibit children's online activities, but it does require parental consent to the collection of personal information from children. There is built into the statute-- not just the rule, but the statute-- a data minimization principle. That is, an operator should not condition a child's participation in the activity on the collection of more than the personal information that is required to drive that activity. And so perhaps there's some room today to talk about data minimization principles and their prominence within the rule.

Here are for those of you who don't know, in a simple way, the six requirements for COPPA. I won't go through them, but hopefully if the slides are available--

PEDER MAGEE: Yes, they will be.

PHYLLIS MARCUS: --subsequently. These are the six dos and don'ts of what you have to do to comply with COPPA. It makes it look simple.

[LAUGHTER]

But one of the things that Peder and Jim asked me to talk about was what changed in 2013. And you heard Commissioner Wilson talk about the protections that were enacted in 2013. She issued a lovely shot across the bow for those in the room and beyond that the Commission does not intend to weaken the protections that were enacted. So for those of you who need a refresher, here is what was laid out in one slide and what changed in 2013.

New forms of personal information were included. The most complex of those forms were that persistent identifiers that can be used to recognize a user over time and across different websites or online services were included in the definition of personal information. And the

basic handy four-word summary of that is that behavioral advertising is covered under the revised rule from 2013.

Also, photos, videos, and audio files containing a child's image or voice and geolocation information. More precise, geolocation information sufficient to identify a street name and the name of a city or town. So if you want to tick off those three things, you'll know a lot about COPPA.

There are-- I'll call them carve-outs-- we can debate how we term them. There was a recognition that some sites may be designed for children but also for others to use them, and the question was how the rule will treat differing visitors to those sites. And there was a very specific set of recognition that where those sites employ an age screen, the sites can sort their visitors into 13 and overs, under 13s, and treat those different groups differently in terms of the information that's collected from them.

We'll talk a lot today, I'm sure, about support for internal operations. There was a specific laundry list of activities that were recognized to be those necessary to run the activity behind the scenes. One of the things that was built into the 2013 rule change was a process by which operators and others could apply to the commission to expand that list of support for internal operations. I don't think anybody has done that.

PEDER MAGEE: Yeah, I don't believe on internal operations.

PHYLLIS MARCUS: So nobody took the commission up on their invitation. More recently the Commission issued enforcement-- refrain from enforcement policy-- how do we call it? How do you call it?

PEDER MAGEE: Enforcement policy statement.

PHYLLIS MARCUS: Enforcement policy statement regarding voice as a replacement for search. And I'm sure that will be discussed today as well. Another mechanism that was built into the 2013 rule review was the method by which operators, service providers, others, technology providers in the field could apply to the commission to administer new forms of parental consent. And in this case, several entities have applied to the commission. And the commission has approved some and rejected others.

So new forms of parental consent, in addition to the ones that were enumerated originally, include government ID matching, knowledge-based authentication questions, and face match to verified photo identification. And that process remains open. So those technology providers

in the room who are interested in really creative approaches might apply to the commission for recognition and codification of their processes.

The commission has issued a number of cases-- been very active in this field-- clarifying the coverage of COPPA. So I just list a couple of those in shorthand here. IoT devices through the *Vtech* case. Ad networks were intended to be covered by the 2013 rule review and here are some of the cases the commission has issued. And platforms-- the big splash over the past month with the YouTube action. So should I move on to California now?

PEDER MAGEE: Yeah.

PHYLLIS MARCUS: So most of you I'm sure everyone who's listening and is in the room knows that California has enacted its own very comprehensive privacy legislation that goes into effect on January 1. The intricacies could fill volumes but I've pulled out the one that pertains to children.

In general, the California act provides an opt-out for the sale of personal information. But when it comes to teens and younger children, that opt-out right becomes an opt-in right. And it's an opt-in right where the business has actual knowledge of the consumer's age.

Query what actual knowledge means. It may or may not overlap with what it means in the COPPA context. But that's not all. There is a sub or major clarification to the California rule that says that businesses that willfully disregard a consumer's age are held to have had actual knowledge of the age. And again, there is no definition of willful disregard.

So there's been quite a bit of discussion in the legal field as to what the obligations might be under the California rule with respect to sites and services that appeal to children under age 16 or that are directed to them. And I posit here, in my last bullet, that arguably businesses that have reason to believe that children under age 16 use their services will need to implement an age gate mechanism to sort their users into over and under.

And based on the California rule, services that are-- where a service has actual knowledge of the consumer's age and that age is under age 13, you get a COPPA-like acknowledgment that a parent or guardian must affirmatively authorize the sale of the information for teens aged 13 to 16. There's a sliding scale. The teen, herself or himself, must affirmatively authorize the sale. And that's where we stand.

PEDER MAGEE: Great. Thank you very much, Phyllis. And if you could hand this down to Jo. She's going to

give us--

JO PEDDER: [INAUDIBLE] key--

PEDER MAGEE: Oh, I'm sorry. You don't have slides. You don't need that.

JO PEDDER: No. Do I need-- Oh, it's on. OK. Well, thank you very much for inviting me to participate in the workshop today. The ICO has got a really good relationship with FTC colleagues and a history of collaboration, so it's great to be able to give the UK perspective for the review of the COPPA rule. Just for anyone who doesn't know the ICO is the UK's regulator for information rights legislation. We cover data protection and freedom of information regimes.

And over the next few minutes, I just want to give a brief overview of our children's privacy regime, and in particular talk a bit about the work that the office is doing in this space. Our Information Commissioner, Elizabeth Denham, has made it clear that this is one of the most important files or issues currently on her desk. And the reason for that is that we know, and we've heard from Dr. Radesky, how much kids use online services apps and various other information society services.

SPEAKER 1: Jo, can you move your microphone a little closer?

JO PEDDER: Yeah. And we know that kids use tablets and iPhones before they can ride a bike. So our concern as the regulator is the collection and use of data in ways that kids are not always aware is happening or in ways that are detrimental to them. But we don't want to keep kids out of the digital world. It would be too late even if we tried to do that. What we want to do is to empower them and keep them safe within it.

So just briefly, the UK data protection regime is set out in three pieces of legislation-- the General Data Protection Regulation; the Data Protection Act of 2018, which sits alongside the GDPR and tailors it for the UK context; and the Privacy and Electronic Communications Regulations, which cover the rules on marketing, cookie technologies, and the like. Before GDPR, I think it's fair to say there was relatively little consideration of children in the legislative regime. It really wasn't a particularly big focus. But that couldn't be more different now post-GDPR.

GDPR was generated through a recognition that developments in technology and new innovative ways of processing personal data meant that the data protection regime needed a reboot. And GDPR recognized that kids, particularly, needed different treatment and

recognition as opposed to adults. There's a particular recital that sets out the purpose and intent of the legislation.

PEDER MAGEE: Jo, I think the microphone should be a little closer to you.

JO PEDDER: Sorry. Is that any better?

PEDER MAGEE: Yeah. Thank you.

JO PEDDER: And it says that children merit particular specific protection because they may be less aware of the risks associated and the consequences of the processing of their data. It also says that where information society services are offered directly to a child and the basis for the processing is consent, then parental authorization is required if the child is under 16.

Member states then have an option to lower that age to 13-- if they wish anywhere between 13 and 16. And the UK has done that and set that consent requirement at 13. So there are some similarities with COPPA. And then GDPR also requires privacy notices to be really clear and concise so that children can understand them.

And in addition to the GDPR, UK parliament decided to place a duty on the information commissioner to create the Age Appropriate Design Code, which is a set of standards that sets out for information society services the standards that they're expected to meet when they process children's data. I think the background to that was that parliament recognized the reality that kids are experiencing in the digital world.

We heard figures already, but some that we often refer to are from an Ofcom study in 2017, which said that 53% of kids between the age of three and four are online, and that goes up to 99% of 12 to 15-year-olds. And separate research also estimates that by the time a child reaches 18, there are approximately 70,000 data points held on them.

So where kids are asked to declare their age and they're honest about that, they often don't actually experience any difference in the service that they receive once they've declared how old they are. So parliament decided we need to think again and take a more holistic design that approach that builds on the requirements of the GDPR and that's why we're developing the code.

So as I've said, the code comprises 16 design standards rooted in the requirements of GDPR, but that explain then how it applies to kids' data. It's slightly different in that it takes a more

expansive view and says that it's for information society services likely to be accessed by a child. So it covers apps, connected toys, online gaming, educational and news websites.

It contains practical guidance and sets out what we actually expect of these services. And although it's the first of its kind, I think it's gaining a lot of interest and is generally moving in the direction of travel. And we've already heard some advice about the importance of the design taking the lead.

The code is on a statutory footing, which means that the ICO and the courts have to take it into consideration where it's relevant when they're considering any regulatory action. And if an organization fails to comply with the code, and in doing so, it also breaches GDPR, then we can use our regulatory teeth. We have considerable enforcement powers that include enforcement or stop notices. And we can impose penalties of up to 20 million euro or 4% of global turnover, whichever is higher.

As was already mentioned, we followed an open process in trying to develop the code. We've consulted with a broad range of stakeholders across different sectors. And we really did take on board the fact that parents and kids often don't feel their voice is heard in the development of regulations. So that's why we commissioned the specific research talking with kids about how they feel about the rules.

The standards are all interrelated and cumulative, and an organization needs to apply them all to show that they are actually complying. Some of the general standards include those aimed at governance and accountability requirements, developing online tools to help kids actually exercise their rights, and one important one which is around detrimental use of data. So this states that organizations must not use kids' personal data in ways that are obviously detrimental to them or that goes against established industry standards, or other codes, or government advice.

And then there are more specific standards around transparency, connected toys, and nudge techniques. There isn't time to go through all of them today, but just to mention four particular standards that are pretty key. First, we've got one that says that organizations must make the best interests of the child a primary consideration when they're designing and developing the services. And this takes into account our obligations under the United Nations Convention on the Rights of the Child. And that defines a child as anyone who's under the age of 18.

It requires organizations to take into account as well the differing needs of children as they grow and develop. So the way that we've done this in the code is to set out age bands which reflect the different needs as kids grow up and where that's relevant to the particular standard. So for instance, around privacy notices and transparency, we've given advice for the different age brackets about what to do.

Secondly, we've got an age appropriate application, and this requires organizations to need to understand the age range of the users and their different needs. They need to take a risk-based approach to recognizing the age of their users. So that means establishing the age of the user with a level of certainty that's proportionate to the risk of the processing that's going on and then tailoring the service to the needs of that particular user. Or if an organization is not able to do that, they can apply the standard to all users of the code. And that then ensures that users who may have lied about their age or where they don't have great certainty will still afford a level of protection.

The third standard that I want to mention is default settings. So privacy settings are useful where kids are able to genuinely exercise choice over whether their data is used. This is often found where it's outside of the core service provision and is being used to enhance or develop and personalize a service. Many kids will just accept those default settings. They won't change them. So it's really important in our view that organizations set them at high privacy by default. This offers the highest level of protection and at the lowest data cost. And it ensures that privacy is baked in rather than bolted on.

And then finally, geolocation is another one of the key standards. This deals with the fact that persistent sharing of location can mean that kids feel a diminished sense of their own private space. So unless geolocation is core to the service for something like maps-- map apps-- it should be subject to a setting that's off by default. And children should also be given a sign that they're being tracked or that the geolocation is on. And where their location is visible to others, that should default back to off after every individual use.

Just really quickly to cover the feedback we've had on the code-- it's generally liked. Nobody's said it's not necessary. People like the principles-based approach, and the flexibility that's built in, and the fact that we've got the best interest of the child as a key principle. They like the privacy by default and the recognition of different development stages. There are a few concerns around the cost of implementation and a worry that age verification by default may become the default. And there's also some questions about the time to implement-- how long

we'll give organizations to do that.

We're reflecting on that feedback and we're redrafting the code. We're also developing a report that sets out the headlines and our responses to them. Once we've done that, we will lay the code before parliament and it will have the opportunity to consider it. And if it's accepted, it will then be issued after 40 days and then come into effect 21 days later. And then we will set the transitional provision timescale, which could be anything up to 12 months. Thank you.

PEDER MAGEE: Thanks very much. Great. Well, thanks Phyllis and Joe. So we just heard about some other legal regimes approach to children's privacy. And to get the discussion started, my first question is, as the commission undertakes its COPPA rule review, are there any concepts from the other laws that you would recommend incorporating into COPPA or that should inform our review? We heard things like default settings, willful disregard, or a requirement to do a little bit more about looking into your users' age-- things like that. And maybe, Laura, could you start? And then if the other panelists could weigh in, that would be great.

LAURA MOY: Sure. Yeah. Thank you and good morning. So I wanted to start out maybe by talking about a few trends that I see in looking at these other laws that we've just discussed. We've just discussed four other laws and they are-- well, I'm sorry-- three other laws. And there are new components to all of them. And I think that there are some trends that are common across them that it's worth talking about because it might inform, and I would argue it should inform, what the FTC does, if anything, with COPPA moving forward.

So the first is that-- I don't think that this is news to anybody-- but the fact that we're seeing multiple laws being passed all over the world related to privacy right now shows that we need more privacy protection not less, right? These laws are all universally about protecting people, and in some cases protecting children specifically, from inappropriate collection and use of information and providing people with more control and fostering trust online.

And the trend toward more laws in this area shows that we don't have that trust yet. We just don't have it. And so we need arguably more regulation. And we need to figure out how to actually provide the trust that people need in order to participate fully online.

So the second trend that I see across these is that I think that all of these laws that we just discussed have components of them that indicates a trend toward providing more than mere notice and consent. I mean-- and in the US, we have had a tradition of focusing on the notice

and consent aspects of our privacy regulatory regimes in the past. But that's not what we're seeing in these global trends.

So Jo was just telling us about the UK code, where we're trying to prevent detrimental uses of data, trying to ensure that privacy is designed into products. The GDPR includes some of the FIPS, including purpose specification and use limitation requiring entities to state at the outset what they need information for and then limiting the collection of-- or limiting the use of information that is collected to fulfilling those purposes. So something more than just consent.

And something that I think is really interesting about COPPA is that COPPA has this. So COPPA does have these provisions in it that we don't focus on a lot. We tend to speak in these conversations about the notice and consent provisions of COPPA. But COPPA does prohibit conditioning a child's participation in an online activity on the child disclosing more personal information than is reasonably necessary. And so that is like purpose specification and use limitation. It's built right into the statute.

And so when Dr. Radesky was giving some examples at the outset and you look at the fact that Subway Surfers is collecting-- requires full network access and is collecting information about network connectivity. This Children's Doctor Dentist app is accessing storage on the device. There are these questions that already arise not just about notice and consent, but about whether things like this are compliant with COPPA, because COPPA does already have built in something that is-- we see on this global trend-- it does already have these restrictions built in to prohibit information collection that exceeds what's reasonably necessary to provide a service.

And COPPA, of course, also has this requirement to protect the confidentiality, security, and integrity of personal information. So that's something that we see asked at-- a global level asked in GDPR. And we have it in COPPA. And perhaps the FTC, as it moves forward with this rulemaking, could look at how some of these other regimes have thought about what reasonably necessary information collection looks like, what reasonable protection of confidentiality looks like, and to flesh out some of the rules that implement those provisions of the statute, in addition to notice and consent.

And then a third trend is I think this idea that we need more information to make informed policy decisions about privacy. So all of these regimes have an access right built in so that users not only get to consent to information collection on a case by case basis, but also can

request information about what data about them an entity holds to inform decision-making at a broader level. We also have that in COPPA.

And so taking that out a step and looking at what authority the agency has, this agency also has the ability to do that on behalf of all of us. So in forums like this workshop, which is a great place to collect information, but also through its 6(b) authority, which it can use, and I would argue should use, to collect more information about what entities are that are child-directed-- and maybe entities that are not child-directed-- what information about children they are collecting for what purposes, and to just build a broader knowledge base.

And then the fourth thing which is a relatively small or smaller on a scale of abstraction-- more concrete thing I should say-- is that all of these in all of the regimes that we just talked about, there is an increasing discussion of what protection for teens should look like. I mean, we know that kids between the age of 13 and 16-- teenagers, in general-- we have to draw the line somewhere-- but we know that teenagers, in general, they lack a lot of the cognitive and judgment abilities that adults have.

And digital storage is extremely cheap information about what we do online, potentially has the ability to live forever, and we don't want teens maybe to have the rest of their lives impacted negatively by something that they did in a moment of poor judgment when they were 14 or 15 years old. So just a few trends and things to think about. Thanks.

PEDER MAGEE: Great. Claire, did you want to--

CLAIRE QUINN: Yes, thank you, Peder. There's a few points I think I'd like to raise looking at the GDPR in relation to COPPA and children. What I think is there are several areas that we can learn from. The age of the child, obviously. A child is still a child at 13, so we do need to look at some special protections for that age group. And I think we see that in the CCPA and the GDPR, and there's learnings to be had from that.

To Laura's point, I think the rights are highly significant in GDPR. The fact that the child has these rights is very important. And I think looking at some of them-- the right to be forgotten is absolutely vital when you think what children can share, what they can do online. And that has an impact for the rest of their lives. So we need to look at those rights. We need to understand what rights a child should have. And right to be forgotten, I think, is a key one.

And talking also a little bit to the transparency issue-- the transparency principle in the GDPR

is-- it's strong. I think it's a great requirement. And I think you cannot have-- or we know you cannot have informed valid consent unless you've been transparent about what's happening. We don't see privacy policies that are clear and accessible. At safe harbor, we spent a lot of time working in that area. A child is not going to understand if the parent doesn't even understand.

And we very much welcome the code in that sense in that we are building into our program children's privacy notices, just-in-time notices, information that the child can understand. And I think the GDPR speaks very clearly to this. The guidance is provide something that they can understand. You can use animation. You can use signposts. But if-- the child and the parent need to be able to understand what is happening in a service and we don't see a lot of that right now. So I think that those three elements for me are important learnings from the GDPR that we could use and work on.

PEDER MAGEE: That's great. Anyone else would like to weigh in on ideas we can take from the other regimes and inform our rule review process? Phyllis?

PHYLLIS MARCUS: Let's wait and see how the conversation develops.

[LAUGHTER]

PEDER MAGEE: Janne.

JANNE SALMINEN: Good morning. Thanks. First of all, thanks for inviting me here. I came all the way from Finland, land of the polar bears and whatnot. So I work for Rovio Entertainment Corporation. Those of you who don't recognize that name, probably recognize one of our most popular products-- the Angry Birds mobile games.

So from our point of view, because we're mostly on the receiving end of all the regulation-- hopefully, not enforcement action, but only regulation-- so when looking different-- because we operate on a global scale. Essentially, when we launch a game through any of the app stores, whether Google Play or Apple App Store, it goes to well over 100 countries, I think-- well over 100.

So when we talk about children, for us-- for example, China just enacted their new legislation October 1-- that's 14 years. If you talk to UNICEF, which we talk a lot-- we're doing a lot of good stuff with UNICEF-- they're saying it's going to be 18. A lot of the international treaties on

children-- sorry, it's going to be 18. GDPR-- the default setting is 16, whereas some countries it's 13, some where it's 14, 15. So California-- 13 or 16, depending what you're doing. So for someone operating in the field, consistency would be really great.

[LAUGHTER]

Because the way it works, of course, because essentially-- especially in the free to play world, you're operating with a lot of volume. So in order to operate your business, you don't want to tailor-- you don't want to have a lot of versions of your product. So you essentially end up going with one globalized [INAUDIBLE]. So you have to then decide that do you want to go with the highest age limit which will effectively-- in my opinion, will limit the availability of apps to kids, because the industry has to choose the highest age limit and go with that.

PEDER MAGEE: All right. Thank you. So it sounds like there's some agreement that maybe ideas like right to be forgotten, transparency, age consistency are things we could potentially take from the other regimes and at least inform our-- inform the agency as we undertake the rule review process. Jim, do you want to--

JIM TRILLING: Sure. Continuing along that same theme of consistency or lack thereof-- so we've heard this morning that COPPA, of course, is triggered where an entity operates a child-directed website or online service, or where an entity has actual knowledge of collecting personal information from a child. And Jo told us that the GDPR focuses on whether an entity is offering an information society service directly to a child, and that the UK Age Appropriate Design Code will focus on services likely to be accessed by children.

And then to add to that, Phyllis pointed out that the CCPA's approach equates a business's willful disregard of a consumer's age with actual knowledge if the consumer is under 16. Are any of those approaches better than others and why or why not? And any thoughts on how different or similar they are to each other.

LAURA MOY: So I think from a consumer advocate standpoint, one of the problems-- one of the big challenges with the actual knowledge standard is that in some ways it creates arguably the wrong incentive for companies in terms of figuring out whether or not they have children on the platform. So if you have looked at the criteria for child-directed and you think that you're not child-directed, you think there's a possibility that there's children on your site or that maybe there might even be a fair number of children on your site or service, then you might-- one

might reasonably conclude that the best thing to do is to avoid developing actual knowledge that there are, in fact, children using the site or service for as long as possible, because as soon as you know that, then you do incur additional legal requirements.

And something that's interesting-- so you know-- and there's not an easy answer to this problem. This is really hard. And this arises in a lot of privacy laws, not just COPPA, and a lot of-- I mean, a lot of laws in general have it that are based on what a party knows or does not know. But the willful disregard standard is at least interesting in that it is attempting to address that. So it's attempting to address that in something that looks like burden-shifting, essentially.

So there now is an affirmative, or arguably-- we don't-- it hasn't been actually interpreted yet, if I'm not mistaken-- yeah-- there's arguably an affirmative obligation now for parties to take that step and find out. And from a consumer standpoint, that seems like a step in the right direction.

JO PEDDER: Can I just add to that? I'd just say that I think taking that approach of deliberately trying to limit it also misses an opportunity that organizations have to actually build trust and get child users on board early but with the right protections. And that's where our design approach comes in. That it is understanding the users and putting those right default settings in place, et cetera, that I talked about. But that then also develops their potential for a wider consumer base that then builds that trust and may use them for a longer time.

JIM TRILLING: Sure, Claire.

CLAIRE QUINN: And I would say that there's much confusion over audience definition. And we have seen for far too long terms and conditions that state if you're 13, you're not allowed in. Blocking children from things where they are very likely to be attracted to them. And I think that there is a responsibility in industry and for us to do the right work to open up with restrictive services or appropriate age services when we know that children are accessing these sites. It is not good enough to continue to say I'm general audience and put in your terms of service no 13-- you 13s welcome here, because we've seen this for far too long.

So we don't have all the answers. There's much confusion over it. But I think it's something that needs to be debated. I think we need to look at the fact that these sites need to take responsibility, platforms need to take responsibility for child users. And that the willful disregard is a great concept because there is much willful disregard going on today. You should open up and you should-- it might be age verification. If you're low risk, it might be an age gate. It

depends on what's happening in the service.

Age gates are fine for low risk content, low risk processing of personal information and data. But they're not OK when there's a high risk to a child, when it's to the detriment of the child. We all know that kids game age gates very easily. We have evidence of that on our social platforms. So I think there is much work to be done around that. And I think that there is a responsibility needed to be taken, particularly when you are actually offering content for children and saying that you're general audience.

JIM TRILLING: Phyllis, did you want to weigh in on that?

PHYLLIS MARCUS: I'll weigh in. You might not be happy.

[LAUGHING]

JIM TRILLING: Moving on.

[LAUGHTER]

PHYLLIS MARCUS: I would argue that with your recent enforcement actions, I don't think the FTC necessarily feels hamstrung by the current definitions. And without importing some of what's happening internationally, it seems that there is some flexibility in defining the reach of the rule to, arguably, the same kinds of services without the definitions that are being presented by the GDPR, for example, or the UK ICO code.

And the flexibility seems to be in maybe some uncertainty around what form of actual knowledge actually is required or an expansion to sites that have a significant number of children already. I know there are a number of factors in weighing how a site is directed to kids, but buried within those factors certainly seems to be the flexibility on the part of the agency to approach cases that might not have been so obvious in a prior generation of COPPA enforcement.

JIM TRILLING: Since you've raised that point, Phyllis, how should evidence regarding the usage of a service by a significant number of children factor in to a determination as to whether or not the services child-directed or how should it factor in to actual knowledge, how should it factor in in general to a determination that the service is covered by COPPA?

PHYLLIS MARCUS: Well, you have two very different buckets and they used to be very distinct. And they're moving closer and closer together now so that there might or might not be overlap. The statute says actual knowledge that you have taken personal information from a child. It's very one on one transactional. The child-directed factors are such that-- in a way, it's kind of like a minestrone soup-- you throw it all in and something comes out. But among the factors are competent and reliable empirical evidence of audience composition. And so that's a relatively rigorous line.

I know that the past-- one of the more recent enforcement actions against Musical.ly indicated that there were-- I think the quote was a "significant percentage of children," without that amount being defined. And so arguably that was competent and reliable evidence that established that there were some threshold of children engaging in this service. Back in 2011, '12, '13, the commission declined to pick a bright line, and say that above this line, you would have a site or service directed to kids. But it is a factor and it now has informed a particular case.

So I don't know that I have an answer for it. I just know that people are seeking some certainty and there is some confusion as to which bucket you fall into. And when you're planning your services, you do need to know whether you are or you aren't-- and if you are, there are an awful lot of protections you need to enact before engaging.

LAURA MOY: And so I think I'll also just add a couple thoughts. So one is that in at least one of those cases, too, you had a company that was telling other parties that its platform was a good place to reach kids. So I mean, notwithstanding the application of the factor test, or the question of whether it's a general audience site or child-directed, if you are telling marketers that this site or service is a good place to reach kids, then there's-- it's a slam dunk argument that you're child-directed. So at least-- so there is at least-- there at least should not be ambiguity with respect to that.

And then the other thing-- so I think that this also raises a good question about the complexities of applying both the child-directed and the actual knowledge standard when dealing with multiple parties operating on the same platform. And it's one of the complexities that has kind of become-- gotten worse in over the last several years. It's just-- it's harder sometimes to tell which party has the knowledge or which party is child-directed, and which party or parties are collecting the information and whether they're all doing so-- that they're all acting in concert-- whether they're all acting in a way where they are aware of what the other parties know, such that they can coordinate to comply with COPPA.

And so I just wanted to bring this back then for a second to the reasonably necessary collection standard, and just say that that reasonably necessary collection standard then applies to the primary site or service and it needs to be aware-- or maybe in some cases with a content provider that is using another platform-- and it needs to be aware of what information collection is taking place by other parties that are operate-- that are also operating the same site or service or that are acting in concert to offer the site or service in order to ensure that it is compliant with this prohibition on collecting more information than is reasonably necessary to provide the site or service.

And then finally, just to-- not to sound like a broken record-- but these are complexities that would be served I believe by greater information collection on the part of this agency, which does have this really robust 6(b) authority to collect more information, build a much more detailed picture about how information collection is taking place, and what sites or services know or don't know about the age of the users on their sites.

PEDER MAGEE: Thanks. And actually just-- that gives us a good opportunity to pose one of the questions we got on Twitter, which I think is relevant to what you were just saying. And the question is what does-- should reasonable collection of information look like? And maybe we can start on the other end. Janne or Dr. Radesky, if you guys want to weigh in.

JANNE SALMINEN: Yeah, I can probably try and answer first. I mean, of course, my background is in mobile app development. So, of course, anything you do on web is a lot different. But for a mobile app developer and publisher operating on a global scale-- so privacy-- and I'm talking privacy in general. I mean, children's privacy is one thing. It's a subset of privacy in general. So privacy is really a process.

So a lot of times people think this is now the counsel is [INAUDIBLE] this process and telling the tech teams how to operate when it's really the other way around. So this is really-- I mean, we will, of course, advise our tech teams, but it comes down to the design of the product, or, in our case, the game. So we try to collect as little as possible.

We're a big fan of data minimization. So we do not know our end users. We do not collect their names, their pictures, their addresses. To us, they are more or less anonymous. We, of course, in order to operate the games, we need certain data, but that's typically just numerical identifiers.

So for example, in relation to the GDPR coming around, we organized in Finland these-- well, workshops like this, but several meetings. We had tens of mobile developers and publishers sitting together. We also invited the Finish Data Protection Authority to join in to understand what is expected of us. We're-- right now Rovio is also organizing a similar event for the California legislation. So we want to understand how it affects the business and what can we do about it.

For example, we had-- back in the day we had a Rovio account where you could register in the games. It's now gone. We took it out. So it is no longer there. And, for example, we put a lot of effort in-- you've probably seen this where, especially in Europe, if you request your data from a service, they-- please send us a copy of your passport, and what your address, and whatnot, and then we'll maybe have a look at three weeks from now. So we tried not to do that.

So we're doing everything through the app. So the best way to identify a person is essentially through the game that the person is using anyway. So we have automated everything. So there's a button that you go to Settings. You can ask my data to be deleted. You can ask for not to get personalized offers. Everything's there. It's tokenized. Again, we have no idea who the person is other than a string of numbers and we're very happy with that. It's working quite awesomely. So--

[LAUGHTER]

--thanks to our tech team. So, of course, we get every now and then approached by email. But for example, if you were to-- if you're a player of Angry Birds, you would approach us, send us a copy of your passport, we wouldn't know what to do with that because we do not-- that information doesn't mean anything to us. But now you just provided us with this information now we have to deal with.

So data minimization really is the key in our opinion. And, of course, when you take that to the topic of the day-- the children's privacy-- same thing works there. We do not collect any more data than is absolutely necessary to operate the service. And that's what we've tried to do.

For example, there's ample opportunity-- lot of products out there have Facebook login buttons. And now with probably the platforms are now providing-- they want services like Apple's-- the Apple's login service. So we only collect the data we need to log and synchronize progress through different devices. There's an opportunity for the industry to collect more data

there. We try not to do that, because again, we don't want the data.

And there's the-- what I'm hoping that doesn't happen is the unintended consequences of regulation. That by regulating the business more, companies like us who are putting a lot of effort in data minimization, we actually have to start now collecting more data. So willful disregard-- what does it mean in practice? We, of course, want to see the California AG's guidance on that.

But, for example, with the CCPA, if you look at the California residency that the CCPA applies to, it's for example, California residents who are outside California traveling. So do we now need to start logging IP addresses of where people are? Do we now need to start profiling people in order to comply with the legislation? I hope not, because that's very counter-intuitive and really goes against the idea of data minimization.

PEDER MAGEE: That's interesting the tension between wanting to minimize the amount of data but then potentially having to collect more data to comply with additional regulations. Dr. Radesky, did you want to--

JENNY RADESKY: Yeah, I think coming at this from a medical research background, I find that the IRB, knowing that we are doing research with children, requires us to have data minimization to begin with. And they have so many different safeguards that we need to take to show that we know how to protect vulnerable populations. So hearing about all the after the fact, finding out that your users were children, or some of the research that I presented today that's like, oh-oh, little kids are using this, I think is a less efficient way of managing the problem.

Instead I really like the idea of having a child design guide or an age appropriate design code because it's starting from the beginning, and baking it into and designing it into the products that kids would be using. And if it's your intention as a developer, I want kids-- I know and I want kids to be using this product, then to use data minimization standards.

So to answer that question about how much data is really necessary-- I first started thinking about this last year when we did our in app advertising study. We started looking at the permissions that different apps were requesting from our research devices. And some of them, like the Masha and the Bear apps, were asking for location. And there was no reason in the app that they would need location. And so we were looking at which of the dangerous permissions apps were asking for when it didn't seem that they needed that at all to actually make the app run.

. .

I was fortunate to talk to Jeremy Roberts from PBS Kids last week about what they do. How do they-- basically they hash up the device identifier so it's not at all traceable to the kids. It's something that they can use to make their app better or to know who-- how much their users are using their apps or for how long and how that engagement is, but it's not something that could ever be-- if they were hacked, it's not anything that could be traced back to the child or connected with other data that's been collected about the child.

So I've also talked with Toca Boca, because our output showed that device ID was being shared with Crashlytics. And I wanted to know how do you know how Crashlytics is using this? I understand you need app analytics, but you-- what sort of contract do you have to make sure that Crashlytics then isn't sharing it with anyone else and after how much time it's destroyed?

Because we have those same questions asked of us in the IRB review process whenever we're working with children's data. When are you going to destroy it? Where is it going to be stored? How many different safeguards can you put into place to make sure that this-- there's no loss of confidentiality to our research participants?

And that's why I also think it shouldn't only be up to the app developers to be making these design choices. Whenever I'm thinking of where the design changes should be, the app stores are a huge place. And I'm grateful that Google Play has talked with me a lot about the changes that they've made with their app stores to try to have the apps' developers themselves verify that they want to be a child-directed app and to be able to then maybe location by location, depending on what the age restrictions are, be able to only really deliver the age appropriate apps to kids that will do the least amount of data collection and the least of other advertising practices that are inappropriate for kids.

And finally, I just think that there's going to be a change in the way that consumers are expecting-- they're going to want more ethical tech design. They're going to want to know and expect that there's going to be-- I can delete my data button, and I can review what you've collected about me, and I can see the transparency of, oh, all these ad networks know that I love Delta Airlines. So there's-- I think that consumers are really going to become smarter about this. And so if you're an app developer, it's probably in your best interest to become one of these companies that's more trusted in that way.

PEDER MAGEE: Thank you. I think Claire wanted to weigh in. And we're starting to get pressed a little bit for

time and I do want to cover a couple of other things. So if you want to quickly weigh in.

CLAIRE QUINN: I'll be quick. I just want to say we very much understand what's happening with PBS because we actually work with them and provide the technology for them for PBS Kids. And actually, Toca Boca is one of our members, and I can very much speak to the position with Crashlytics in those apps.

But what I think is important is we see-- we hear a lot of pushback from industry that we can't collect age because it goes against the data minimization principle. But there are a lot of creative ways to understand that you have child users that don't necessarily go to collecting lots more data about that child. Within our technology side of the house, we're doing a lot of work around establishing audience and how to go about that. There are schools with databases. There are all sorts of organizations where we know these are children.

And what I think is really important here is neutral third parties need to look at establishing the age and the consent. We need to look at ways to do that that are creative. And there are opportunities for that without collecting huge amounts of data. You can flag that these children are in a particular age group and then treat them accordingly. You don't necessarily have to collect a huge amount of data on them.

If you just say, well, we're not doing anything, we're not collecting any data, it very much limits what an Apple service can do, and it limits their business, and it may mean that the child doesn't get such a great experience. So I think there are ways to do all of this, and we can discuss and debate those and reach different conclusions that will really help industry and protect kids at the same time.

PEDER MAGEE: Great. Thank you. Just as I said, we're getting a little pressed for time. We want to cover a couple of other topics. One of which is the safe harbors under COPPA. When Congress enacted the legislation, it included a safe harbor provision in the statute to incentivize self-regulation. And the safe harbors are a significant part of the landscape from COPPA's standpoint.

So we have-- that being said, we have heard some criticism of the safe harbors around things like transparency, and concerns about organizations potentially forum shopping and trying to find the easiest safe harbor. And I would just like to hear from the panelists on how they think the safe harbors are working, whether they're being effective, what types of improvements, if any, should we consider in the rule review. Maybe, Phyllis, do you want to start that--

[LAUGHTER]

--as a practitioner?

PHYLLIS MARCUS: Well, I can talk about what was built into the 2013 enhancements where there was requirements of additional information to be submitted to the FTC for the agency's oversight of the safe harbor programs. And I recall that there were a number of times when Hill inquirers came knocking during the time that I was helping enforce COPPA as they were looking at other privacy regimes and possibly folding in a safe harbor-like approach.

I'm not sure there was ever uptake outside of that, but the safe harbors have really persisted in great ways to help enforce COPPA along with the FTC. I can't speak to the value judgments. I think Claire is the representative here from the safe harbor--

PEDER MAGEE: Sure. And that's a great point, though, about the idea of the safe harbors from COPPA showing up in other regimes. And Jo, did you all look to COPPA's safe harbor approach in the GDPR or the Design Code?

JO PEDDER: Yeah, I think we don't have as much experience in that but we have tried to learn and take into account the experience. I think we certainly see the potential for codes of conduct and certification measures to expand on the code, but it's an area that's still in development. I think we particularly recognize the need for robust oversight and approval mechanisms, which is what we're building into our own processes as part of that to maintain that trust.

PEDER MAGEE: Laura, it looked like--

LAURA MOY: Yes.

PEDER MAGEE: --and then Claire.

LAURA MOY: Yeah, thank you. Yeah. So I think it's an interesting idea-- the safe harbors-- but in practice, there are a couple-- I mean, there are a few, but there are a couple of really big problems that I'll mention. And one is it's really difficult to get transparency about the safe harbors and about how they are working. We know that the safe harbors file reports with the FTC, but it's as a practical matter those are not public and it's very difficult to get a copy of them.

So for members of the public, it's really hard-- including parents-- it's hard to get a handle on what they are doing and how well they are functioning. And it's really difficult even to get

membership lists for a number of the safe harbors. And I understand that this is part of-- one of the main problem-- one of the main reasons that that takes place is because the safe harbor programs are in competition with each other and are concerned, rationally so, that other safe harbor programs may try to poach their members by taking a look at their member list and then pitching their own services.

This is-- I don't even know how to address this problem. This is really difficult to address. But it's a sign of a bigger problem that is when you have these safe harbor programs competing with each other and the customers are-- and the customers are companies that are providing child-directed services, then they may at times-- and I'm not saying that this is universally the case-- but they may at times be competing with each other based on claims that they will be easier to comply with or make the process simpler for members. And that may at times be in tension with what the most stringent regulations would be to ensure very high privacy standards for users of those sites and services.

PEDER MAGEE: Great. And Claire, I know you want to jump in.

CLAIRE QUINN: Yeah, I very much would.

PEDER MAGEE: If you could maybe a minute or so, and then Jim's got a final question.

CLAIRE QUINN: I'll be quick.

PEDER MAGEE: Thank you.

CLAIRE QUINN: So I would say, frankly, that not all safe harbors are equal. Some of us have very robust programs with ongoing compliance monitoring and a lot of hard work going on that we would welcome an opportunity to share more publicly. The companies that come into safe harbor, they're coming and they're putting their heads above the parapet. There's a lot of wild west out there.

But I think one of the issues that we have with safe harbor right now is the shopping around. We should all have a level playing field when it comes to compliance. You can shop around for service levels. You can shop around for added value. But when it comes to compliance, a company should not shop around. What we find is that we've had to stop working with a couple of members.

We've lost a couple where we've refused to-- we've lost a few, actually, where we've refused

to allow standards that we don't think are meeting the requirements of COPPA and our program and they've gone elsewhere. We often get undercut on price. And we're at a point now where it's not huge amount of money in compliance, but we need to cover costs. But we will not go so low as not being able to provide the ongoing rigorous compliance that's needed.

So I think some of the answers-- to try and be quick-- some of the answers are in that we need to be policed, we need to be able to share the work we do more openly. There are elements of our annual safe harbor reports that I think could be shared publicly. Obviously, there is some proprietary information in there. But I do think that there is some work to do and the FTC need the resource to be able to audit us.

For example, we don't do the annual required audit because one audit is not enough. You've got to be constantly on top of it. And one safe harbor report maybe isn't enough. Maybe there's room for new measures where you can shine a light and have a look more closely at the work we're doing, because as I say, we're not all equal and that's not how it should be right now.

PEDER MAGEE: Thank you. And it sounds like ample area for comments to the rule review. So we are really down to the wire. So I'm going to ask for a really quick response from everyone. There is a lot that we could discuss about age gates. The particular question that I want to ask is, are age gates effective in screening out children? If so, only younger children perhaps, and how do we know? Phyllis?

[LAUGHTER]

PHYLLIS MARCUS: Well, there's a lot there. So I would commend you to speak or ask this question to Dona Fraser when she is on a subsequent panel, because I know that CARU came out with an analysis of the Snapchat service and they talked about things more robust than age gates that were helping to assure CARU, which is another safe harbor approved under the COPPA program, that there were protections in place to manage the experiences for their members.

Are age gates effective? Well, you've thrown that open as a question in the rule review as well for how to manage general audience sites or mixed audience sites. And if you don't have an age gate, I don't know what you guys are going to go with instead. So I'll be watching you.

PEDER MAGEE: All right. And we're going to keep this a lightning round. So I want to jump to Dr. Radesky and

frame the question in light of the observations you've been making in your study of preschoolers under five.

JENNY RADESKY: I think that one simple age gate is not going to be as effective as if when the parent purchases the tablet, can they set up the tablet so that it is for a child user? When they're setting up their Wi-Fi, can they set up their Wi-Fi with the structure and the needs of the family?

When the child is accessing the app store, does the app store know that they're a child and how does it make sure that the apps that are presented there are going to respect the child's needs? And then the apps that are presented there, how are they monitoring who their users are? So it's so many different levels of this that are required.

PEDER MAGEE: And does anybody else want to weigh in quickly before we break?

JO PEDDER: I'll just agree with that. [LAUGHS]

LAURA MOY: Yeah. And I'll just agree with that and also just say that I think-- we don't think generally that they're terribly effective-- the one stop age gate is not terribly effective. And just to reiterate that this is the type of question that the agency can-- you ask what kind of research would answer this question-- that's the type of research that this agency can do. And using not just the-- its notice and comment proceedings, but also using its 6(b) authority to look into this more.

PEDER MAGEE: Claire.

CLAIRE QUINN: Age gates kind of have a use. They're not robust enough for some services. It's risk-based. It should be risk-based. The GDPR is very much risk-based. COPPA has a sliding scale of consent. An age gate can be appropriate in a service where there's low risk in terms of the personal information data collected and how that's processed and used. But then there are times when an age gate is not robust enough and that a child can game it.

And we need to have ways then of understanding that we're dealing with a child. Sites and services should be put on notice that they're dealing with children. They should know-- there could be a registry of kids, a single sign-on for kids, where their ID is carried with them. It doesn't carry personal information in it, but it's flagged as a child. There are all sorts of creative solutions that industry can be working on. But an age gate needs to be used in the right time, the right place, depending on the level of risk.

JENNY RADESKY: And I'll just change-- just to reframe my answer is I've never really understood the idea of a simple restrictive age gate as a yes, no, come-- yes, you can do this, no, you can do this-- because I see technology as needing to be designed around the way the family wants to use it. And so a simple age gate isn't going to answer those questions for family members. It's not the same thing as being able to set up your tablet and being what do you want your child to be able to do on this? That's a very different thing than just a how old is your child?

PEDER MAGEE: So unfortunately we are out of time. We're going to be taking a break from now until 11:05. If you want to use the cafeteria, please keep in mind that it closes from 11:00 to 11:30. So you should probably head there quickly. And we will resume promptly at 11:05 with remarks from Commissioner Phillips. Thank you--

JIM TRILLING: Thanks so much to the panelists. Thank you.

[APPLAUSE]

PEDER MAGEE: Hi, everyone. Could everyone please take a seat? We're about to get started so that we can stay on schedule. So if everybody could please take a seat.

Thank you and welcome back to our webcast viewers as well. It is my pleasure to now turn the podium over to Commissioner Noah Phillips for remarks.

[APPLAUSE]

NOAH JOSHUA PHILLIPS: Thank you for that. Good morning, everyone. Welcome back. Of course, what I'm about to say are my own views, not necessarily the views of my fellow commissioners or the Commission as a whole. It's great to see such a level of interest in the future of the COPPA rule. . This kind of stakeholder participation is a hallmark of FTC rulemaking in general and your involvement in that is crucial. It's also a hallmark of the history of the COPPA legislation.

In 1998, Senator Richard Bryan recognized the remarkable consensus that the House and Senate had achieved on COPPA, and the fact that that was due to the input of a broad set of stakeholders, noting that the revisions to the original bill were worked out carefully with the participation of the marketing and online industries, the Federal Trade Commission, privacy groups, and First Amendment organizations. Senator Bryan explained the goals of the legislation to enhance parental involvement in children's online activities to protect their privacy

and safety, to maintain the security of personally identifiable information collected from children online, and to protect children's privacy by limiting the collection of personal information from children without parental consent.

Senator Bryan also recognized that the interest in protecting children online was not without bounds, pointing out that legislation accomplished its goals in a manner that preserves the interactivity of children's experience on the internet and preserves children's access to information in this rich and valuable medium. Senator Bryan's remarks highlight an important concept. The American privacy framework is built on identifying risks and then designing a solution that balances competing interests.

That requires evaluating the sensitivity of information involved and the potential harms that would result from its collection, use, or disclosure, and then creating a solution that will limit these harms while still allowing appropriate use of even sensitive information. With COPPA, rather than trying to protect children by limiting their experience on the internet, Congress instead created a comprehensive, yet flexible, framework to protect both children's privacy and their ability to access interactive content across the internet.

Our American privacy framework recognizes the trade-offs at issue in the privacy debate, balancing privacy interests with innovation and competition, and protecting most the data considered to pose the greatest risk if shared or otherwise misused. This approach, like any other, is not infallible, and reevaluation and recalibration may at times be warranted in light of changed circumstances. Nevertheless, our risk-based framework has permitted innovation, competition, and economic growth for decades.

In 1998, when Congress enacted COPPA, technology looked quite different. At that time, a major concern was that children were providing their personal information through website registration forms and surveys or posting contact information on electronic bulletin boards. Unlike the phone ringing or the mail carrier arriving, parents could not observe these communications. The first three cases the FTC brought under the COPPA rule are illustrative.

The girlslife.com website targeted girls aged 9 to 14 and offered features such as online articles, and advice columns, contests, and pen pal opportunities. Partnering with bigmailbox.com and looksmart, the girlslife website also offered children free email accounts and online message boards. In these three cases, the FTC alleged that the defendants each collected children's names, and home addresses, email addresses, and phone numbers.

None of these websites posted privacy policies that complied with COPPA or obtained the required consent from parents before collecting this information.

In 1998, social networks, smartphones, geolocation, and static IP addresses were barely on the horizon. However, by 2010, the FTC recognized the changes in the online environment, including children's use of mobile technology to access the internet, warranted another look at whether the rule was sufficient. In December 2012, after a thorough notice and comment process, the FTC announced amendments to the COPPA rule which address changes to the technological landscape.

Among other things, the amended rule updated the definition of personal information to include geolocation information, as well as photos, videos, and audio files that contained a child's image or voice. The amended rule was expanded to cover persistent identifiers that can recognize users over time and across different websites and online services, such as IP addresses and mobile device IDs. The amendments also made clear that the COPPA rule covered child-directed sites or services that integrate outside services, such as plug-ins or ad networks, that collect personal information from visitors. In addition, the amendments also clarified that if plug-ins or ad networks have actual knowledge that they are collecting personal information from a child-directed website or online service, they must also comply with the rule.

As we consider whether COPPA needs further amendment, I would make three recommendations. First, in contemplating changes, we must keep in mind the original congressional intent behind COPPA. It would be easy to stray from that mandate, especially in these times, and to substitute our own preferences in the place of legislatures. Technology has evolved in ways unimaginable in 1998. But we need to ensure that any amendments to the rule are grounded in congressional intent.

Second, any rulemaking must be grounded in facts and supported by data and empirical evidence, rather than just predicated on unsupported fear or speculation. Just because we are talking about privacy, or even just because we are talking about kids, more regulation is not necessarily better, including for kids. Finally, we should focus on the impact that conduct being or to be regulated actually has, and in particular, whether it causes harm.

There are those who will tell you that what we need to avoid-- that we need to avoid using personal data at all costs, especially when it comes to children. And our children are indeed

precious and technology can indeed present risks, which makes it easy to scare all of us who care about children. But not all risks are the same and not all harms are the same. The ability of a strange person to contact and communicate with a child is not the same as an advertisement appearing when a child is watching a show. We need to be able to recognize that.

What is more, focusing entirely on the possibility of harm and discounting completely the potential promise of technologies seems the wrong course to me. Our approach should be one of taking care for children and for data both. For example, e-learning platforms can support teachers, students, and parents, creating customized lesson plans or dynamically focusing on areas an individual student finds challenging. To do so, they need to use personal data.

As much as a child's interest in online content or TV may sometimes frustrate me as a parent, and it does every weekend, every day, there is still great value in entertainment and even in the advertising that pays for it. That's a value to parents and kids. COPPA is about empowering parents and protecting kids. We should keep that in mind.

In doing, we should balance the risks and help children, parents, educators, and others understand them. We should recognize where data support new technologies that can be important public goods. And we should allow rulemaking to reflect the thoughtful process in which all of us are engaged today. Thank you all for your time and I appreciate your participation in this process.

[APPLAUSE]

PEDER MAGEE: Hello. In case anyone missed the first panel, my name's Peder Magee from the FTC's Division of Privacy and Identity Protection. With me is Maneesha Mithal, Associate Director of the Division. We're moderating the second panel this morning, which concerns the scope of the COPPA rule. Thanks to Commissioner Phillips for his remarks. And I will now introduce our panelists. Their bios are included in the materials, so it will be brief.

First, we have Parry Aftab, Executive Director The Cybersafe Group. Next, Malik Ducard, a Vice President of Content Partnership at YouTube. James Dunstan, who serves as General Counsel to TechFreedom. Dona Fraser, Vice President of the Children's Advertising Review Unit. Josh Golin, Executive Director of the Campaign for a Commercial-Free Childhood. And

Don McGowan, the Chief Legal Officer in Business Affairs of the Pokémon Company International.

Again, we're hoping for a interactive dialogue among the panelists. So with that, I'll turn it over to my co-moderator.

MANEESHA MITHAL: Hi. Thanks everybody for participating. So Peder and I are going to split up the panels. So for my part I'm going to spend about half hour or so talking about an issue we touched on in the last panel, and that is the scope of the COPPA rule. I want to talk about both the directed to children side and the actual knowledge side.

So as people know, you can be subject to COPPA in two ways. The first is if you're directed to kids, and the second is if you have actual knowledge that there is a kid on your site or service. So let's just start with the directed to kids test and do a little level setting as to who is covered under the COPPA rule under the directed to kids test and who should be covered under the COPPA rule under the directed to kids test.

So if you look at our rule, we list a number of factors for determining whether a site or service is directed to kids, including the subject matter of the site, the visual content, use of animated characters, or child or oriented activities or incentives, music or other audio, age of models, celebrities, language, advertising, and any empirical evidence. So those are just some of the factors in the COPPA rule.

And so I want to start by throwing open the question, are these the right factors? And regardless of whether they're the right factors or not, should some of them be weighted more heavily than others? So who wants to take that first?

PARRY AFTAB: Good morning. I think that we need to recognize that most of the industry these days, as opposed to 20 years ago, know who their audience is. And they're marketing to their audience. And they're monetizing their audience. They know exactly how old or pretty much how old their users are, and they're telling it to their ad agencies and people they're trying to promote and their investors.

So I think that what we need to do is we can look at the other older factors, but everything is musical and animated these days for all ages. And I think that perhaps we need to start looking at what the industry is telling others about what they know on their platforms. And perhaps maybe even so far as to require that once a year they notify the FTC with a

percentage they believe are under the age of 13. And that might allow things to get in there.

JOSH GOLIN: And I'd just like to piggyback on that because I think that one of the things we hear is that it's so hard for operators to determine if their content is child-directed. But at the same time, we've had this huge scandal around advertisers being upset that their content-- their advertisements were being placed on inappropriate content, on white supremacist content, on things that they didn't want to be associated with. So we've had a whole move towards brand safety and platforms giving advertisers assurances about where their ads are going to be placed.

And as part of those assurances, they can tell-- they tell advertisers whether you're going to be reaching children or not. And so if the platforms are able to tell advertisers this, it seems to me that they're able to tell what's child-directed. And again, echoing a point that Laura Moy was making this morning, this seems like a excellent place for the commission to use its 6(b) authority in order to understand more fully what the platforms are telling advertisers about what they know when there are children or there aren't children on their platforms.

MANEESHA MITHAL: Dona-- Dona and then Malik.

DONA FRASER: So I'm not convinced that all content creators know precisely the age of their audience. I think that they may have a sense of who their target is. But I think that once they get out in the real world, what may have been originally perceived as a mixed audience or for older children, entices younger children. I don't think that a lot of companies are intentionally getting into the kid space knowing the vulnerabilities to that, knowing the liabilities of that. I think a lot of companies are being quite careful. And I'm a proponent of that I think companies want to do the right thing. They don't always know what that is.

MANEESHA MITHAL: So actually, before we get to Malik, I want to just unpack what's been said so far. So I think there's been two threads. One is that companies know who their intend-- or do companies know who their intended audience is? It sounds like yes. And then the other is, what is the actual audience? And where there is a disconnect between the two is that-- is there one that should be weighted more than another or-- Malik, I know you're going to answer the prior question. But I want to throw that out there. What matters more-- the intent or the actual audience, or is it both, or does it continue to be a multi-factor test?

DONA FRASER: I mean, I think optics matter. And I think that the last few cases we've seen both at [INAUDIBLE] and I think at the FTC, it is an optics issue. Because what is perceived by the

audience may not always be what the idea was behind the building and creating of that content. And I think that there are ways to use other empirical evidence that other technologies and other self-regulatory and regulatory bodies are using with regards to media data and all that stuff to determine who your audience is.

MALIK DUCARD: I would add that-- I think my answer covers both questions in a way. The COPPA factors that have been outlined, we really do believe that those are the right factors. But I think that what's really important is that there's balance of the factors, between both content, whether it's subject matter or the content of let's say a video, and content-- so audience and who you're advertising to and what the intent was. And having the right balance is important.

We get concerned when one factor is looked at not in an inclusive way but in an exclusive way. So audience, for example, with audience as the sole factor. We think that that gets to a skewed reality. So you can imagine-- we're in World Series time right now. And if a popular sports game has a large amount of viewership on that, there's going to be a large amount of children who are watching that as well. Does then that make that match, that game, child-directed? And that's an area that we don't think it should go in that direction. But the proper balance is important.

The second point I'd like to make is around clarity. So once you have that balance, we think that clarity to creators and to platforms on where the line is drawn between child-directed, mixed audience, general audience-- that those lines are a little bit unclear. And there's a need for more guidance. So as everyone knows, YouTube recently announced product changes that we'll be making in the next few months.

When we announced those product changes, there was an overwhelming amount of requests for clarity, confusion in the creator, developer landscape around where do I draw the line? Is my content child-directed or not? Or I believe my content is not child-directed, but I don't have enough clarity to really understand how I should be classifying that content. And I know that there's creators in the audience and a lot of creators watching this livestream right now because this is something that meaningfully impacts their lives.

Some of the questions that came into my team include, for example, does describing content as family friendly or kid safe mean it would be classified as made for kids? If we just want to be clear that the video doesn't include swearing, does showing a child in the video mean it's made for kids? If I use an animated sequence for my cooking show, does that mean it's going

to be defined as made for kids? And so on and so forth. So we think that clarity from the FTC in this process which we're excited about is helpful.

MANEESHA MITHAL: So it's interesting and people should please put up their tents if they're interested in responding to a point. But I just-- one thing Malik-- or does that-- maybe it doesn't stand. I'll just take notes.

PARRY AFTAB: They used to in the olden days before we had plastic.

MANEESHA MITHAL: They used to stand. So Malik said something very interesting. He said, on one hand, one factor shouldn't be dispositive, but on the other hand, there's a need for clarity. But aren't those two things at odds? So it would be much clearer if we said X percentage of kids are on your site, therefore you're kid-directed. So I just want to see if anybody wanted to respond to that, but I saw that Josh and Dona had put up, and then James.

DONA FRASER: Who wants to go first?

SPEAKER 2: It wasn't me.

DONA FRASER: So I think that part of the confusion was properly displayed in the TikTok decision. So I think that TikTok proved that it's very difficult to determine who the targeted audience is. And with TikTok we saw that there was evidence of a lot of preteens and teens and who appeal to younger children. So younger children always want to age up. They want to engage with that. But you also had a CEO who was out there talking about engaging the younger child audience. So there were a number of factors. It still made it difficult to, I think, make the case that TikTok was directed to kids.

So again, I think back to what Malik was saying. I think the clarity issue is one thing. And I don't think that there is a hard line. There's no silver bullet on this. But I think we have to figure out what the combination of factors are and I think giving clarity to those specific factors are key. And many of those factors, I think, seem to be more helpful in the post hoc evaluation of something as opposed to when you're building it out.

MANEESHA MITHAL: Josh-- sorry, OK. [INAUDIBLE]

JAMES DUNSTAN: So I wanted to springboard a little bit on what Malik said. And specifically, the directed to that notes celebrities who appeal to children. Well, there are a lot of little kids out there who have

baseball players and football player posters on there. Those are celebrities. Does that mean that all sports sites now are directed to children?

I mean, I think that one-- that one in particular really needs, I think, some discussion because you really run the risk of transforming a lot of truly general audience sites into kid sites if you just apply that as a celebrity who appeals to children as somehow-- and if you combine that with some mystical percentage of kids that you can think may actually be on the site. We run a real danger of, I think, being incredibly over-inclusive on sites that we would conclude are directed to kids.

MANEESHA MITHAL: Parry.

PARRY AFTAB: I think-- and I'll address something James said-- we have never in the 20 years that COPPA has been out there ever looked to the fact that there's a baseball or football player being used on a site and saying that it's therefore directed at children. It is-- to use a quote from the US Supreme Court-- there is this penumbra of indicators as to whether you are child-directed or-- and so what we need to do is do something with it.

So the Cybersafety Group is in the process of building free-- totally free-- an app that will allow people to go in and indicate what do you know about your users, all of the rest-- I'm not collecting information from you, so I'm not going to tell the FTC. But do you have all of the factors that we would normally look at to help them find the clarity. And I welcome Google to help us play with that as we help them understand where that definition is by seeing all of the different factors that come in saying talk to a lawyer but maybe you're child-directed.

MANEESHA MITHAL: Don.

DON MCGOWAN: I mean, the term is child-directed and not child-attractive. And I think that the intent of the statutory language has to be understood to mean something. Going back to what Commissioner Phillips said, we shouldn't substitute our judgment for Congress.

MANEESHA MITHAL: So we've talked about intent and audience composition. There's some factors that don't necessarily appear in the rule that we've seen throughout the years. Things like marketing tie-in of toys, the name of the site. So app store categories is another one. So what-- how should those factor in? Is that part of the calculus or is that something that we should consider

adding?

JOSH GOLIN: Oh, I think all those factors absolutely should be factored in. And I think that one of the things we've seen as a carryover, something that CARU has worked on extensively is the tie-ins with PG-13 movies that were then used to market an inappropriate movie content to a younger audience. And now we're seeing the same thing with-- Angry Birds is a preschool media franchise.

And so to say that that's a general audience app when you have a-- or those are a family of general audience apps when you have a preschool movie franchise seems-- and toy franchise-- seems a little disingenuous. So I think-- and the app store category certainly give us all sorts of signals about what the intent is and what's going to be actually recommended to children. And as Dr. Radesky said this morning, also give us an intervention point where we don't have to deal with 10,000 apps on an individual basis.

So it seems to me that how these things are marketed actually-- if we're looking for factors to weigh a little bit more, how these things are marketed should be something we weigh more. But not just how an individual app or an individual video is marketed, but how franchises are marketed, how associated toys are marketed, because those are all part of the ecosystem in which children are receiving information about what's appropriate and parents are receiving information about what's appropriate for children.

MANEESHA MITHAL: So we have a great question that's just come in from the audience that I want to throw out there. And the question is, if it is unclear if an app or product is child-directed, what would be the harm of erring on the side of being directed to children and therefore covered by COPPA?

MALIK DUCARD: I can jump in on that one and I think it connects to something that Josh was saying as well. So we really believe that when you have an adult who is watching children's content and reasonable measures are taken to really identify that as an adult, that that adult should be able to watch that content in a way that the adult is used to watching other content. And the reason I think that this is important is because there are many, many use cases that this is not a small thing, but many, many use cases where adults legitimately watch content which might be deemed child-directed.

So for example, on YouTube we have a category that is-- falls into family blogs and parent blogs. And any given creator might in that category one day within a video talk about Halloween costumes and what's the family going to be doing in Halloween. And then in the

next video or the same video talk about the top 10 tips for safe Halloween, which may not be interesting to the kid but will be interesting to the parents.

And then clicking into that, the engagement that you lose when you move to child-directed setting like comments and that sort of feedback loop goes away. And in the example that I'm sharing, parents are commenting to the video, to the creator, and there's a real back and forth feedback loop that is really central to digital and how so many of the platform operates today, especially YouTube.

MANEESHA MITHAL: And I think Don and then Josh.

DON MCGOWAN: Yeah, I just want to leverage off something that Malik just mentioned, which is the idea of people over 13 who are watching content that you might think is targeted towards people under 13. If you represent a brand that's been around long enough, there will always be adult fans who have a nostalgic good feeling about the content, and when it's made available to them, they'll watch it also.

And I would say the idea of automatically treating that as child-directed just because it's something that we know is attractive to children-- that's why I say directed versus attractive is a criterion to keep in mind. It's not YouTube's fault that a piece of child-directed content was uploaded on-- or a piece of child-attractive content was uploaded on their site and was watched by a grown-up.

MANEESHA MITHAL: Josh.

JOSH GOLIN: And I would just say if YouTube and Pokémon and other brands have evidence that adults are watching this content by themselves, then that's evidence that the commission should be getting using its 6(b) authority and information we should be getting from companies, because with all due respect, I don't think we just want to take those companies for their word here today. I think we want to actually see what data they have in terms of individual adults without children watching children's content.

MANEESHA MITHAL: Dona.

DONA FRASER: So I want to go back just a couple of comments before about the marketing to kids. And I think at CARU, what we really look at is when something is advertised to a child during specific TV time. So I've seen content and marketing things-- for let's take Fortnite-- and it may be attractive to children. However, it's not being targeted to kids. It's not being sold during TV time. It's not being coupled with other things that will be attractive to kids. So we would never take the position that that was directed to kids. We're not seeing it during TV time and things like that.

And the other factor that I know gets talked about a lot and gets confused a lot is the issue of ratings in the app store fronts. And the fact that these ratings are not about whether or not this is a privacy issue, whether or not data is collected. It's solely about the content of the product and the appropriateness. The ratings are really intended for a guide to parents. So I think that there is a conflation with regards to what that rating means and what it should be intended or interpreted to be. 4+ does not mean that it's necessarily intended for a child audience. It's about appropriateness.

MANEESHA MITHAL: Jim.

JAMES DUNSTAN: Yeah. To answer your specific question, what's the harm of just treating them as directed to children, it's very simple. I mean, we assume that large-- much of the internet and much of the web that we see is going to be free. And the reason that it is free to us as consumers is because we pay a price in terms of being subjected to advertising. And we know that the numbers are-- and how we are monetized on our use of the web.

And the fact of the matter is there is much less value in a website to a marketer that is directed to children because of all the restrictions as Malik was talking to and other restrictions as well. They simply do not want to advertise or are not willing to pay as much because the advertising is not worth as much money to them. And so the danger is you lose the monetization, and ultimately you lose content creators, you lose the incredible diversity we have of content on the internet if people can't make money off of creating it.

MANEESHA MITHAL: And Parry, I want to call on you, but-- so it seems like we're focused a lot on the advertising and the content. So there's a lot of discussion this morning about a lot of COPPA is always focused on verifiable parental consent before collection. There's a lot of other parts of COPPA. There's the data minimization. There's data security. Are the concerns about over-designating

child-directed content-- are those mainly about verifiable parental consent or do they also include these other requirements in COPPA? And Parry, do you want to--

PARRY AFTAB: Yeah, I'll address that as part of my other comment. Attractive to children is very different from targeted to children. And at some point, those things that are attractive to children develop enough of a preteen audience that it flips the business model. And when we start recognizing that there's so many kids, now the company is going to respond to that, monetize it, deal with it, either try to keep the kids out or figure out how to comply.

As we look at this-- and I know that some people on the panel are more concerned about the advertising and the content that's being delivered to kids and whether or not it has to comply with COPPA. I think that the restrictions on what sites can do-- and collection doesn't mean that they're grabbing the information and selling it to others. It means the ability to even post information or share it using email or any messaging technology.

So it sounds like it means I'm collecting it and taking it, but it means that it can be shared even if nobody's watching. So those kind of restrictions on the ability of people to communicate, if they really aren't preteens, is a cost of-- and an inappropriate cost. We just have to be smarter and we're not.

And I'm not here on behalf of the IEEE, but I am the Youth Privacy and Cyber Security Advisor for the IEEE. And no one's bringing the standards groups to bear here. And we really aren't seeing the engineers and technology people talking to the public sector and talking to the policymakers. And if we're going to come up with solutions, we can argue all we want, but until those groups sit down together without media in the room and see if there's a way to address this, we're always going to be asking the same questions.

MANEESHA MITHAL: Don.

DON MCGOWAN: I just want to leverage off something Parry just said. I sit on the board of the National Center for Missing and Exploited Children. And through my work with them, one of the things that we're always worried about is issues around child safety. To go to the question of what do you lose if you just immediately treat everything as though it's child-directed, you lose the ability to keep track of certain things and certain behaviors that if directed towards a child are particularly dangerous to the child on the part of the people who are engaging in the communications technologies.

MALIK DUCARD: And I'd like to add if I can-- the other thing that you lose is the ability for creators to engage with their audiences, and with parents, and people who really get into a two-way street of feedback. YouTube is more than just a video platform. It's truly an engagement platform. And we see all the time when adults are treated as adults and not as kids, when we're able to reasonably identify that they're adults, that there are a lot of really, really valid and critical use cases.

We have creators, family vloggers, who have children with special needs. And they are communicating with an audience of families of parents who have similar joys and challenges and issues in their families. And when you look at the comments and that engagement on parent to parent, you really, really see how important that engagement is. Science education creators where a homeschooling parent may ask that science educator to do an experiment the next time in the video, and that two-way street leads to a next video that is really great, not only for that family, but for the entire community.

So we're worried that when you treat adults as children, then you lose all of that. And that's just something that's so essential to the creative community and the impact that they're having on their audiences.

MANEESHA MITHAL: So I want to unpack something that's been raised about this idea of a distinction between directed to kids and attractive to kids. And I think a good case study is the *TikTok* case that we brought. When you think about intent, let's assume that they didn't intend for lip-syncing to be so popular with kids. And at some point it became clear that that was an activity. And I think it's Parry you said, you can morph and flip a switch.

So I guess let me first of all ask does everybody agree with our enforcement action stating that TikTok was-- or does anybody disagree that TikTok is kid-directed?

PARRY AFTAB: I agree 110%.

MANEESHA MITHAL: So then-- so I guess-- so the follow up question from that is so what obligation do app developers, device manufacturers, others who are creating these products, what obligation do they have to continue to do risk assessments to make sure that they have not morphed or flipped the switches, as Parry said? What obligation should there be?

PARRY AFTAB: I don't know that it's so much an obligation as they shouldn't be running a business as they're

not watching their audiences and their customers and the people they're reaching. So I think that it's included within their business operations to know where their audiences are and their customers. And if they're not watching that, they won't be around much longer.

JOSH GOLIN: I would say they obviously have an obligation and there are so many signals that these companies get that if we want to give them the benefit of the doubt and they're not child-directed but they just end up being child-attractive-- I mean, when the *Wall Street Journal* runs an article about a nine-year-old influencer that just signed a deal with Nike on Instagram, and as Dona said, nine-year-olds are not appealing to 15-year-olds to sell sneakers. It's the seven-year-olds and the eight-year-olds that are interested in what a nine-year-old is wearing on their feet.

That should be a signal to Instagram that the whole world knows that Instagram has a large portion of it which is where children are on the site that there aren't supposed to be. So I think there-- and there are so many signals that people on this end that I don't-- that I'm not aware of that I'm sure you get that your businesses are attracting a large portion of children. So I think there is an obligation to constantly be assessing are we flipping from-- are we so child-attractive that we're starting to attract children? And I don't think that should even be controversial.

DONA FRASER: So I think if we're going to build in assessing your business as it goes along, I think we need to be mindful of the fact that-- I don't think this is unique to kid-directed or child-attractive sites, I think it's businesses across the board have to constantly assess and reassess who their business and their target audience is. But if we're going to build it in as a factor in determining child-directed, then I think we need to be mindful not just in this situation but in all situations across the board as it applies to COPPA, is the cost of doing business.

So we're talking with a lot of small app developers who don't have the infrastructure and the money to do some of this stuff. And I would ask that that commission in reviewing the rule think about the cost factors involved here and whether or not this is an easy lift or a hard lift for a company, and do we need to tailor some of the factors for the smaller app developers versus the big conglomerates.

MANEESHA MITHAL: Don.

DON MCGOWAN: Dona makes a really good point there. I look at it this way-- the law has to allow you to be

terrible at business. And some of the things-- the obligations to report, and disclose, and maintain, and find out information about your audience is the law requiring you not to be terrible at business. And that isn't really the job of the law. And I mean, I'd like to hope that we're not terrible at business. But certainly, I think that if the law-- it creates a standard that requires us to monitor and be good at business-- that's not necessarily the greatest piece of statutory drafting I can think of.

MANEESHA MITHAL: But let me just kind of push back on that for a second. So if the law requires you to periodically assess your popularity with children or-- so if the public policy is that we want to make sure that sites that are directed to kids are policing their sites to make sure-- to be informed as to whether they're directed to kids or not, why shouldn't that be a legal requirement, I guess, is-- and Parry, do you want-- I don't want to put you--

PARRY AFTAB: I didn't want-- Don, did you want--

DON MCGOWAN: Hop on Parry.

PARRY AFTAB: --to reply? I think that when we talked about advertising before, Dona and a few of the others are advertising centric, where we tend to be broader in cyber safety as well as marketing. And I think when you look at how you're marketing your app, what you're saying about what you're doing-- what did you tell Apple? What did you tell Google when you registered it? What do you tell people who may want to buy ads? What did you tell anybody who needs to know about it? Where are you advertising?

All of those things-- if you're doing that, that's an indication not so much of the advertising practices but that you know you are directed at preteens. And then when you get to 12 to 14, that's a little tough. But you know that you're doing it and you're promoting it. If you're not promoting it, then you're bad at business. But you might be also out of compliance with COPPA.

MALIK DUCARD: And if I can jump in-- I would also-- I think a lot of the points being brought up are really reasonable points. And I go back to the balance of the factors. The balance of the factors between content and context. And if you solely focus on audience, you get into the sports use case again, where if there's a popular site, a popular match, popular game that's popular for everyone, or music videos that have large audiences, they're going to have a large kids audience as well.

And that needs to be taken into consideration. But so, too, do the other factors of context and content. So I agree that these are reasonable points and audience is important, but I also agree that you've got to have a true balance across the spectrum.

MANEESHA MITHAL: So Josh-- and Jim, I'll get to you-- but Josh raised an interesting example of the nine-year-old influencer on Instagram. And certainly they have actual knowledge as to the nine-year-old. But the question becomes, so then now they see this trend, at what point do they become child-directed? So Jim, you can answer that or you can finish up the prior.

JAMES DUNSTAN: Yeah. Actually, I was going to come on on that. But quickly, as to what you're telling your advertisers, that goes straight to intent, which I think is a really important factor. If you are intending to market the site to children, then you're directing it to children. I think that's a pretty easy answer. But then-- and repeat the question again.

MANEESHA MITHAL: So I was using Josh's example of the nine-year-old influencer on Instagram. And without naming particular companies, let's say you're a social media company that knows that you have large numbers of kids on your site, a large number of influencer kids. How should that play in as a factor in determining whether a site or service is child-directed?

JAMES DUNSTAN: So I'm going to flip this on its head a little bit and put my private practice hat on because I've counseled a lot of app developers, a lot of computer game developers, a lot of television series producers. And I walk them through and if-- I also at the end of that discussion say, oh, and by the way, you're going to have to go on an annual basis and reevaluate what you did before, or in case of Pokémon, did 15 years ago. And if we find ultimately-- if you find ultimately that it's now attracting too many kids, you've suddenly flipped a switch.

I mean, you've just raised the gate in terms of somebody wanting to get into that market. I mean, the garden walls have just shot up to the sky at that point because now that's not even anything I can control in terms it's not my intent to direct the children, but if suddenly I become too attractive to children, it switches the model. Boy, it's really tough to counsel somebody now. So yeah, let's get into this business because it may get your knees cut off two years down the road.

MANEESHA MITHAL: So this might be a good time to introduce the hypo. So this is kind of along the lines of what we've been talking about. Company D operates what it intends to be a general audience sports fan site, but it turns out that 25% of the users are children. Should the site be considered directed to children? I think, Jim, you gave your perspective on that. Does anybody

else have any views of this? Oh, sorry.

PARRY AFTAB: I don't think it's a percentage. I think-- I keep saying the number--

MANEESHA MITHAL: What about 50?

[LAUGHTER]

PARRY AFTAB: Well, 50, yeah. And I think-- and it goes back to what James was saying-- in that if you have kids, you're directed, you're expecting them, you're monetizing them, you're doing all these things because you know you have a substantial portion of youth market. If you don't care and you're ignoring them, they're just part of everything, that's one thing. But if you are making money in a space that is directed or deemed to be sufficiently attractive to kids that it's deemed directed at, there is a cost of doing business.

And when you do business with kids, there's a higher cost of compliance. You have to make sure they're safe. You have to make sure they're secure. You have to make sure they're private. And we have always as a community recognized that kids deserve better protections than these adults can get because we can protect ourselves better than kids can. So if you're now benefiting because you have so many kids who are using it, yeah, there's now a different cost of compliance. It'll cost you more. Otherwise, age gate or create a separate site just for the kids so they'll leave you alone and keep talking to the adults.

MANEESHA MITHAL: Well, so it's interesting that-- I think some of the comments that have been made said that the percentage doesn't matter, but I think nobody disagreed with the TikTok case. And so at some point, TikTok knew because of the large numbers of kids on their site that lip-syncing was an attractive activity for kids. And so how do you distinguish this hypo from the TikTok hypo? Is it a context? Or do you distinguish this hypo from the TikTok hypo? I guess not hypo--

PARRY AFTAB: Well, Musical.ly had actually put an age gate in initially. And then they found out how many-- they had actual knowledge of how many people had been on the site that they now recognized were under the age of 13. So they had proof at some point based upon what they did which was maybe not a great decision on their part.

MANEESHA MITHAL: So doesn't that mean percentages do matter?

DONA FRASER: I think they do matter. And I mean so-- I mean, with Musical.ly, TikTok, one of the reasons they put an age gate up is because we opened an investigation and they said we've got to do something. So that that was the first step for them. But they still were not acknowledging the fact that they had a large-- what we considered to be a large portion of kids.

And really our assessment was really based on engagement in the app and seeing how many kids were there. You could just open the app and see young children. So it was clear to us that whether or not it was 25% or 35%-- and quite frankly I know that a lot of companies use 35% as a threshold. And I agree that I don't know what the number should be, shouldn't be.

Again, I don't know if there's a silver bullet here. But I do think that we need to use it as a factor. But the other issue is that all the other factors-- I think some of them may be slightly outdated or the way that we assess what children appeal to is different, I think, now 20 years later.

PARRY AFTAB: Dona, did you also investigate or consider Snap and Instagram and some of the others?

DONA FRASER: We did investigate Snap. I could talk about that all day.

PARRY AFTAB: Oh, OK.

[LAUGHTER]

All right. Great. But whether it's Musical.ly, TikTok, or the rest, I think somebody really needs to question the legal fiction of we don't know we have a substantial audience of preteens.

MANEESHA MITHAL: So I'm sorry, Don, did you--

DON MCGOWAN: Oh, I was just going to say, look-- I find sports examples very interesting in this context, because I think I might be the only person up here who's ever bought a Super Bowl ad. Maybe Malik has. I'm not sure. But at a certain point--

MALIK DUCARD: Not personally.

[LAUGHTER]

DON MCGOWAN: --you don't think to yourself I'm buying a Super Bowl ad, it's during a football game, the content of football we've deemed to be appropriate for children notwithstanding that it's pretty

violent. But nobody thinks that they're buying an ad focusing on children when they buy a Super Bowl ad. And you spend about $5 and 1/2 million to buy the space. So you want to make sure you know what your audience is when you spend that kind of money.

I don't necessarily know that the idea that-- I mean, sports are attractive to children. We all know that. But that doesn't necessarily mean that if you create a sports-related activity, you've created something that is child-targeted or child-directed.

MANEESHA MITHAL: Well, so I wonder if context matters here. So we think about the Super Bowl and we think about sports, and as-- one of the impetuses for the rulemaking was this idea that we have these new technologies like voice-activated devices and interactive TV. So is watching a TV-- I think somebody raised this point this morning-- is watching the Super Bowl on TV as a family different from having a sports app that a kid could watch alone or a device-- voice-activated device that sits in a kid's room that talks about sports scores or things like that? So wondering if context matters. Josh.

JOSH GOLIN: I mean, yes, it certainly matters. And it doesn't just matter as context, it matters technologically. I mean, if we're watching the Super Bowl and everybody is seeing Don's Pokémon ad at the same time, that's different than if a child is watching sports on something and they're getting served a behavioral-- personalized ad based on their experience that they've had on the internet and where they are and what the site knows about them. So that context in moving from trying to reach everyone and hitting some children versus trying to hit a very specific user with very specific characteristics absolutely changes the entire calculus, I think.

MANEESHA MITHAL: Well, so we've spent a lot of time on directed kids and before I turn it over to Peder, let me just spend a few minutes on actual knowledge. So one of the things that the rule says is-- well, it seems is the rule says you have actual knowledge basically if somebody tells you. Somebody tells you my kid is on the site. You get a complaint saying a kid is on your site. It seems like it's directed to a specific kid.

Is there something that we should consider about requiring an obligation to do more due diligence? We talked about the CCPA willful disregard standard this morning. Is that something that we should consider in revising the rule?

JOSH GOLIN: I-- not to go twice in a row-- but I mean, first of all, I think there's a couple of things to unpack here. First of all, there's what the rule says and what the new rule might say. But I also think

that it's important to look at enforcement priorities and the effects that those have on changing how people interpret actual knowledge. Let me give a very concrete example.

For years, YouTube claimed in its terms of service, as we all know, that it was for 13 and up, even though it was an open secret that there were tons of children on YouTube and that this was a place that advertisers went to reach children. On September 4, you guys announced your settlement with YouTube.

Now, there's another-- there's a site called-- a game called Fortnite that people may have heard of in this room, which try and find a nine-year-old who doesn't play Fortnite, try and find a 10-year-old who doesn't play Fortnite. It's really, really hard. For two years, Fortnite said in their terms of service that they were for 13 and up because they didn't want to comply with COPPA and they didn't want to deal with all that stuff.

On September 10, six days after you announced the enforcement action, the settlement with YouTube, Fortnite changed its terms of service and now acknowledges that there are children on its site. Now it has a children's privacy policy. So enforcement actions go a tremendous way towards changing what companies actually know about children when they have a motivation to know what's going on.

MALIK DUCARD: So if I can jump in-- there's a few things there that Josh brings up. One, I'll say that five years ago we built the YouTube Kids app specifically to be the place for kids under 13 to go. And we did recently, or earlier last month, announced the product changes that we did to really treat kids viewing child-directed content-- to kids who might be unsupervised watching child-directed content on YouTube in a different way and an appropriate and right way.

But I'll also add to your question on knowledge-- we think that there's a big difference between actual knowledge and constructive knowledge. And we think that the actual knowledge standpoint and approach really is the right approach. There have been some who've said, well, Google and YouTube has really good machine learning. Can't you use that to identify accounts?

And that's something that is flawed for a few reasons. One, machine learning classifiers-- it's not a perfect science. Two, it's also not used by everyone. I think that the bar would be set in a way that not all companies would be able to use that. And those are some of the reasons why we'd be concerned around going, clicking in deeper with actual knowledge or creating constructive knowledge.

Last thing I'll say is that we generate actual knowledge all the time through the ordinary course of our business. And one thing that-- I'm not sure if this is a known-- we haven't talked about it much. But every single week on YouTube alone, we terminate thousands of accounts on the platform that we get actual knowledge on where there might be a child who's under 13 and we think that that's the right approach.

MANEESHA MITHAL: Peder.

PEDER MAGEE: Thanks. I want to continue a little bit on what Malik was talking about on the actual knowledge. And we did hear in the first panel-- I think Laura Moy raised a concern about in talking about platforms that have user-generated content. They would be on the hook if they have actual knowledge that they're collecting information from the users of that child-directed content. And if there's a concern that the platform is going to bury its head in the sand to avoid getting actual notice, should we just be talking about a constructive notice standard?

MALIK DUCARD: I think that there are reasonable points being brought up and there are reasonable signals to be looking at on how to inform actual knowledge. But the sense and the feeling that I have-- that we have is that that constructive knowledge in the way that you described is a bridge too far that really could cross the line even on privacy, and that there are concerns around what might you have to do to create that constructive knowledge. That the actual knowledge that we do generate through the ordinary course of our business is significant and meaningful.

And as I mentioned earlier, every week we're terminating on just YouTube-- it's bigger when you look at the broader company-- but terminating thousands of accounts every week on the platform based on that actual knowledge. But this is one of the reasons why this forum is so useful and we're so encouraged by it, because I do think that there are reasonable ideas, thoughts, and signals, and points that we should consider as an industry.

PEDER MAGEE: I think, Josh, did you want to weigh in?

JOSH GOLIN: Sure. I mean, I absolutely think that a constructive knowledge standard is a better one for protecting children. And for exactly the reasons you say about the don't ask, don't tell mentality that has clearly developed at so many of the bigger platforms. And who knows what's going on with the smaller platforms. That's why my organization and many in the consumer advocacy community support the Markey Hawley bill, which would legislatively change the standard to a

constructive knowledge standard.

PEDER MAGEE: Parry.

PARRY AFTAB: I think that when we look at constructive knowledge, we also need to look at willful disregard. And so actual knowledge is a kid by kid basis. And constructive knowledge is you've got a section that's relating to students, you've got a section that talks about certain things. You get a sense because they tell you that they're in fourth grade. You have a whole bunch of people from a certain location.

But I think that the more information you have, the more it falls into willful disregard. And even though we don't use those words in COPPA, it is used in California. And it really applies on are you directed at kids? And it really comes back to that. So I think we need to look at that. How much do you know? When is it more than just constructive knowledge? When does it turn into you really should be careful about this, because if not, you might be guilty of willful disregard?

PEDER MAGEE: Dona.

DONA FRASER: So I would suggest that it may make sense to take a look at risk and harm coupled with the knowledge standard. So maybe constructive knowledge makes more sense where there is an increased risk to the child versus actual knowledge and there's less of a risk to the child. I just don't think that one or the other, especially moving from actual to constructive, for everybody in every scenario makes sense.

PEDER MAGEE: So assuming that a platform-- a general audience platform-- has actual knowledge that some of the content there is going to be child-directed. But again, it's a general audience platform. And we've heard a couple of things today about the nostalgia value of looking at things that might fall into the child-directed classification. Are there any-- is there any context in which a platform could assume that the user of the child-directed content is actually an adult?

MALIK DUCARD: I think there are a lot of scenarios where the user viewer of a child-directed content is an adult, which is one of the key reasons why we think it's so important to be able to treat adults as adults when they're watching children's content and reasonable measures are being taken to identify that as an adult. I'll share a personal example that comes to mind.

A couple of years ago, I very randomly had the opportunity to interview the Reverend Jesse Jackson about his life and different things. And one thing that I did in that interview was I

actually went on to YouTube and found a 40-year-old clip of him on *Sesame Street* doing the "I Am Somebody" speech to a beautiful group of diverse kids and young Jesse Jackson. And it was an incredible clip I showed him. He was speechless. For a man who has so many words, he was speechless when he saw it because it was the first time he'd seen it since he did it.

And I think about, well, what if I was not able to comment to the other people who are interested in this clip and communicating about the history and the context of it. Or even flash forward to now Bruno Mars, let's say on *Sesame Street.* I like Bruno Mars. I'm an adult. And I'd like to be treated as one so I can comment with others. So I think that the notion of treating an adult as an adult when we take the measures to identify that person as an adult is really important.

And there are a lot of use cases that I would say-- I would actually describe the YouTube experience as broken when you don't have that. It's not a nice to have layer. It's something that is central. I think of color TV-- if all of a sudden it became black and white, you would consider that television broken. And that's what YouTube is without that engagement for, and with adults, with parents, and the like.

PARRY AFTAB: Malik, how many of your users are registered users who have been age gated versus just people who are viewing YouTube without a registration account?

MALIK DUCARD: Good question. I don't have the answer to that. But I think where you may be going on that is that there have been questions that we'll probably talk about on the panel-- should a platform like a YouTube age gate everyone? And is there some form of screen that we put up for all users? And the challenge there-- and I think it's a very reasonable discussion and question to have-- but I think that the challenge there is that YouTube also needs to be used signed out, logged out.

There are so many use cases of YouTube where you might be someone who wants to view content for whatever private personal reasons as an anonymous user without having your login credentials and information logged in. So it's a good point, but that's why we think that the logged out scenario is so crucial.

PEDER MAGEE: James.

JAMES DUNSTAN: Yeah, so I think this really tees up a critical issue here and that is the more regulatory burdens we put on protecting kids, the more burdens we're putting on adults. And at some point, we

are going to run into the First Amendment and we've got to recognize that. And certainly in the context of discussing GDPR and other [INAUDIBLE], we do have a First Amendment here.

And COPPA, as it was created in 1998, and as Commissioner Phillips noted, was a fine line of First Amendment dancing that got it right. But if we keep pushing this and we keep putting more and more burdens on platforms to age gate everybody, now the rights of adults who have nothing to do with children are now impinged. And at some point, we're going to buck up against the First Amendment and there's going to be a real challenge here that we're going to have to face.

PEDER MAGEE: I understand. But I think in the platform context-- and Malik I liked your example of the *Sesame Street* episode-- but I mean, I think it's fundamental to COPPA that we look at the nature of the content. And if it is child-directed, we have a default-- we assume it's a child visiting there. So I guess my question was are there any layers you can build in that would allow you to overcome that presumption? But even with your example, I don't know how you wouldn't-- you shouldn't have treated you arriving on the *Sesame Street* video as a child.

MALIK DUCARD: Well, I think in that scenario the problem with treating me like a child is that I wouldn't be able to engage as an adult. And maybe another scenario is that the science creator on YouTube-- the science educational creator who is making great how-to and physics content for an audience. Imagine the classroom that goes beyond the borders of their wall. And there are a lot of scenarios where a homeschooling parent asks that specific creator to do something next. And the engagement with that adult, with that parent, actually has a positive impact on what the next video that created is going to be.

And oftentimes, you'll find in the comments section on family blogs that there's a community. It's not just creator to the viewer. It's viewers. It's human beings who are connecting with each other on the topic of the video or the channel. If it's a creator-- a family creator who shares that they've gone to marriage counseling, for example. And then you look into the-- and these are real examples-- you look at the comments, there's a back and forth on parents on this content that in some scenarios may be deemed child-directed. But with adults who are treated as adults, specifically, you see it really be a valuable component to the experience-- more than valuable, just central.

PEDER MAGEE: Did anyone else want to weigh on this? Otherwise we'll-- OK.

DONA FRASER: Are we suggesting that if parents are trying to engage with their kids in an online environment

similar to what Malik is talking about, that we're now assuming that they're all children? I mean, so we've had this conversation as a safe harbor with you all that if something is downloaded and the target is preschool kids-- they can't read-- the presumption is that it's the parent who is engaging, who's downloading, who's creating an account if possible-- whatever it is.

So I think that to make the presumption that if you visit something that is child-directed, the presumption is that everyone's treated as a child I just think it's inappropriate. I think that we need to have some sort of other test involved, because you have a lot of parents who I think are looking at the content before they want to allow their children to view it. So we need to allow for that. We need to allow for parents engagements before their children do anything.

PEDER MAGEE: But say you do that and you collect data from the-- in this case, the parent that arrives there first-- are you suggesting then that when they hand it over to their kid, all bets are off and they can collect from the subsequent users?

DONA FRASER: I guess the question then becomes what data is being collected? And I think that that's a case by case situation. What data is being collected? Is it just an IP address? Is it device ID? What data is actually being collected?

PEDER MAGEE: I would think that the personal information as defined under the COPPA rule would be my assumption.

DONA FRASER: So we're assuming that PII is being collected. But if it's a child, then haven't we already engaged some other process beforehand to do that?

JOSH GOLIN: I mean, we heard from Dr. Radesky this morning that these-- with the preschool apps, they're frequently not being prevetted by adults. But I would also say the COPPA says that this is what happens with child-directed content. And so if there are-- if the industry wants to make carve-outs for adults viewing child-directed content, I really think the burden is on industry to demonstrate how often this happens.

So we can-- because we can't talk about trade-offs and potentially trading off children's privacy based on a few-- I mean, and genuinely touching anecdotes. I don't want to downplay them. But we can't make policy on that. We can't make rules based on that. So having an understanding of what industry knows about how often adults are viewing this child-directed content and what technological solutions they would propose for carve-outs for those adults.

But child-directed content is the heart of COPPA. I mean, that's-- we've talked-- we spent a lot of time talking about the general audience and the mixed audience, but the child-directed-- that's what COPPA is about. And so it seems to me very dangerous to start talking about carve-outs for adults viewing child-directed content without having a much more knowledge about what those look like, and how often they look like, and how we can be sure that on repeat visits it is that same adult and now that the device hasn't been handed to a child.

MALIK DUCARD: If I can jump in-- yeah, I think there's some good points there. There are a lot of I know creators who are watching this stream right now-- some in the audience here-- who are happy that this process is underway, because I think one of the big values of this process, Josh, to your point, is there's a need to get more intel information and feedback. And I encourage the FTC to really, really open up the tent to be inclusive of creator voices who have some of the anecdotes I've shared, but even more, and can really share how central, how critical this is.

I'll share one more anecdote, a personal one that I did. I tried to be a creator off and on. But about a year ago-- I'm on a board of a nonprofit, LA Makerspace Two Bit Circus Foundation, and we do STEAM education in libraries and schools. I created a video to try and help to teach kids how machine learning works and to try and teach caregivers and librarians how to teach that. And created a fun video that has candidly two audiences. One is, hey, future people of the world, here's something that you should care about. And here's a very simple way to think about it and learn it.

But the ultimate audience was actually teachers in the classroom, caregivers, parents, librarians to take this project and then actually unpack it in a more robust way for kids. All in one video-- the adults who watched that should be able to ask me questions about, well, when we're doing this project and we have a question, what's the answer. And the kids who watch it should be treated as a kid. And the anecdotes go further than just a few examples. It's really a robust, very central experience and platforms like YouTube.

PEDER MAGEE: Sure. Parry.

PARRY AFTAB: We've done a terrible job with kids. We treat-- in COPPA, it took them two weeks from the time COPPA became effective to understand that they had to be 13 or older. And I polled 10,000 kids a month in person when I talked to them, and the average age that they claim to be is 24 because it's not so old-- they used to say 96. And I'd tell all my clients to screen for any 96-year-olds. And if they could still type, it's OK to leave them on.

But we need to recognize that the kids are very good at this. And so it's punitive as far as they're concerned. If they say they're under the age of 13, they can't do things. We in the nonprofit-- I'll put my nonprofit hat on for a moment-- we in the nonprofit community are doing a bad job. There used to be something called the ad bug a million years ago. It was a little bug. And it came from the label company-- whatever the big label manufacturer was-- and it would help kids identify ads. And the kids would click on them to show how much they knew.

Well, maybe if we can give them something beneficial if they self-identify as under 13, that may solve a lot of this with something-- that maybe they can't do the full fledged communications, but they can do something else that's interesting and fun in connection with how they're engaging without you collecting it. So they are self-identifying as under 13. And it's in some ways more effective than age gating, because they know to lie there. And if you can come up with something fun for them to do that's age-directed that might be very interesting, it might be a way around this.

PEDER MAGEE: Well, maybe that's a good segue into the mixed audience exception. I did want to talk a little bit about that, because that concept does have kids self-identifying. But the mixed audience sites are sites that are child-directed, but they don't target children as their primary audience. And this was added to the rule in 2013. And the idea was to-- if you fall into this category, you can age screen, and you can treat kids who identify as under 13 in a COPPA compliant way and the rest of the audience as 13 and over.

When we announced this proposal, some commenters were concerned that this was just going to be a big loophole that undermined kids privacy. Kids were going to lie. And then other commenters worried that it would significantly expand the range of sites that would be covered by COPPA sites that otherwise would have been considered general audience are now considered mixed audience and they have this additional obligation.

So I just want to open it up. Have these concerns borne out? What are you seeing with respect to mixed audience? Is it working?

DONA FRASER: So I've worked with a lot of companies who have utilized the mixed audience environment. I'm a fan of it. I think it works, but it's also a costly thing to do. You're essentially creating two products in one. But I think the reason that a lot of companies like it, that do use it, is because children are not lying.

So under the previous COPPA regime, when kids saw an age gate, they knew that that was intended to block them out and they would lie about their age. In a mixed audience environment, the child is still allowed in. They don't know that they're missing anything. So they get what I call a vanilla environment on one side if you're under 13. Over 13, you're going to get all the bells and the whistles.

So I'm not a fan of age gates, but I think in the mixed audience realm it does work because it's not about blocking the child, it's about allowing the child in. I think age gates that block users out-- and we did a case with Snap with regards to non-COPPA compliant age gates. And we've taken the position that these types of age gates-- we're hitting a low bar. If the low bar is just making sure you have a COPPA compliant age gate, that's not enough.

I think that we need to talk about what's happening behind the scenes. Because if you have a child at home who has all of a sudden learned how to crawl over the gate that you have leading into the kitchen, you don't just keep building a higher gate. What you do is you know the child's getting in, so now you've got to take all the knives off the counter, you've got to lock all the cabinets, you've got to plug up all the outlets. You increase the security. You don't just keep building higher and higher age gates. It doesn't work that way.

And I think we need to take a look at what age gates work and what scenarios they work. If we're going to continue to block children out, it's not a matter of if they breach an age gate, it's when they breach an age gate. A mixed audience environment allows children in without having to lie.

PEDER MAGEE: Any other thoughts on mixed audience? Maybe I'd love to hear from Don perhaps on how Pokémon has dealt with that.

DON MCGOWAN: Sure. I mean, we've-- having, as I've mentioned the nostalgia-based audience as well as the kid-based audience, we've got a lot of experience with age gates, and age gating, and parental verifications around them and all of that thing. We use a technology that's been provided by a company called Veratad that it basically takes your-- you take the last four digits of your Social Security Number, add them together, and put that sum in an API window that's called-- and that sum authenticates you, which is a great piece of technology that we love. We pay about $0.35 per API call. But we think that's a great way to authenticate people in.

We found that the mixed use environment-- the delivery of the experience to kids who haven't been able to get parental authentication and parental verification is a great benefit. It was a

good piece of creative rulemaking from the commission. And it's allowed for people to experience things that they might not have otherwise had a chance to experience. That they might have felt, well, now I have this barrier-- like Dona describes it-- sitting in front of me and I need to go deal with getting past this barrier in order to be able to access this thing that I want to access rather than allowing for delivery of something that the child wants to see in an environment where they're not being required to authenticate to see it.

DONA FRASER: And I think VPC-- obtaining Verifiable Parental Consent is a hurdle, especially in the mobile app environment. We're not seeing a lot of it because it's difficult to implement. I mean, I would argue that VPC may actually be a misnomer. Are we really verifying the parent and child relationship?

I mean, outside Email Plus where you have to give a child's-- a child has to give their parents' email address-- do we really know outside of that environment whether or not this is the parent of this child? And that's what we're trying to figure out here. And I would suggest that we try and figure a way to roll that back and look at it, because we're authenticating that someone's an adult, they're over 13, but we're not doing anything about determining whether or not that's the parent of this child.

PARRY AFTAB: Or the parent with legal authority over that child.

DONA FRASER: Right.

PEDER MAGEE: Well, just sticking with this topic for a minute longer, we have heard from different stakeholders that there's some confusion about when somebody is mixed audience as opposed to general audience-- maybe what the threshold is. Can you talk to what guidance you give and how you make that determination.

DONA FRASER: I mean, part of it is taking a look at all the factors. And also looking-- talking to companies about, well, let's look at your marketing tools. Let's look at how you intend to market this. Who is your target audience? Who is your intended audience? A lot of companies have products where they're like this is our main audience, but we anticipate that we may get a large number of children. If you anticipate that, my advice to you is that you create a mixed audience environment so that you can create a safer environment and then you don't have to go through the process of doing VPC, but you're allowing all of your users in to engage in your product.

MALIK DUCARD: The only thing I would add to this topic is that the-- on the topic of mixed audience-- we believe that the spirit of that exception is right, but we would also encourage the FTC to consider expanding it as well to child-directed in that-- treating adults as adults when they are watching kids content, and there's reasonable measures that are being taken to really identify that as an adult, would be a good expansion and a good way forward.

PEDER MAGEE: Well, we've got just a little bit of time left. And since this is a rule review process and we're looking at where COPPA is now and maybe where it should go, I'd like to give each of the panelists a shot at a final word. And if you could, very quickly-- if this is possible-- describe what you think is the most powerful impact of COPPA over the past almost two decades, and what, if anything, you would change about COPPA. So we'll go right down the line. Parry, you can start. And briefly, please.

PARRY AFTAB: Well, 20 years ago, nobody was thinking about kids privacy-- only the insiders. And COPPA took a very brave stand. After the FTC said get your act together, we don't want to do this, and everybody ignored them for so long. So the best thing that it did was raise the appeal of addressing kids privacy and recognizing that these are serious issues.

The one area I'd love to see improve is doing a better job. I think that the FTC has done extraordinary things with some of the new enforcement issues. But I think maybe some of the watchdog groups-- I think you're part of that and I guess we're a part of it-- we always were at Wired Safety-- some of them look at it and try to help you understand when things are going wrong, so we can be the eyes and ears online because we all have the same thing at stake. We care about kids. And so I think that that would help.

PEDER MAGEE: Great. Lightning round. Malik.

MALIK DUCARD: All right. Lightning round.

[LAUGHTER]

So I think that the past 19 years, I think that COPPA really, really added so much to the mix on meaningful protection for kids, putting parents in really more of a driver's seat where they belong, and the rule has evolved over time. In terms of areas of improvement, I think it needs to continue to evolve to reflect some of the realities of today's world and topics that I've hit on like treating adults as adults when they're on kid's content and really engaging with their audiences.

The other thing I'll say because I think that there's a topic that we didn't click into too much is really thinking through as you move forward in the rulemaking on the immense value of content creators and developers. What this next generation of creators are doing who are empowered by platforms, like YouTube, that have really given small businesses large voices and an ability to really, really change people's lives for positivity is really extraordinary. And I encourage the FTC to click into that more and see what's at stake with some of the decisions it makes around rules, because I think harm can be done to the very constituent, the very group that we all care about on this panel, when that's put at risk.

PEDER MAGEE: James.

JAMES DUNSTAN: So when we look at COPPA, we often forget the second P in COPPA, which is Protection. And I think we need to go back to the legislative history and look at what we were really protecting kids about. And first and foremost, it was predation. It was sexual predators. And if you look at the hearing, what Robert Petoskey, the FTC chairman, said at the time, that's what we were worried about. And I think we've done a great job in COPPA in that regard. COPPA as part of a overall enforcement on child predation.

But my concern is I fear we are moving into taking a protection statute and turning it into an anti-advertising statute. And I think if we do that, as Malik said, you're going to harm an ecosystem, you're going to harm the marginal players, and all you're going to be left with are the big tech companies who can afford the regulatory overburden of this. I think we've got to be really careful about that.

PEDER MAGEE: Thanks. Dona.

DONA FRASER: So I think that what COPPA has allowed-- and I agree with what most have said here so far-- is that it's allowed for through safe harbors and great self-regulatory model to show that there is a way to self-regulate in this area. And to that end, I would ask that what I'd like to see moving forward is increased scrutiny over how safe harbors operate. I think that we can be more transparent. I welcome the transparency. I welcome more scrutiny. We have nothing to hide. And I think it can only help the environment.

The problem is that between the seven safe harbors you have in the United States, we may represent probably less than 10% of the entire market. So there needs to be a really increased effort with regards to educating consumers and businesses about COPPA. I think the FTC

should take the lead on that and I think safe harbor should be obligated to follow that lead.

PEDER MAGEE: Great. Josh.

JOSH GOLIN: So I think in terms of what COPPA's accomplished, first of all, it's really the only law we have to protect children online and that's important. We have fewer regulations around how you can advertise to children online than we do on children's television. So we see things like influencer videos being very commonly aimed at children on the internet when they wouldn't be allowed on children's TV. So it's important to have some restrictions on marketing.

We have the data being used to fuel the most powerful persuasive technologies we've ever had. And to some degree, COPPA has kept children out of that somewhat. But increasingly it's not. And what I would love to see from the commission-- we're starting this process three years early. So if we're doing a special rulemaking three years early, I hope that we would take a little broader stance than maybe some of the 25 questions that you asked in the notice and really ask-- really dig in to what's going on.

What does industry know? How is this data being used? When we're talking about a mixed audience site, what do the sites know about a child when they're arriving? What are all the signals that they're bringing with them about that individual child? There's so much that the industry knows that I don't know. And frankly, I don't think the commission knows. So I would hope since we're opening up the can of worms three years early, let's open the whole can and let's use that 6(b) authority to really understand what the industry is doing, so we can make rules that aren't just based on speculation.

PEDER MAGEE: Great. And final word, Don.

DON MCGOWAN: Lightning round. Dona stole my thunder. I think one of the greatest legislative creative aspects of COPPA is the safe harbors. As somebody who sits in the industry, they are very useful to us. I've been working with Dona for years. I've followed her through her career travels and it's been fantastic having somebody who can advise us on what we need to do to be correct.

I'm not afraid to sit inside the Federal Trade Commission's house and advocate that they should get more budget for enforcement. I think more budget for enforcement for the FTC would be a great idea. More enforcement activities. It's always easier to be a good guy when the bad guys are getting kicked in the shins.

PEDER MAGEE: Great. Thank you. And thanks to all the panelists.

MALIK DUCARD: Thank you.

DONA FRASER: Thank you.

[APPLAUSE]