JIM TRILLING: Welcome back from the lunch break. We have a brief presentation by Morgan Reed the president of ACT, The App Association. And then we'll move right into our next panel.

MORGAN REED: Hopefully, there'll be some claps afterwards, but I think there'll be-- I'm not sure that it'll still be sustained. I see a few folks filtering in. All right. So as Jim said, my name is Morgan Reed. I am the president of The App Association. I am also a recovering developer. And I have spent most of my life in front of keyboards, either working with software companies writing code or otherwise. I go back to an Apple II with a tape drive.

So our organization represents more than 5,000 companies worldwide. But for the audience here today, I'm going to focus down on a subgroup of our membership. We run a developer exchange, a private closed developer group that has more than 800 companies and developers on it, where people are free to ask questions, make comments, talk about monetization, commiserate. And I'll read you some interesting quotes from there.

We did a survey of that audience. And in addition, we did a series of focus groups and one-on-one interviews with independent kid's app developers. These are developers who specialize in educational applications, applications that are directed at children. And these are folks who own it. We've heard a lot about general audience applications, mixed app applications. This is to talk about the folks who know exactly who their audience is and how they're going about them.

And that leads me to something. I want to thank Jim and the rest of the team at the FTC. A lot of times, these events spend a lot of time talking about small developers, but never actually hearing from small developers. So I really appreciate the FTC time and thoughtfulness to include some of these messages along with it.

So most of this you know. And I'll go through it really fast because it's a backup of all we've heard. Price Waterhouse Cooper sees kids 12 to 15 consuming 20 hours a week of screen time. The American Heart Study shows kids 8 to 18 were post-COPPA seven hours a day. We've all heard from everything we know up to this date that YouTube kind of owns the space in the general audience. YouTube Kids grew fast, but 80% of kids are using YouTube the general audience version, making it the largest single kid's digital entertainment platform.

I looked at a PWC marketing material, and they actually estimate that YouTube general audience will actually account for 25% of kids digital ad spend by 2021. I thought that was a fascinating juxtaposition. PWC acknowledges that this is a general audience application, and

yet they believe 25% of kids targeted ads will actually appear there.

So TikTok is not far behind in audience. I will say from the small kids app developer side, the result of the FTC action against Musical.ly/TicTok is unclear. We heard a lot about it earlier today. I think that's yet to be seen.

When I talk about general audience, really you have to think of it in this context. A general audience from a user perspective is free, ad supported. Free will always be in quotes for that reason. Unfettered, meaning that you don't feel restricted by what you can get to, how you do it. It's easy, it's low friction.

Widely available. I can get it on any platform, in any case, in any context and I can get to it rapidly. And then finally, entertaining. We've talked a lot about serious stuff here, but the entertainment value, even when it comes to educational, is important.

What do parents say? I'm going to say something provocative, and that is, is that the study by Danah Boyd, Ezra [? Hargitay, ?] Jason Schultz, and John Palfrey in 2011 still holds true. And if you haven't actually gone back and looked at that study you should.

To nutshell a really long and thoughtful piece, basically, it's that parents are making decisions regardless of the regulatory framework that they're presented with. And that kids are doing things that are expected of children who are testing out the range of privacy and their own information sharing. And so there is a tendency for us to look through the regulatory lens. And what this study did back in 2011 is look through it through a behavioral lens and what people are accessing. It didn't make a commentary about whether it was good or bad, or respectful of privacy, but let's match it up with the behavior.

Now, the other part is, 85% of parents, when you ask them directly, say they are concerned about children's digital privacy. And the good news is, basically, most parents, nearly 100% think that parental controls are a good idea. And what was more astounding is, 65% of 11 to 15-year-olds also think parental controls are a good idea. You'd think this would be awesome, right?

Bad news. Parents don't really use them. We're seeing some, as high as 47%, of parental controls in the platforms. But in general, when you poll parents, one in three actively use the parental controls. And I think this is something that was very interesting in our first presentation. Pew finds 81% of parents have knowingly allowed their child to use general

audience YouTube.

I mention this because earlier today we had a presentation talking about an IRB approved study to look at children's behavior on their own platforms. The fine doctor showed us the list of the applications that they were there. Remember, if it's an IRB approved study, then there's been some parent engagement in all this. And yet, the majority of the applications she was showing in her study were general audience apps.

That means the parents involved actively circumvented the controls. And I'll remind you, she said that 35% of her users had their own tablets. Some point along the path, the parent had to actually say put in a false state. Weren't we told, don't put 94 in, do 24 because it doesn't make you look too old?

Well, this tells you even when informed parents are engaged they are parenting in their own way. So even in an IRB study, they're doing that action. Why? Friction, restriction, and cost.

Every layer of friction you add alters parent behavior significantly. We jokingly refer to it as the over the shoulder factor. If a parent wants access to something and they have to pass it from the back seat to the front seat of the car more than one time, the parent moves on to the next thing. So the more friction you add to an application directed at children the less likely it is that the parent is going to take the steps necessary to get through it because the competition, of course, is as I said, free, unfettered, widely available.

Restriction. Kids balk against some of the restrictions. I can't get to this, I can't do that. And they say that to the parent. And from the parent's perspective, fine, I'll just put in a different age date. They're participating, they're parenting but they're not using the regulatory construction that we all understand.

And then cost. I'm going to read you something. We'll get to a lot of other developer quotes, but this is a quote from a parent that just came in on the developer exchange yesterday. This is to a kid's app developer who collects no information. It's an educational app. It's actually quite a good app.

Quote, "Firstly, I already sent a hate letter. Did you not receive it? Second, why do we need to spend money on some garbage game just so kids can learn.

I got this game because I thought it was free. But no, instead you are making me spend like $10 so my kid learns. No, take your business somewhere else and I will write a no star review

and get my friends to write one too. I will do this until you allow my kids to play everything for free. Thank you."

Now, for my members who are building educational apps for kids, that last bullet, friction, restriction, and cost, that's not an unusual email. It was more hyperbolic than most but it's not unusual. That should present you the difference there are community is seeing when it comes down to this stuff.

These numbers from our survey. 92% of our developers see that general audience user generated content-- sorry, Julia-- UGC is the biggest competitor not fellow kids app developers. It's not just saying us saying this. The Children's Technology Review found that in 2013 they reviewed 673 releases from studios like Toca Boca, Noisy Crow, Touch Press, and Duck, Duck, Moose. That's now dropped to 105. So we are seeing less high quality educational valuable content because the market is just not there.

Now, down to the questions and answers directly from developers. Here's what they're hearing from their users-- from their parents. It's cultural. Parents don't want to pay for software.

We get requests from users, why don't you have ads so it's free? We're seeing that more prominently on Google Play than Apple. There is a bit of a culture difference between the Apple App Store. There's I don't want to say more pressure, but there's a more acculturated concept that you pay directly for goods and services on Apple versus Google Play, which has more of a culture of free, user generated, it's more available content.

And I thought this one was really interesting. This is from a developer who has kids in the COPPA age range. "I'm a parent. I let my kid watch videos on general audience apps. I know about the privacy issues, but it's fast, easy, and they like it."

This is from someone who works in our field and knows this stuff. And I bet you, if I did it where everybody would close their eyes and have a show of hands, how many of you have let your own under 13 child access a general audience application? Yeah, a lot of hands go up.

And this is the problem. So we talked about general audience is free, unfettered, widely available, and entertaining. The COPPA side, expensive, onerous or friction full. We have to find some way around that. Restrictive, fewer features, fewer capabilities, less known or available, and it's entertaining-ish.

I use the "ish" because something that our industry faces in large regard. It was interesting, because Rovio spends a lot of money I know doing the same thing. When you're up against an hour-long user generated content video on some kind of video sharing site, that content is quick, it's easy, it's entertaining for the kid. They watch it. For us, as a small guy, or even Rovio as a giant multi-billion dollar company, we've got to hire artists, programmers, program managers, project managers, lawyers to look over the COPPA language. Every time we roll out a new feature or new capability we've spent thousands of hours or at least hundreds of person hours to put that new content out.

And you're competing with billions of hours of video that's coming out constantly across multiple streams. So our stuff is entertaining but it's a huge cost to get that entertainment there to provide 30 minutes of new content versus two hours of video that you see from UGC. So it's very unbalanced in what we face.

Is COPPA the barrier? I thought this quote really summed it up. "Seamlessness is expected. But with COPPA, seamlessness is impossible." And that has been one of the single largest areas of concern.

Our folks are looking to provide a COPPA compliant environment. And they're finding doing VPC is really hard. We want to make it this way, we just walked away.

And why do they want to do it? We wanted to create a hub for kids to promote creativity. So these are not folks who are looking to take data and provide interest based advertising. They're trying to figure out how to do it so they can build an engaging product.

Parental consent makes the whole process very complicated. And this is the depressing part. But I have no good answer. And why? Because developers need insight to make better products.

The loss of analytics that's been happening throughout the ecosystem is huge. 100% of our respondents, the only thing we had 100% on at all, was yes, we need analytics. Interestingly enough, most don't blame the platforms for the restrictions that have happened on the analytics.

They feel it's just a fact of doing business that the Apples, the Google's. The Flurry's, everybody in the world who's been pulling back from providing analytics is finding themselves there because they're unsure about the regulatory environment. That doesn't mean parents

aren't concerned about privacy, but there is this concern. And you say it here on the response, the platforms are always reacting.

When you say, well, do they really need analytics? Yes, they really, really do. I don't want to collect information on kids, but I can't set up a way for my app to work on the phone, tablet, and parent device seamlessly without creating accounts. You heard that earlier. And I know that some apps use tokenization and do some other ways to pass the information, but it's tough, especially for small developers.

We saw in that initial study that we talked about this morning that parents are providing the app to the kid, and maybe it's on the phone and maybe it's on the tablet. The better your content, the more COPPA-conscious you are, the harder it is to provide the actual solution that everyone in this room wants. We have one whole branch of our membership that deals with applications that are in the special needs capability area. And this has been the hardest hit.

They need a lot of data, and intrusive data, and data that may be stored on the device in a way that allows a child who needs a special vocabulary. For kids with autism or speech difficulties, they need to collect data on that child, preserve it, move it forward with devices and capabilities. The hard part is, you'd say, well parents with kids with special needs, they've got to be the most engaged parents. Unfortunately, they're not.

For a lot of families, especially those where they have a lot of income insecurity, if they have a kid with special needs, they are the least engaged that you can find. And that's something that's highly heartbreaking and disappointing but it's something that our membership who works with those communities understands full well. So we've got to find a way to make sure that special needs has its own opportunities.

And I don't think this happens by accident. We say that VPC is intentional friction. It's clear from everything we've heard in the last two panels that the authors of COPPA, we don't really want information collected on kids. So friction is intentional. And this is leading to the destruction of general audience applications basically wiping out COPPA apps off the face of the map.

And I would say-- and I know I'm short on time, sorry, Jim-- that we should take a page from what we learned during the Napster, LimeWire fight, which is the more you found ways for content to be provided legally, the more it pushed back on the piracy applications, the LimeWires, the Napsters of the world. And the more you saw people gravitating to legitimate,

upfront paid content.

And they did that by reducing friction. Now in the IP space in the music and movies, that space was having to do with licensing. But in ours, a lot of that friction is created by a regulatory sphere that has some uncertainty in it. So I would argue that we should take a page from there, find out a way to have results that engage parents, but reduce the friction. And that gets to my big ideas. And I'm a little over.

We have to find a way to allow the big platforms to be engaged on our capabilities. Finding ways for an Apple, or a Google, or a Steam, or any of the larger platforms to provide an API that allows us to check against for a child that doesn't force us to build our own product. Allowing [? Karu, ?] and [? Pryvo, ?] and the rest to engage and intersect directly with those platforms is also something that will be good. But the platforms are not going to take that burden on if the liability perspective and the opportunity to innovate is tough.

We also need to make re-consent easier. One of the things that harms our ability to create new content and push it out is getting re-consent becomes a barrier for that next stage. Remember I said, friction is our biggest barrier to implementation? Adding that friction for re-consent is a nightmare.

And then, as I said, innovation of platforms is going to be critical. But I think we should look and take a page from the FDA's 2013 mobile medical application guidance, and what's happening in Fintech on the use of regulatory sandboxes. We need to look for ways to allow the bigger platforms to innovate in this space alongside the safe harbors, and give them some space.

Can we use the fingerprint? Can we use face ID? Is there some way that we can directly interface with the larger platforms to get the consent we need so that we can provide the products that everybody in this room over the last two panels said they want? And with that, Jim, I appreciate you giving me some extra time. And I'll go to the end. Thank you.

[APPLAUSE]

JIM TRILLING: Too depressing. For those who were not here this morning, I am Jim Trilling, an attorney in the FTC's Division of Privacy and Identity Protection. And I, along with my DPIP colleague Kristin Cohen, will be moderating today's third panel. We're going to be talking about definitions, exceptions, and misconceptions associated with the COPPA rule.

We want to begin by thanking Morgan for his presentation, which will definitely help inform some of our discussion. We have a terrific group of panelists and a limited time to discuss a number of issues. So I'll refer you to their bios.

Just to introduce them briefly, we have John Ahrens, the CEO of Veratad Technologies, Inc., Ariel Fox Johnson, a senior counsel for policy and privacy at Common Sense Media, Sheila Millar, a partner at Keller and Heckman, LLP, Morgan, from whom you just heard, Steve Smith, the Chief Information Officer of the Cambridge, Massachusetts Public Schools, Amelia Vance, senior counsel and director of education privacy at the Future of Privacy Forum, and Samantha Vargas Poppe, a principal at Equity Matters, LLC.

As with the other panels, we will be working to make this an interactive discussion. And we do have question cards available for those in the audience. And those who are watching online can propose questions by following the instructions posted online.

So as I said, we're here to discuss definitions, exceptions, and misconceptions. I want to start off by focusing on misconceptions. I'd like to ask each of our panelists to say what they think the biggest misconception is about COPPA. Happy to go right down the line. Why don't we start with you, John.

JOHN E. AHRENS: Sure. Well, one of the misconceptions I think has already been identified earlier in one of the panels. The terminology of a verifiable parental consent, the association of the verification on identity, and the fact that whether or not that person is the parent of the child. I think that is one of the interesting questions that we get when we're about to provide a service, and a potential client says, so are you going to verify that the person that we're verifying is the parent?

Basically, we're doing the job of verifying the identity in that. And so I think that may be one of the interesting things you could take away about misconception.

JIM TRILLING: Ariel.

ARIEL FOX JOHNSON: All right. And thank you to Jim, and Kristin, and the FTC. Common Sense, I think, is-- the biggest misconceptions I hear are one, that it covers 13-year-olds. And two, that it's a flat prohibition on collecting personal information from kids.

I think these misconceptions really show the gap between what consumers expect from

COPPA and then what COPPA is actually doing. Consumers do think that we should be protecting teenagers, at least young teenagers. And while COPPA does have some flat prohibitions on use, it's been primarily enforced as a notice and consent statute. And I think consumers at this point are looking for more.

JIM TRILLING: Sheila.

SHEILA A. MILLAR: Thanks, Jim, and thanks to the FTC for inviting me today. I'm going to highlight two misconceptions. One is that COPPA covers content, which of course it doesn't. The second is going to really come out of Morgan's presentation. And that is that COPPA prohibits analytics.

The support for internal operations exception has been extremely helpful in allowing companies to use and collect certain data for restricted purposes under COPPA. We didn't talk about it this morning. But if we map GDPR and COPPA, they actually map really well. They have different approaches, but if you layer on the legal basis for processing versus the COPPA prescriptive approach and the exceptions, they map really well.

Where they don't map well is the ePrivacy Directive. And so when we see last week's Court of Justice of the European Union decision on the need for express informed consent for any use of non-essential cookies, which is directionally where the UK ICO cookie guidance goes, that's going to have an enormous impact, I think, in a very negative way, preventing businesses from collecting information that's legitimately necessary to operate their businesses. And I think the experience of COPPA is that that can be done in a way that is privacy safe that reflects the risk-based approach of COPPA.

JIM TRILLING: Amelia.

AMELIA VANCE: I think there are two big misconceptions that I frequently hear. First, often from children and students themselves, that if you are under 13 the internet is not for you. That all of the statements and all of the websites that say this service is not for people under the age of 13, and the limited number of sites that actually are I think really furthers this idea that the digital ecosystem is something you have to secretly be in or that you just can't participate in until you're of age.

And then the other misconception I hear a lot is something that Ariel and Sheila were getting to, which is that there's this conflation of several worries about child privacy and safety. And COPPA's up there in the clouds, is the umbrella that hypothetically covers all of this, whether

it's concerns about advertising, concerns about whether an app is appropriate, whether it has adequate security, whether it has appropriate privacy controls. And nobody quite knows exactly what it actually is. And so getting down to the nitty-gritty, and maybe not seeing COPPA as a one size fits all but as a piece of the ecosystem is something that I'm hoping we'll see more of moving forward.

MORGAN REED: That VPC is a technological problem not a sociological problem.

JOHN E. AHRENS: I'm going to have a slightly different perspective, and challenge this on a whole different level. And that's that I think there's a misconception that all parents are well-informed enough to make a good decision about consent. And I would say that probably the majority of them are not in a position to make a well-informed decision.

For us in the room, it's sometimes difficult in terms of service privacy policy to really understand what's being collected. It's more than just whether there's advertising or not. And to expect parents to make a really good decision about a product I think is not correct.

SAMANTHA VARGAS POPPE: Thank you, Jim, and Kristin, and the commission for including me in today's conversation. From an equity perspective, the biggest misconception I think that I see is that this law protects all kids equally. I think that it's from a generation of legislation of one size fits all legislation, and really hasn't done a good job of including a focus on the fact that different populations in an increasingly multicultural population of youth have different experiences that influence their decisions. More recent discussions in privacy have touched on this. And I challenge everyone to bring that into these debates while they're thinking of how to strengthen this role and make it work better to protect kids.

JIM TRILLING: I want to follow up first on Samantha's misconception. Can you tell us about some of the demographic and social trends and unique concerns regarding children of color and their privacy?

SAMANTHA VARGAS POPPE: Absolutely. Thank you. And I'm glad that you asked that just because I think that this panel will get very technical. And it's just a good place to start.

Recent data back in June from the Census Bureau came out and showed that for the first time as of 2018 the children of color represent the majority of children in the US population under age 15. So the population's not what it looked like 5, 10, 15 years ago. And that's only to an expected growth in those populations.

I think that that drives a lot of outdated assumptions about how people and children and parents interact in this space. I am a consultant with UnidosUS, a national civil rights and advocacy organization focused on opportunities for Hispanics. I identify as Latina myself, so that's the population that I'll just use as an example to walk you through what I'm talking about here.

One out of every four children under age 15 is part of the Latino community. Various reports tell us that Latinos have an estimated spending power of over $1.5 trillion dollars. We know that the digital divide looks a little bit different today. Latinos are over indexing on mobile platforms. They're accessing the internet at rates higher than the general population via mobile devices.

And so then, with all of those things coming together at a very high level, it's no surprise that Latino population and kids are being targeted to try to turn a profit. Unfortunately, a lot of times that comes in the way of flagrant violations of COPPA that allow people to-- bad actors. I'm not saying that everyone is in this mix at all, but we've seen a strong tie in the research that violating COPPA, getting data, and using it to target certain populations for junk food.

We see research showing that a lot of the ads that Latino kids and African-American children are seeing, somewhat upwards of 95% are for junk food products. And again, I think there's parts, different layers of this conversation. But I believe that some of that lax enforcement of COPPA helps open the door for some bad actors. And that's just something that we have to think about how this all comes together, and how we can learn more about the interests of a more racially diverse population that we're dealing with as the reality of our youth population today.

JIM TRILLING: Does anybody else want to weigh in on the demographic trends that Samantha identified and how policymakers should be reticent of those trends when it comes to rule reviews and also when it comes to the legislative landscape?

MORGAN REED: The only thing I would say is that the special needs community, the disabled community is an area where these devices have had a profound life changing impact on people. And that we need to make sure that, I think somebody else when you said life doesn't begin at 13. These adaptive technologies need to be made possible for kids starting as young as possible so that they can see, so that they can communicate, so that they can engage in the world around them. And I hate it when COPPA becomes a barrier for a child to say I love you to their mom.

And that's what we're trying to avoid.

KRISTIN COHEN: Now we've covered the misconceptions. So we're going to move on to the definitions were going a little bit out of order from the title. And one of the most core components of the COPPA rule involves how we define personal information. The statute specifies several pieces of information that are considered personal, your name, your address, but it also gave the commission the ability to determine if there were other pieces of information that would allow the either physical or online contacting of the child. And in 2013, we added, as Phyllis told us about this morning, the commission added three pieces of personal information that were covered, persistent identifiers used to track users over time and across websites, geolocation information, and photos and audio recordings that included the child's image or voice.

So I'd just like to ask the panel how that has worked in practice? Have those additions helped to improve children's privacy, have they had unintended consequences? We heard a little bit from Morgan. I think I know where he's going to come down. But we'd love to hear from the panel on that.

ARIEL FOX JOHNSON: I think it has improved kids privacy. I've seen the FTC and the New York attorney general going after actors who are collecting personal information like persistent identifiers, and protecting kids from those persistent identifiers being used to create profiles of the kids or behaviorally target them. I think we also see that in newer definitions of personal information, like in the California Consumer Privacy Act and the GDPR, we see unique identifiers and things like persistent identifiers tracking someone across sites and services and over time included as a piece of personal information just the same way as we additionally see new things like biometrics. And I feel COPPA is maybe like ahead of its time in understanding that these persistent identifiers and things that ways you could be identified online should be protected. But that's where we see everywhere else going now too.

SHEILA A. MILLAR: I think one of the big changes from the 2013 rule did involve the definition of video and audio files. When we think about the policy behind COPPA, which is privacy and security by design, we didn't call it that at the time but that idea that you don't collect more information than is necessary to allow the service to be provided is core to COPPA. Prior to 2013, I think a lot of companies offered apps or websites that allowed kids to upload photos. But certainly, if you're in the kid's space, you were very attentive-- somebody mentioned earlier that predation was a really core concern that drove adoption of COPPA. So you would blur any identifiers. You wouldn't allow a child to say, wear a T-shirt that you could visibly see Lafayette school to

identify that child.

That really was a sea change. And I think there's been an adjustment. People are accustomed to it now. But I think to Morgan's point, as we now get more focused on Americans with Disabilities Act, and compliance, and ways to get folks, including children, more engaged in the world.

How do we make it easier for them to use adaptive technologies, to be part of a community, to feel connected without putting up too many barriers? So it comes back to that risk balance. What are we trying to solve for? So the policy of advancing how we protect children with the hurdles necessary, in many cases, hurdles that are put up to protect their privacy, I think we're still struggling to find that balance as technology and society changes.

MORGAN REED: We've been strong proponents of more enforcement by the Federal Trade Commission, including in front of Congress because our members all are part comply with COPPA. So their world view is, hey, I'm doing the right thing, how come nobody else is? Why are we standing alone? And we know that's not true, but that's how it feels. And you saw that from the quotes.

So I think to your, point to Sheila's point, I think one of the key elements there is, how do we reduce the friction for parents? How do we inform them, as Steve said? How do we engage with them in their language they speak at home? How are we able to take advantage of what the platforms are doing for their own business purposes to make it possible to appropriately engage, meet them where they are, help them parent?

Because I think when it comes to these questions of what persistent identifiers we use, well, if those can actually help us better inform the parent reduce the friction, then that probably leads to a better product, and, as you say, better protecting of children's privacy. So there has to be a better path on that.

SHEILA A. MILLAR: Well relatedly, I think the cross device point that you made earlier, Morgan, is kids are playing, they're using apps on their phone and their tablet, so how do you make a privacy-safe experience that allows the business to simply leverage that persistent identifier? I think, again, we're looking for privacy-safe experiences that minimize the data collection from children.

And when we first-- and I was on the panel back in 2011, whenever we had the last workshop-- but if we have a world where before I can set a persistent identifier to do analytics, to do frequency capping, to do you spam or protection or various other things that fall within that

definition, if we automatically say that's per se personal information and you need parental consent, that enormously adds to the friction. It enormously adds to the parents' burden. And I think the question we need to ask ourselves is, is that the right trade-off going forward in terms of protecting privacy?

AMELIA VANCE: I think all of this, though, is much less about the definition of personal information and much more about what is then required for verifiable parental consent. Because when it comes to the definition of personal information or personally identifiable information, the train has left the station. We have GDPR, which PII is everything ever. You have over 130 student privacy laws, which define personal information extremely broadly, which obviously covers the vast majority of children.

And so I think the focus really needs to be less on what is personally identifiable because we've had a million and one researchers, others show how disparate pieces of information that don't seem identifiable could become identifiable. The identification is a spectrum not a definite. And because of that, this conversation should focus more on what rises to the level of needing that parental consent, as well as what use cases, what potential uses, what potential sharing should not be per se allowed.

KRISTIN COHEN: So you're jumping the gun, Amelia. VPC is next on the list. But before we get to that, I do want to ask the panel if anyone has-- this is a rule review, so we did make changes in 2013. Are there other pieces of information that we should consider adding to the definition now, keeping in mind the standard of allowing the online or physical contacting of the child.

And as part of that, I just wanted to read one of the questions we got in an earlier panel from I don't know if it was from Twitter or an audience member. But it's asking whether a COPPA is broad enough to capture concerns about sensor level data collection, cameras, microphones, other skin contact sensors. I did not know there were those. I guess that's the fingerprint. So I'll open that up to the panel.

ARIEL FOX JOHNSON: And if we think biometrics should be included.

SHEILA A. MILLAR: I think the use case, if you look at the COPPA rule revision including videos and photos, if you have child-directed properties or actual knowledge, that actual knowledge standard becomes very challenging in a world where I've got a security camera outside my house, and my neighbor's kid runs by and they're captured on the video. If I look at the video I have actual

knowledge, but does the operator? So I think they're really challenging questions.

And I think we also alluded earlier to the flip side, which is security. So increasingly, device producers are saying use your fingerprint, use facial recognition. These are security mechanisms to safeguard the device. So again, it's a matter of what is the balance that we're trying to strike to incentivize good security practices and protect children's privacy?

And with respect to persistent identifiers, the commission made the call, based on the input last time, that there should be this exception carved out to a per se rule about persistent identifiers. So within that framework of COPPA, I think directionally we need to think about those use cases and the law of unintended consequences about broadly defining these things as personal information.

KRISTIN COHEN: All right. Do you want to move on to--

JIM TRILLING: Sure. Let's go ahead and move on to VPC. We've discussed in several different contexts today that COPPA requires that online sites and services directed to children must obtain verifiable parental consent before collecting personal information from children under 13. Rather than prescribing a particular method that must be used, the rule says that the method must be reasonably calculated to ensure that the person giving consent is the parent.

We heard from Dona Fraser on the last panel and from John just a few minutes ago that there are questions as to whether the verification that is being done really does link a parent to a child. We've also heard from Morgan and again in the last panel, that parental consent is expensive and can result in significant drop off rates. Morgan showed some slides with feedback from developers and others about the challenges with VPC.

What is it that makes getting verifiable parental consent so difficult? And should the commission consider any changes to the COPPA rule that could both do a better job of ensuring that is the parent providing the consent and also make it easier for operators to obtain the consent? And I'm sure we will solve this quickly. Who would like to be the first weigh in.

MORGAN REED: I think there's two things that we have to consider about VPC. I would argue, VPC is intentionally frictionful. Because the other side of VPC is I can collect data on kids. And as we've heard over and over, part of what seems to be the concern is collecting data on kids. But if you have VPC then you can do certain forms of collection of data.

So some of the friction inherent in VPC-- I mean, some of the friction is inherent in VPC. And I think one of the areas that we need to look at is, I'm not sure that that equates to parenting. So if the outcome of VPC is to connect a child with a parent, OK, that's a regulatory concern. If our job is to help a parent be engaged with their child's digital [INAUDIBLE] life, then I'm not sure a single swing gate VPC is a great mechanism.

If you look at some of the just in time capabilities that you've seen the two major mobile platforms come out with, some of their parental tools, some of the way that they've been rolling this out, it's clear that they're working around the concept of VPC and going into ways of how do we engage with parents? How do we talk to parents about it? It's by no means perfect, but it's a lot closer to what parents have.

And I want to give the FTC a lot of credit here. They have a regulation that stipulates certain things. That doesn't necessarily equate to good parenting. And I'm not sure how you guys can work within the four corners of law to produce a VPC that matches with the way people want to parent online. That's why I go back to VPC is not a technological problem, it's a sociological issue.

JIM TRILLING: Do others want to weigh in?

JOHN E. AHRENS: I'd like to weigh in just for a moment, if I could. Of course, we come at this from a bit of a different lens because, as Morgan points out, that there's probably a good case to be made that this may be as much a sociological problems as it is a technology problem. And I say "problem," but challenge.

You earlier mentioned that maybe there's a cost issue involved. And certainly it's a cost issue involved. How we balance the cost and performance is something that goes on every day in our business. For those of you who don't know us, Veritad Technologies is a company that got its start in the early 2000s. We were one of the pioneers at developing and delivering an online age and identity verification based on trusted and verified data sources.

So today, of course, many years later, we're doing many more things than just using the data. We're using documents, we're using biometrics, we're using these other technologies that can be leveraged to verify an identity. So enter the issue of friction and cost because it's going to be a balance of all of these things that will compete for the first position. And from a technology point of view and a cost point of view, those who are delivering a service like ours,

they have their raw costs for getting these trusted and verified data sources together and having enough of them to create a good service for someone to consume, and with good reasonable certainty know that the person on the other end of a not present transaction is who they say they are.

And so we heard Dona mention the no silver bullet. We share that saying with each other quite a bit because there really isn't a silver bullet necessarily about any of this. But with good reasonable certainty, if you leverage enough of these technologies, you get closer to that place where you have some certainty. But when you do that, of course, you increase the cost.

And so the friction goes up, the cost goes up. And so you naturally have this competing balance that needs to be addressed as to how much friction. Of course, the friction is intentional. In fact, some parents might say I'm so glad that there was some friction in this, that you just can't get through. You're going to get declined if you don't give the right information, that kind of thing.

Yeah, I think we see this as a place for us to participate from the technology side of this. Exactly from the sociological, not much to add on that piece of it. But certainly, to give you some insight on the cost and the performance and how this all operates, I think there's certainly a concern in the developer community about the cost of actually providing a service that verifies the identity of the end user.

MORGAN REED: I want to add one thing. Don, in the first panel, for those who weren't here, said that it was $0.35 an API call is what their cost was for Pokemon. Now imagine that for a small developer. That's real.

ARIEL FOX JOHNSON: And I think it's useful to look at, as I believe Dr. [INAUDIBLE] and others have been saying, at different places where we can put in parental consent. From commonsense research, we know that something like 20% of kids are downloading apps by themselves. We know that as more and more people move to mobile there's less co-watching.

So in addition to apps having responsibility for trying to get parental consent, where are other places where we can ensure friction and we think parents may be more involved and can indicate that they are kids and that they need special protections?

AMELIA VANCE: I'd like to just jump in from the broader privacy landscape where we've been having all of the same discussions often with many of you from the FTC. It just seems strange to me that we're

spending a lot of time, as Laura mentioned this morning, on the notice and consent piece of all of this when the broader privacy conversation is moving away from notice and consent, and saying notice and consent is not enough when we're talking about adults.

If it's not enough when it comes to adults, I don't know why we'd have a higher expectation when we're talking about kids. Focusing more on that than on the use limitations and other pieces there, and underlying privacy protections, I think it's really important to focus much more on the latter than the former.

JIM TRILLING: Before we shift gears, I do want to follow up on some of the comments that have been made in Morgan's presentation and elsewhere about platform's role or potential role when it comes to VPC. Are there any changes the FTC should consider that might incentivize platforms to create VPC methods that can be used by other operators? Morgan.

MORGAN REED: I'll just reiterate. I spend about 40% of my life right now working on digital medicine and health care. And one of the most profound changes was when the FDA, who obviously has a lot at stake, produced their guidance from 2013 where they exercised what's called regulatory discretion. They essentially set up a risk pyramid and they said certain behaviors we really don't want to regulate. Don't call us. Leave us alone.

Then they have another category, which is we don't see an immediate risk of this. We're going to watch it but we're not going to require you to file a 510(k), et cetera, et cetera. And then there's the other category that had an obvious risk.

I think there's a lot to look at the way that the Federal Trade Commission could exercise some regulatory discretion, and experiment with ways to use the existing platforms and their current authentication mechanisms to provide a callable API for developers. I would suggest that it would not be that the FTC should abrogate their responsibility, but find ways to either do what Fintech does in regulatory sandboxes, saying only in this category or only in this feature. Or look at the FDA's model and say, what are some kinds of ways the data can be collected that still qualifies as a PII, Personally Identifiable Information, and yet we see the harm or the risk either for the data being used harmfully to kids or providing something that's not appropriate under COPPA? I think there's some ways to look at the way the platforms can serve a function. But they're not going to take that risk if the liability is too high both from a legal perspective and as a PR perspective.

ARIEL FOX I think we also have to be very careful with that, as I said earlier, we're defining what parents

JOHNSON: are consenting to on those platforms. A good example of this is the family stores, on both iOS and in Android. Some parents were going in thinking, OK, all of these things are appropriate for my child to watch. Some were going in thinking that COPPA protections attached to all of that. Some were coming in and just thinking, OK, there's protection from stranger danger.

And so, making sure if there are these sorts of experiments, that it is very clear when parents are consenting, what they're consenting to What is the piece there, and making sure that there's not a mismatch between consumer expectations and what is actually the choice that they're being given.

JIM TRILLING: Right. And that also relates back to one of Dona's points on the last panel about understanding of what content ratings are indicating and what they're not. Samantha.

SAMANTHA VARGAS POPPE: Yeah. I just wanted to make a quick point. A reminder that at its heart, COPPA is here to protect kids privacy and not companies bottom lines. And I think that's something that is easily lost in these conversations. One thing that Steve mentioned earlier was how difficult meaningful and informed consent can be. And I think it's a theme that we've been hearing.

And you know what? I don't think it should be an easy thing, honestly. I think a lot of parents do need to really understand just exactly what they are consenting to. And [INAUDIBLE] that's incumbent to others in this atmosphere to help make that information accessible, and understandable, and transparent, especially with an increasingly diverse population where English might not be a primary language, educational levels are varied and mixed.

There's a lot of fear and distrust of government. Now that's not technically related here, but just that sensitivity to privacy and information that's shared online. So I think that's just part of the broader consent conversation that we just really have to be mindful of and think about how that conversation affects different populations.

SHEILA A. MILLAR: Yeah. To follow up on what Samantha said, which I think is an excellent point, of the issues that you did not call out is-- or in maybe enough detail is the very specific notices that are required by the rule are quite prescriptive. And I do think it's worth evaluating whether or not you can simplify notices to be more useful to parents, number one. The second point I want to make follows up on what John said. It's not just a matter of cost in terms of getting VPC. But most of the more robust VPC methods have a cost on parental privacy.

And the notion that we would then have some big database that is a mediated way has its

value. And it has been looked at by the FTC over the years and not favored because of the potential security vulnerabilities that such a database might hold. And so these are all great concepts worth re-exploring in 2019 into 2020. But I think we want to be mindful that this whole risk calculation, there are burdens on parents as well as protections on children, and burdens and costs on businesses. And we're trying to find the right balance to protect children because that's the most important concept here.

MORGAN REED: But I think it's your former colleague, Dr. Lorrie Cranor, who's done some of the best research, and Amelia can talk about this too, on is there any actual way to get consent at a level that people understand? Dr. Cranor was the CTO for the Federal Trade Commission previously.

This is an open question. My only concern from what Samantha said, and I agree with you, my concern is the outcome is in order to make it hard to get consent, that what we do is lay waste to applications that are intentional about their application for children. And basically, everything is moved to the audience.

What did you guys say earlier? Folks were talking about intentionally or actively making sure that I don't know that they're a kid. Finding a way to say, I don't know if it's a kid.

If we make it so hard that you wipe out the people who want to do the right thing, then it pushes everybody into the general audience category. And the courts have made it pretty clear there's First Amendment speech protection around advertising and other activities. So again, I don't know the FTC-- it's not an easy road. But Lorrie Cranor's work on this is really good about what does consent look like.

KRISTIN COHEN: Thank you. Those are all really helpful points. So we want to have some time to talk about ed tech, which is an area that the commission has been thinking about and concerned about for a while. We held a workshop. In fact, a couple of the panelists here were at that workshop in 2017.

And you'll see in the rule review notice, we have several questions about ed tech and how the commission should approach it. There is nothing in the rule itself that says anything about schools providing consent for parents for ed tech. But the commission has given guidance to vendors that where the use of the data is for an educational purpose only and for no other commercial purpose that vendors can rely on the consent of the school.

At our 2017 workshop though, we did hear from concerned parents saying that they felt like

they didn't have control over their kids data. I have a comment card from a parent who was here at least this morning, may still be here today saying that where her child goes to school they're partaking in the one-to-one program. She or he has not been given informed valid consent to her children going online. And how can schools become more transparent? He or she feels that she's not getting the information she needs.

We have also, though, heard from schools about the incredible burden that would be placed on them if they had to get every parent to consent to every app or program that they wanted to use in the ed tech area. That was a lot of background, but I want to start broad before we drill down, and just ask the panel you know do you think that the rules should be amended to directly address ed tech and schools giving consent? And if so, what changes would you recommend? And I'll start with you Amelia.

AMELIA VANCE: Yes. Yes. Right now we're in a weird, gray area. It's very frustrating for a lot of the districts that Steve can talk about that we work with, as well as for parents who are like, wait, do I have rights here or not? And it's really important that it be very clear. Can a school consent on behalf of parents, and are parents allowed to then opt out of a particular technology being used?

And in order to provide the context of that, it's important to know what today's classrooms look like because it's very different from any of us who went to school. You had the first one-to-one device program, where every kid gets a device, a tablet, a laptop back in 2009, so just about 10 years ago. We now have a system that is really fundamentally run around technology.

You're taking roll through technology, you are perhaps playing math games, having personalized learning opportunities for reading, all sorts of things throughout the day. It is in some ways as if ed tech is the new text book. And so it's very important when we're talking about is there a right to opt out, is there a right for parents to delete data to realize that we are talking about them being able to exercise a level of control on schools that we've never anticipated before.

It is giving a parent the right to say my child has to use a different textbook, for better or worse, whether people like the tech in the classroom or not, that's essentially what it is. And so are we going to put schools in a position where teachers have to have 30 different textbooks? Or are we going to make sure that schools can continue to function and parents can exercise rights when it comes to non-core educational opportunities products, et cetera?

KRISTIN COHEN: Steve.

STEVE SMITH: In addition to my role as the CIO in Cambridge Public Schools, I'm also the founder of the Student Data Privacy Consortium. And I spend a lot of time traveling around the country speaking to school districts in all the states. And right now, 27 of the states have joined the consortium.

The number one question or kind of muddy issue is the overlap of COPPA and FERPA. That always comes up every time. To put a little more context, what Amelia was saying about today's classrooms, districts are all different sizes. But it's fair to say that every district in the country uses somewhere between 100 to thousands of apps every day.

To think about parental consent for 1,000 apps in the various classrooms, it really is an unmanageable feat to be able to record who consented for which app. So the practice based on the guidance of schools being able to consent on behalf of parents under the conditions that the app is only used for educational purposes and no commercial use, coupled with schools leveraging what's known as the school official exception in FERPA to share student level information. The school official exception has some other kind of controls around it, where the schools need to actually have control over the outside provider and control over that data.

So the practice that the consortium has been promoting across the country is the use of model data privacy agreements that establish this school official exception and allow a school district to share student level data with the vendor knowing that the data is only going to be used for the purpose that that application, that educational purpose, it's not going to be resolved. When we're done using it the data will be deleted. So it has all those controls over it and enables us to onboard and know that the application has been vetted properly by professionals.

Like I said earlier, I'm concerned that a portion of our parents would not be able to make informed consent on applications. They'd be consenting to things that are inappropriate and maybe not allowing things that are perfectly secure. From a school district's perspective, the idea that schools are professionals that are charged with the protection and safety of children in the school environment, in an online environment, on the playground. And I feel like properly trained school officials can make very good decisions about apps and ensure that the data is being protected when the data is being shared with the providers.

So some way of tying COPPA to potentially the school official exception. How you would do

that I'm not sure. But knowing that those controls exist within the school official exception I think would be something to consider.

KRISTIN COHEN: Ariel, did you want to--

ARIEL FOX JOHNSON: Yeah. I think it's important to remember that kids in school are particularly vulnerable, even more so than kids at home. Their parents are further removed, you're dealing with all kinds of different populations, you're dealing with parents, as Steve was saying, who have even less ability to provide informed consent and to know what's going on, and feel like they have a choice or their kid might be left behind. It sounds crazy to have 30 textbooks, as Amelia was saying.

We also have never had this level of commercialization and information collection living on about our kids as they're trying to learn and trying to figure out who they are and who they want to become in what should be a protected space. We hear from parents at Common Sense that they feel like they don't know what's going on in schools. So parents need to be able to have a better sense of what's going on.

It also seems like there's a middle ground in terms of schools being able to make smart decisions. And in that sense, any sort of exceptions for when parental consent is allowed, there should be higher bar for when you can consent for non-commercial purposes, for making sure that there's informed notice for parents, for making sure that there are appropriate deletion rates, for allowing for analog options when possible. Products could identify as education products if they want this exception.

Right now, there's a lot of consumer products, even products that say we're not for use in schools, that are used in schools similar to products say they're not for kids under 13. So I feel like there are smart ways to better protect students. But unfortunately, education is currently one of the spaces where we see they're not being protected. I think this is also an area where the FTC-- I know you guys have had workshops on this-- but could use it's 6(b) authority to dig deeper into what's going on in the ed tech market because this is obviously a huge market and a huge way that kids are profiled and collect information these days.

KRISTIN COHEN: Well, I'd like to drill down a little bit into ed tech and how the COPPA rules should work. And we're going to use a hypo, wrong hypo. So Company Q is an ed tech vendor that sells an app used in the classroom to help kids with their reading. Sorry, this was slightly different than what

I have here. Thanks, Jim.

I collect from children their name and their voice recordings to share with their teacher. I have contracts with several large school systems. But I also make my app available to parents individually. And sometimes teachers sign up directly.

And considering how you think COPPA should work, should I be able to get the consent of the school for this information collection, or should I be required to get the parents' consent? And if I can get the school's consent, what about a teacher, or does it need to be at a higher level? I will start with whoever wants to weigh in. Steve.

STEVE SMITH: Yep. I definitely feel like the vendor should be approaching the school district to sell the product and engaging at a higher level than the teacher. Typically, teachers are not allowed to engage in a contract. Yes, I know it's happening and they are signing up. But technically, a contract between the school district and any type of vendor would have to be done at the district level. Based on that model, that would take care of the parental consent.

KRISTIN COHEN: Ariel, do you want to weigh in?

ARIEL FOX JOHNSON: I agree that it shouldn't be at the teacher level. I don't know what Q is doing with all of this information? And that would affect my opinion on whether the school can consent on behalf.

MORGAN REED: [INAUDIBLE] the hypo is Q. I think there's one small area that's worth noting on this. Ironically, some of the platforms, in order to protect privacy, actually don't let developers know what school systems have purchased their apps because you can do a volume based purchase. So you'll see 10,000 of your apps disappear, being bought in one day. And you're, that's definitely a school, if you've got an educational app.

And so back to reaching out to your-- sometimes it's a classroom, so it's 60. But you get a hint that there must be something going on. But sometimes it's hard. And then you have to backtrack and figure out who was it that bought it.

So there are some ironic realities of trying to protect the identity of the purchaser of the application and not collecting information can lead to a quixotic tilting at a windmill to figure out which school district do I need to reach out to. I think that's a solvable problem. But it's one that we shouldn't be too handwavey about because that's good privacy behavior. Don't let the developer necessarily know unless they-- from a data minimization perspective, if they don't need to collect the information then they shouldn't be collecting it. And you only know that an

application might be used in an educational environment if you are aware of what school district it is.

STEVE SMITH: I just want to say, there's two sides to that too. There's a huge awareness building that needs to happen in the schools so that the teachers don't just sign you up. They know that there's a process to go through to have it vetted and on boarded. So it's a building awareness on both sides.

SAMANTHA VARGAS POPPE: This is an important conversation to have. And tied to my work with underserved populations, we frequently see in various policy areas across the board where certain bad actors are trying to take advantage of financially insecure populations. And this is something that I'm particularly concerned about in the educational technology space because we have so many cash strapped school districts with teachers who, and administrators who want to do the best, and parents who fall into that too. And it's easy to check a box.

Not every district is lucky enough to have its own Steve Smith, I'm sure. But I think in talking about this, we need to think about how different school districts, based on financial resources, might fall victim to some bad actors getting in there, getting kids data, doing who knows what with it. So if we do move to school consent, really do need to make sure that it's the right administrators and people doing it, but that there are certain strong definitions and safeguards to help protect children, and parental, of course, parental involvement.

AMELIA VANCE: I think it's important to take a step back when we were talking about ed tech and privacy and as I said earlier, acknowledge that we're actually in a very different legal landscape that's actually much more protective than all other child privacy environments. As I mentioned, you have 130-plus student privacy laws. About 25 states have laws directly aimed at vendors, with vendors on the hook if they're using information for non-educational purposes, selling it, targeting advertising to students. You have FERPA overarching, providing privacy protections there. You have COPPA weighing in as well.

You can also add to that things like student data privacy consortiums, contracts, which mean, again, that the vendor is the one on the hook if they're violating that. In many ways, the data that's being collected through schools is actually much better protected and can be used in ways that are helpful to students, that help students learn while also being reassured of the fact that there are legal protections there. Now of course, the key to that is making sure that we're enforcing those legal protections, that the contracts that are being signed have some

sort of check on them, all of that. And that I think is a better focus rather than worrying about the individual thing.

Because oftentimes, when we're talking about the parent consenting versus the school, I take a step back and I'm like, OK, first of all, that's going to disadvantage certain communities where parents aren't as involved, may miss a form, which as we all know is very easy to do. And if something is so dangerous, falls out of the educational purpose that you need parental consent, well, maybe you shouldn't be using that in the classroom to begin with. At that point, I think we end up with information that is both better protected without maybe causing inequities when we're depending on parents to have to pay attention to those potentially thousands of apps.

KRISTIN COHEN: So going back to the hypo for a minute. One of the questions we get asked a lot is about our guidance that says that where an operator gets the consent of the school it can't be used for any other commercial purpose. And what does it mean to be another commercial purpose?

So looking at the hypo, would that operator, Company Q, able to use the voice recordings to improve that particular app? Or would that be another commercial purpose? Or what about using it to improve their voice recognition software that they use in another non-educational app? Would anyone like to weigh in?

AMELIA VANCE: I think product improvement is a commercial purpose.

KRISTIN COHEN: And that's even if it's to improve the particular product that is being sold to the school for the educational use?

AMELIA VANCE: In many cases, the schools are-- we might think about it like, oh, well, you're getting a free app and they're getting app improvement. In many cases, the schools are shelling out a lot of money for this. I'm sure Steve knows better than I do. You're paying for the service. And I don't think we should be paying with children's data for product improvement. I think that's a commercial purpose.

We have to be careful there because product improvement is a very broad spectrum. If there is a security vulnerability and a patch is pushed through the system, that's product improvement. And we don't want security holes to exist.

If there's a new educational research that's been put out that says kids learn math more effectively. And so this math application puts out, here's a slightly different way to ask this

question, that's improvement. And I think the vast majority of people want those two types of examples to happen.

Where we get outside of that, which is the last part of that hypothetical, and talk about improving things overall is where it gets much more difficult and much muddier in terms of, again, consumer expectations, school, parent expectations. And exactly how far should we go for the good of improving voice recognition generally? Should a company stick its head in the sand and say, well, we know that this voice recognition thing over here worked better when we did it this way but we can't apply that improvement to everything else. The answer to that feels like no, but it also feels like a step beyond that educational purpose.

SAMANTHA VARGAS POPPE: I think that's right, Amelia. And I do think, again, it comes back to what are the policies we're trying to advance, what are the privacy considerations we're trying to solve for? And so if we are going to put strict limits on what Q do with the data to either improve that specific educational product, whether it's for that school district or for other school districts, or to more broadly apply its learning to improve its product line, assuming there are good privacy protection. It's de-identified, et cetera, et cetera. I'm not sure that that's going to advance the goal of expanding educational technologies for children in the schools. Because if you're underwriting the school use for some broader use, that limitation may be enough to say I'm just going to not be in the ed tech space. So I think it comes back to that risk balancing approach and really looking at it with a view of both advancing privacy for children and making sure that we're not putting too much friction, as Morgan says, on legitimate business operations that even if they just strictly advance the interests of the business.

KRISTIN COHEN: Going back to the hypo for-- and this will be the last question from the hypo-- but it's around deletion. COPPA is very specific that parents have the right to have their children's personal information deleted. However, in the educational context, sometimes there's a concern about allowing parents to have their kids information deleted. What if it's a grade?

In the hypo, should the parent be able to go in and have their child's voice recordings deleted? What if the app also has a grade related with the child's reading? Any thoughts from the panel?

STEVE SMITH: So I'll jump in. Considering many of the core applications that districts use nowadays are hosted apps that the student information system that has all the student record information. Obviously, we wouldn't allow a parent to say I want all my child's records deleted.

And then we have the other extreme, such as this particular hypothetical, that's more at the classroom level maybe not as critical. But again, coming back to the idea of we are establishing all these products, as school officials for a purpose, we're almost extending the school's infrastructure. And it becomes a core system, or else we wouldn't be using it. Having those records fall under FERPA, the parents would have the typical rights of being able to inspect and change and correct any errors, but typically not delete the records.

AMELIA VANCE: I think you've run into some really awkward clashes of the law. For example, Wisconsin requires that there be record retention for voice. And so all of a sudden, if this became the rule, you'd have state legislators trying to determine, well, does this belong here or does it fall under we're supposed to keep this for five years?

There are lots and lots and lots of records like that in the educational context that state and federal legislators have decided are important enough to keep. Some of it is because we want parents to be able to access it later. Some because like with transcripts, test results, students may need it down the road to apply to college, to get a job, to travel, whatever it may be. And so it's really important that we consider the school-specific context.

This isn't to say that data shouldn't be deleted. In fact, it is a best practice that you have, not keeping data longer than necessary. It's part of COPPA. But that doesn't mean it's something that should be specified in the rule and reference to schools. Instead, I think it's worth furthering best practices.

There's a district in Maryland that this year held its first big data deletion day. And they took all of the data that was no longer necessary, the behavior tracking in the classroom that had happened throughout that year, not essential data, and a bunch of various education apps, all of that stuff that wasn't necessary and cleared the board. You had that right to be forgotten that was talked about in the first panel for all of the kids in that district. And I think furthering those things as potential best practices, revisiting the data to make sure it actually is necessary, is a best practice, but not something that should be mandated under COPPA because there are too many state laws and policies and other things that would be very problematic to work with.

KRISTIN COHEN: Steve, I want to follow up on this for just one minute before we move on because we need to start wrapping up and moving to other questions. But the idea that parents wouldn't have the right to delete, as Samantha pointed out, not all school districts are created equal. And

whereas you appear to have done a lot of thinking about this, I know others in the room who I've spoken to similarly are taking this seriously, there are a lot of small school districts who aren't paying as much attention to this. Is it fair in those situations for parents not to be able to go in to get this information deleted? And what is the right balance?

STEVE SMITH: There is definitely a large percentage of districts across the country that don't have the capacity to do what I've been describing. And that was really what sparked the creation of the consortium. The tools and the practices that we've created are made in such a way that they can be reproduced across the country in all the states and all the districts so that districts that don't have the resources can use these model contracts and implement these practices.

We are going through a period of time where we've talked a lot about building awareness. You got to build awareness for parents, we get it for school personnel, and it's a growing stage. I don't know if PTAC is still here, but it depends. It depends on every situation.

What I am proposing or talking about is the ideal. It is doable. It is expandable across the country that we can create these systems to ensure that all data is protected in the classrooms.

KRISTIN COHEN: Thank you. So I'm going to turn it [INAUDIBLE].

JIM TRILLING: Company Q has not cornered the market on collecting recordings of children's voices. In 2017, the commission issued an enforcement policy statement that said that the FTC would not bring enforcement actions against companies that collect children's voice recordings as a substitute for text, such as for a search function, as long as the audio recordings are held for only a brief time and used only for that purpose.

The commission opined that these types of uses of voice data could be useful for certain consumers, including children, and pose little privacy risk if the information was deleted immediately. Should this policy be codified in the COPPA rule? And if, so should companies be able to de-identify the recordings to use them to improve their voice recognition software? And I'd actually like to start this one with Ariel since Ariel talked about the product improvement in the ed tech context.

ARIEL FOX JOHNSON: First, I'm skeptical that you can de-identify the voice recording. But I recognize that de-identification is a spectrum. In terms of not treating I guess transcribed text as something that's covered by COPPA, to me, it's the equivalent of an open text field. So if you're otherwise

a COPPA operator, I would think that you should treat transcribed voice recordings the same way as you would treat an open text field, where a kid could say personal information and could easily disclose that when talking to a smart device in the home.

JIM TRILLING: Other views.

SHEILA A. MILLAR: I'll just follow up on a smart device in the home. So first of all, the smart device in the home is not directed to children. And I think that that is part of the scoping conversation that is going to be a really important part of this new request for comments. But I'll draw the analogy to the physical product space for example.

A children's product is defined in the Consumer Product Safety Improvement Act as a product designed and intended primarily for children 12 and younger. My smart refrigerator is not a children's product. Even if children are likely to open the door and access the refrigerator it is not a children's product.

And so I think that tricky line of what's general audience and what's a children's product gets increasingly complicated with the connected products space. If you have a connected children's product. I'm going to separate, Ariel, the home device from a connected children's product. The audio recording does have to have some sort of COPPA approval.

So the analysis of email plus, which could be a great way to get parental consent if it's used for internal marketing. The question about whether speech recognition technology is voice recognition technology I think are two different things. The companies that I've worked with are offering speech recognition technology. So if they collect my voice they don't know it's Sheila Millar. They try to figure out what I say and then provide a response to a natural question in a natural way. So I think we have to unpack a little bit what the questions are to come up with the right policy response. But I think that enforcement discretion concept has been extremely helpful in helping to advance the use of audio technology in a useful way that can be privacy protected for children.

JIM TRILLING: We are almost out of time. So of course, it's a lightning round. In 30 seconds for each of you, we've talked about definitions, exceptions, and misconceptions. What advice do you have for the commission based on this discussion in terms of changes the commission should or should not consider making to the COPPA rule? And why don't we start at the other end of the table. I'll start with Samantha this time.

SAMANTHA VARGAS POPPE: Sure. I think I'd like to leave you just with a reminder that our kids today find themselves at the epicenter of a very powerful and largely unknown digital world, and at the heart of a lot of privacy battles. I think that now is not the time to look to exemptions to this rule or watering down the rule. But that we need to look at how to strengthen the rule.

And I think an easy way to do that would be-- Ariel hadn't mentioned the commission 6(b) statutory authority. I would call on the commission to really exercise that option to learn more about how our multicultural youth and just this complicated nature and evolving, rapidly evolving atmosphere affects our children and how they're operating in this space. I'd also like to just really urge the commission to take action to provide more even and robust enforcement of what is a strong rule across companies on some of these bad actors who are flagrantly violating these protections and putting our kids at risk.

JIM TRILLING: Steve.

STEVE SMITH: I'm going to reiterate what I had said earlier about somehow connecting COPPA to FERPA, particularly the school official exception in a more formal way so that schools are in a sense given more direction about the processes they need to go to vet an app and approve an app. And I think that would help.

We certainly do not want to do anything that's going to hinder the great tools that are in use in classrooms to support teaching and learning. But at the same time, we want to help those schools that don't have the resources to put some more framework around what processes should be in place to ensure that applications are vetted.

JIM TRILLING: Morgan.

MORGAN REED: Samantha's point in increased enforcement of flagrant violators, and frankly faster enforcement of flagrant violators. It takes you guys a long time, which means entire markets shift. Second, take advantage of the way that the platforms are implementing privacy forward engagement tools, whether it's just in time notice or other capabilities to allow developers to tie into that so that we can actually build apps that don't harvest kids information or rely on that harvest and can make appropriate use of information for internal uses. And then finally, don't hold up our progress. Let's find ways to make re-consent effective.

JIM TRILLING: Amelia.

AMELIA VANCE: So echoing Steve, definitely aligning FERPA and COPPA. I think the protections in FERPA are

the right ones, and it makes sense. Making sure that, as I said, there's a little less focus on the notice and consent pieces of COPPA, and emphasizing that there are other COPPA protections that folks have to adhere to. We see this all the time in contracts with schools or in terms of service that we're passing on the COPPA burden to the schools.

You might be asking the school to get consent, but you have responsibilities, the operator. And so making that a little more aware. And then finally, incorporating more kid voices.

Putting them at the table, even if they may not be part of panels. Doing what the UK, doing what Ireland has done. Putting together commissioning research to find out exactly how they are interacting with these systems I think is extremely important and something the FTC could take a lead on.

SHEILA A. MILLAR: So I think COPPA has actually withstood the test of time reasonably well. And the commission has done a really good job at trying to update the rule to reflect technological changes. I think it just remains critically important that you maintain that balance of protecting children with acknowledging that there are legitimate business needs to collect and use data. And putting those guardrails around how that happens, along with making sure that you have the right amount of enforcement resources and that you appropriately target those resources where they're most needed, as well as continuing to offer great educational resources along the lines of the things that you already offer today.

AMELIA VANCE: I think just in any balancing test you have to remember that kids and protecting kids are what's most important with this role. I think I echo every other panelist here. You have to be thoughtful if you're going to make any changes. They should be informed by research. You should use your ability and authority to conduct more research, especially those in the consumer community are able to do. And you should focus on, since you have a role that has withstood the test of time, you should focus as much as you can with your resources on enforcement as well.

JOHN E. AHRENS: So with respect to the regulatory frameworks, [INAUDIBLE] is mostly in the identity in the age verification space. What I would say is that the need may be for the commission to spend a little time with technology providers like ours. A little bit more of that because it may enlighten you to some of the challenges that they're facing too to provide the end user with a product that they can actually leverage, which got a good balance of cost and performance that you'd be happy with.

And there are a lot of technologies and new technologies. The question is, how would they fit into your framework for the regulatory environment? So we'd be happy to participate in that, of course. But I think that would be a potential takeaway for the commission to look into, spending a little bit more time with the technology side, maybe to be balanced with the others that have been mentioned here today.

JIM TRILLING: Well, thank you all for a great discussion. We are going to break until 3:15. And then we'll be back for our final presentation and panel.

[APPLAUSE]

Thank you all. We're back on and we're about to begin panel four, the misuses and misuses of persistent identifiers. Before we do that, we have a presentation by Jonathan Mayer, who's an assistant professor at Princeton in the computer science department and Woodrow Wilson School. Jonathan, come on up.

JONATHAN MAYER: Thank you. Thanks. Good afternoon. Before getting into substance, it occurs to me to mention, I think I might have the dubious distinction of being the only participant today who benefited, albeit briefly, while growing up from COPPA. So thanks, Federal Trade Commission.

My goal is to provide a computer science perspective on technology trends and the state of research around children's privacy online. In some sense, what I'm going to briefly touch on is the computer science parallel to Jenny Radesky's excellent overview this morning. I especially want to highlight open research questions since the commission has an opportunity to encourage research, and to use its own section 6 authority in the course of evaluating the COPPA rule.

So the three areas I'd like to get into are first, trends in mobile device adoption and usage. Then I'll talk a bit about the Internet of Things. And then last, a bit on educational technology or ed tech.

To start, mobile devices. In 2010, the FTC was where we are now, kicking off their review cycle for COPPA in March 2010. And perhaps conveniently, the next month the iPad launched, changed quite a bit in the landscape of children's mobile device usage. So let me highlight some key points from the literature on children's use of mobile devices and devices in the household.

First, unsurprising probably to everyone in the audience, household adoption of mobile devices is now nearly universal, up from about half of households at the time of the last revision of the COPPA rule. About half of children age eight or younger now own a mobile device. And that's most commonly tablets, up from essentially none at the time of the last COPPA revision.

In terms of usage, it appears across multiple studies, children are using these devices in the ballpark of about an hour a day. And usage is much, much higher than traditional computers, which of course is where the COPPA landscape got started. As a corollary, usage of traditional computers is in decline. And a lot of that seems to be because children are playing games on mobile devices rather than playing games on computers.

The last panel mentioned disparate impact concerns that might come up under a COPPA. And I want to mention that it appears to be the case that child usage of mobile devices does have some unequal distribution depending on minority status, income status, and educational status. As for what children are doing with these devices, perhaps again unsurprising to those in the audience, kids are watching online videos, they're playing games, and they're using other apps.

An important point about what children are using on these devices is that it often is free stuff. The same as for adults. And that can put a lot of pressure on privacy because data can of course be quite involved in monetization models.

Let me say a little bit more about online video consumption. Traditional TV viewing time seems to be in decline. It's about a quarter down since the last COPPA revision. Meanwhile, online video viewing time on mobile devices is through the roof. Certainly no surprise to anyone who's engaged with small children in the audience.

The popular categories of video are what you might expect, educational content, cute animals doing stuff, how tos. Unboxings are apparently really, really popular. So not actually like using devices, just opening up the box and getting at the device.

Music videos. Anyone who's seen *Baby Shark,* of course, knows that. Game streaming is particularly popular, since kids, instead of playing games themselves, watching others play games. And then stunt videos, the sort of big dramatic, like here is someone falling on their face type video.

And of course, the landscape of which media apps kids are using seems to be changing quite a bit. YouTube's been around-- it's odd to think of YouTube as like the old media platform at this point. But in a certain sense, it is.

As for gaming, one of the big shifts since the last COPPA revision has been the growth of these just super popular mega hit games that have a younger target demographic than games that were of that level of popularity previously. So some of the better known ones I suspect for folks in the audience are *Minecraft, Candy Crush,* and *Fortnite. Minecraft* about the time of the last COPPA revision, same with *Candy Crush. Fortnite,* of course, coming much later.

As a corollary to these types of games becoming very popular on mobile devices, console and portable console gaming seems to be in decline. Instead of playing a Game Boy or a PlayStation at home children are now playing more on iPads. And gaming time on mobile devices has increased quite a bit. And overall gaming time, some [INAUDIBLE] suggests, is going up.

Now an important thing to note about the shift from consoles and portable consoles to mobile devices is that there is a greater opportunity for privacy impact associated with the gaming on mobile devices than there is with consoles and portable consoles. These games are often free to play and have a monetization model that either involves advertising, which of course is going to have some data associated with it, or involves in app purchases, which of course can involve concerns around consent and what children know about the purchases. And then social features are also increasingly common in these games in a way where they weren't historically in console or portable console gaming.

So there's the state of what we know. Now let me highlight some open research questions. One really important one is there's still not outstanding research on the apps and content platforms, specifically that children are using.

Jenny Radesky gave us some excellent initial results on preschoolers. And that's an important demographic. It's also, of course, important to know about other demographics. And especially as children get older, they're going to have more crossover with the types of apps that adults might use. And so there's a tremendous opportunity for research here and a need for research on what kids are actually doing online.

There's also not as much research as one might hope on the privacy properties of these child friendly apps. And when I say "child friendly" here, I mean apps that children are using, not

necessarily child directed within the meaning of COPPA. So there's been some good initial work suggesting that these apps collect and share personal information just like other apps. In particular, collecting unique identifiers in association with online advertising and analytics. But there definitely needs to be more work on it.

There's also been some work suggesting advertising is very common in these categories of apps. And the ads that appear in these categories of apps are the sorts of ads you might expect in an adult app as opposed to child appropriate advertisements. Again, more need for work on that. And then there's been some initial work on the privacy disclosures with these types of apps, suggesting that they provide limited information and are not necessarily sufficient for parents to make informed choices. Again, more need for work on that.

Another challenging area for research is would these apps consider themselves covered by the COPPA rule at all, and how they comply with the COPPA rule? And so, since I'm calling for all of this research, I guess it seemed to me I should take the opportunity in FTC that's like do some quick research. So I actually looked at the apps that Jenny Radesky highlighted this morning, and looked at the privacy policies of the apps. And I interacted with them a bit to try to get a sense of do they think they're covered by COPPA?

Her preliminary results show that preschoolers are using them quite a bit. And if they do, how have they implemented COPPA? I mentioned this not to pick on any particular service. I want to emphasize this is really preliminary. But to give you a sense of just how challenging it is as a computer science researcher to get a handle on how these types of apps are implementing COPPA or disclaiming COPPA.

So one of the top apps that she highlighted was Netflix. Netflix prides parental controls, including you can create a kid's profile in an app. You can say, I only want this profile to see little kids content or older kids content.

There aren't COPPA disclosures associated with that. And it may be that Netflix is implementing COPPA and claiming the internal operations exemption. It may be that Netflix isn't implementing COPPA. As a researcher there's just no way to say whether Netflix is doing either of those or something different.

Another app that she highlighted was Amazon Prime Video. There's a children's privacy statement associated with Amazon services, but it's broadly applicable to all Amazon services. So as a computer scientist, again, it's very difficult to say in a rigorous way whether there is or

isn't a compliance issue there.

Nickelodeon Junior, there is an easy example as a researcher. So go to the Nickelodeon Junior Prime App privacy policy. It says we're covered by COPPA. Here's what we do to implement COPPA. Detecting compliance there and doing it potentially in a large scale way, there's an example where it is doable.

One of the games that she highlighted, *Children's Doctor Dentist,* has a privacy policy that just says this app isn't child directed. And then another, *Subway Surfers* has a privacy policy that says that the app is general audience, but if we find out you're a child, then we won't do behavioral advertising.

Unclear how consistent that particular direction is with COPPA. And then the age [INAUDIBLE] involves a little dial that by default puts you between December 1999 and January 2000. So over 18, again by default. Is that compliant with COPPA?

As a computer scientist, it's just extremely difficult to give a definitive answer at scale. And we'll talk more in this panel about the ways in which the ambiguities around persistent identifiers and internal operations can really inhibit research.

That's most of what I want to say about mobile devices. I'm being sensitive to time here. Next stop in the Internet of Things. There's clearly been an explosion in adoption. Smart speakers are taking off. It's not clear how long the trend is going to last. But they're certainly getting increasingly adopted in households.

Streaming devices and smart TV ads are also obviously taking off. And so there's some discussion earlier today about children moving from one-way platforms to two-way platforms. It's important to keep in mind as a corollary to that, that some of the platforms that were previously one way are now platforms that are also two way.

And then there's also been a market explosion in internet connected toys. I found it difficult to get good numbers on this part. Part of the issue is that defining the market is itself a challenge. But clearly, a growing market too.

The state of research in this area as of about a month ago was kind of thin. Thankfully, we have the benefit of literally four papers on IoT security and privacy dropping in the past month. And they're really good papers. So there's not a lot more that we know.

That said, there are some big open questions. The first one again being, what specifically are children using? Which brands are they using, which devices by those brands? How are they using those devices? We don't have that fundamental data. And that's very important if the overall goal is going to be protecting children just as they engage with online services in the real world.

Another open question, as with mobile apps, is what the privacy property properties of these devices are. Here again, there's been some recent really outstanding work, including by folks at Northeastern, who set up model living rooms, both in the US and the UK. Some colleagues of mine at Princeton, who actually got their hands on a house just next to campus and set it up as a smart home, and have built this way of collecting information about devices in ordinary homes at large scale.

So there's a lot of evidence that IoT devices are behaving in ways that are similar to mobile apps, which prior work had demonstrated as similar to web tracking. This ecosystem of advertising, where identifiers get shared with a number of entities for ad targeting purposes, ad recording purposes, and also analytics is cropping up around Internet of Things devices, and in particular, smart TVs and streaming boxes in the same way, again, it cropped up around mobile apps and the web.

There's definitely more work to be done here on understanding parental controls and in understanding whether parents are making informed decisions. So there's been a little bit of work on that that suggests that parental preferences are extremely context specific, and audio recording is a particular point of sensitivity. And last, that the existing controls do appear to be quite frustrating to parents. They're difficult to use and they're difficult to understand. Again, more work needed there.

The last topic I want to touch on is ed tech. And here, the high level points I'd like to make are that the investments are absolutely massive. It is clearly a growing market. And some of the particular areas of ed tech that are seeing great commercial interest are in school administration, of course, content management. As a teacher, thank you, please disrupt the course content management space. Classroom communications, educational materials, and exam proctoring.

And here, I just have a slew of open questions I'd like to flag. The state of the research is really not what you would hope, especially given the level of interest and investment in the

field, including fundamental questions like does this stuff even help children learn? There really hasn't been nearly enough good science on that. Again, what are students using, what are parents using, what are teachers in schools using? What are the privacy properties?

How is the regulatory environment interacting with the offerings that are now available? What are privacy expectations? How are folks using controls? How do folks perceive consent? All areas that need a lot more research.

And so I'm enthusiastic that the FTC is starting so early on this COPPA cycle because hopefully, we can answer a lot of these questions in time for the COPPA revision. So that's what I wanted to touch on. I think we'll probably dig in much more again into the identifier and internal operations components of those issues during the panel. Thanks.

[APPLAUSE]

MARK EICHORN: So panel four. I'm Mark Eichorn. I'm an assistant director in the privacy division. And I'm here with my colleague Laura Hoskin, from the Bureau of Economics.

We're going to be spending the next hour and change talking about persistent identifiers. The fact that you guys haven't left is a good sign. We've heard a lot about persistent identifiers over the course of the day. And it's really integral to COPPA, one of the more significant changes in the 2013 revision to the rule.

Basically, the definition of persistent identifier and the definition of personal information was changed. Just so we're all on the same page, the definition now reads, "A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifiers includes but is not limited to a customer number held in a cookie, an IP address, a processor or device serial number, or unique device identifier."

One of the main consequences of changing the rule to include persistent identifiers was to bring behaviorally targeted advertising within the scope of the rule. That prohibition also extends to third parties that have actual knowledge that they're collecting information from kid directed sites. When the commission revised the rule, it also recognize that persistent identifiers are used for many other purposes and in fact, many other essential purposes. So the commission created an exception to allow the use of persistent identifiers for support for internal operations when that's the only type of personal information covered. A lot of our discussion in the panel will focus on either the concept of persistent identifiers or the concept

of support for internal operations.

Just a reminder, comment cards are available here in the auditorium if you're here. Or you can submit questions by email or Twitter. And because the panelists' bios are available I won't go through their histories. But I was going to let each person have the opportunity to say where they're from and introduce themselves. James, do you want to start?

JAMES COOPER: Yeah. Hi. I just recently left a stint here at the FTC. And I'm back at George Mason Antonin Scalia Law School teaching [INAUDIBLE] again.

HARRY JHO: I'm Harry Jho. My wife and I are the creators of Mother Goose Club, one of YouTube's earliest kids channels.

KATHARINA KOPP: Hi. My name is Katharina Kopp. I'm with the Center for Digital Democracy. And for those who don't know, the Center for Digital Democracy is represented by a large coalition of child advocates and a broad coalition, and supported by Georgetown's Institute for Public Representation. We were the ones who led the charge to get the COPPA passed in 1998. And also, we were the ones as part of our coalition who really pushed for the broadening of the definition of personal information to include persistent identifiers.

MARK EICHORN: Hi, again.

KATE O'LAUGHLIN: Hi. I'm Kate O'Laughlin from SuperAwesome. SuperAwesome is a kid tech company. So we're providing products, services, infrastructure to ensure safe engagements with kids when they're online.

JULIA TAMA: I'm Julia Tama. I'm a partner at the law firm of Venable, LLP.

MARK EICHORN: And I want to thank Jonathan again for kicking off the presentation. And I want to thank each of you panelists, for sharing your time and expertise with us today.

LAURA HOSKIN: We want to start off by talking about both the pros and cons of collecting persistent identifiers. And we'll start with the cons. We're particularly interested in how these might have changed since the last COPPA rule review since 2010. Who would like to start? Katharina?

KATHARINA KOPP: Sure. I think it's important to remind ourselves how important it was to have persisted identifiers included in the definition because everyone in this room and everyone above 13 and older in the US today is subject to constant surveillance and programmatic behavioral

data collection and use practices on all their devices all the time. This is a growing privacy problem for all except for children, which are protected by COPPA. So really, persistent identifiers are the foundation for behavior on programmatic advertising.

And today, as a result of this rulemaking, we do not see this programmatic advertising options in the programmatic space. But of course, we see a lot of noncompliance still because it's not being enforced properly. Also, we see the problem for teens and generally for adults.

So really, the children are the only Americans today who are not protected in this way. But before I go into some of the negative impacts, I just want to also remind ourselves why piracy is important. I think we maybe lost a little sight of this, why it's important for all of us.

We here believe that piracy is a fundamental right. It's not something that should be negotiated in terms of pros and cons. But it's a fundamental right.

And where trackers or persistent identifiers are used, that right is typically undermined. And so talking here about loss of autonomy, decision making, integrity of individuals, loss of dignity, loss of seclusion, the rights of seclusion, fair processing of data really increase in undue manipulation. So that's because of information technology to impose hidden influences on users by targeting and exploiting their vulnerabilities.

And as was mentioned in the previous panel, for the first time today, privacy is in our mind also a civil right. So any denial of equal opportunity and unjust discrimination can also come from violations of privacy rights. These are really all in our view cumulative negative effects that impact the individual. And of course, there are societal negative impacts that I'm going to skip out for.

But to mention, increasing inequality we believe comes from undermining privacy rights. And really as we've seen in the last elections, undermining of democratic institutions with voter suppression. But specifically with regard to children, and I'm going to expand a little bit more, I think we have to understand that privacy or the use of persistent identifiers really we have to look at this as a very intertwined space.

We have marketing, we have children's content, and we have data collection. All these are mutually integrated. And so we have to understand the entire ecosystem to understand why persistent identifiers are harmful.

So really, at the beginning of childhood, in the very early stages now, marketers are trying to

attract the attention of children, to develop content, entertainment for them so they can collect more information about them so that they can deliver audiences to advertisers. This has led to an increase in more and more content. [INAUDIBLE] more and more devices, more and more sophisticated ways of collecting information and hooking children to content and entertainment. Specifically, my organization has looked a lot in terms of-- it was mentioned earlier, and for example, in fast food and other unhealthy foods and beverages marketing and advertising to children, who are particularly vulnerable in this regard. We are facing a childhood obesity crisis of epidemic proportions. And the impact on low income and youth of color is particularly high in this area.

And then of course, there are related costs to state health and federal health care. So all these are negative impacts of it. Then also, child psycho and social development, impact on the family and social interaction. We didn't hear that much from Jenny this morning specifically on this, but there is a lot of research.

Obviously, that was the reason why the Center for Media Education at the time was so concerned about it because there was a lot of research that suggested the harmful impacts on children. And we see more and more evidence that industry is experimenting with cognitive and behavioral insights, taking advantage of children. There has been some evidence from Facebook, for example, that has been experimenting with allowing advertisers to target vulnerable teenagers at moments when they feel worthless and insecure.

I for one, as a mother of an 11-year-old, I'm particularly alarmed about that. We don't really know where the long term impacts are of these kind of practices. And we really should think about it as really the precautionary principle not doing harm.

We should spend a lot more time in research and looking into this. I think in Congress, there's proposals to do more research into this space. And we would encourage the FTC also with its authority to really understand the impact of these practices on children.

MARK EICHORN: And anyone else?

JAMES COOPER: Sure, I will jump in. And it may be surprising that I have a slightly different view than Katharina. But those who know me chuckle.

I agree that the issue here, the surveillance issues that are facing everyone are the same that are facing kids. And I think we should start-- it seems that there are two types of harm that

COPPA seems to be targeted at, at least in some ways. And one is the actual just advertising to kids, which I think is a different animal. And maybe we can talk about that more because I think that's quite different.

But I want to think about it more as the privacy aspect. There's surveillance. I don't think as policymakers we should be able to just say, well, privacy and kids and then be done. I think we do need to think in the same way that we think about surveillance and online and privacy issues in the grown up world the same way with kids.

And what is the harm that we're talking about? What is the injury? Because, as we'll talk about later, there are potentially costs to restricting persistent identifiers.

As far as I know, there's not a lot of evidence as far as privacy preferences for children. All of the data, the empirical work that I'm familiar with, it deals with adults. If you look at whether it's the experimental evidence or if you look at field experiments, the [INAUDIBLE] revealed preference, there are a few studies that seem to all suggest the willingness to pay for privacy is relatively small.

That's again, grown ups. Now there are informational issues, there are behavioral cognitive biases. There are some studies that try to control for all of that, and at the end of the day, seems to be what's out there. And this is a conclusion.

There's a survey article by [INAUDIBLE], Taylor, and [? Wagman ?] on the economics of privacy. And they conclude, if you look at the data, that it's pretty clear that consumers seem to be more engaged in privacy reducing activities than privacy protecting activities. And that there's a very small willingness to pay for privacy.

Now we can debate over-- again, there are flaws in each of those studies, or in some of the studies. But I think the takeaway there-- and then especially when you look at what we're talking about here as far as persistent identifiers to target ads, that's usually ranks even in survey, which is stated preference is a relatively low level concern compared to other types of privacy. It certainly does concern people, the creepy feeling of being tracked around the web. But again, it's usually not the top level concern.

When you think about what are the harms that we're trying to address, that's the grown up world. Again, there isn't any the data. And I could imagine kids are more vulnerable.

And if the profiles that are put together on kids were similar to the ones that were put together in adults, which would include other PII, such as name and address, all the gender, all the sort of profile information-- but if we assume that say a company is an operator or a website is COPPA compliant in every other aspect-- and if we go back before persistent identifiers were called PII, if you're COPPA compliant in every other aspect and all you're doing is putting a cookie, a persistent identifier, or other type of persistent identifier on a device, it's unclear whether the type of surveillance would be the same. Because you're not going to be able to link it up with all the other types of information.

It's clear that when you have a Google account, Google knows a lot about you because you've signed up for that account. If you're a kid and everything else is COPPA compliant, the persistent identifier won't be linked up with those other things. So I think we have to think about what is the harm that-- going back to 2013-- what is the harm the persistent identifiers are trying to address from a privacy standpoint? What is the privacy harm? And does it rise to the level that we're willing to impose the costs that, again, we'll talk about?

I think in some ways it comes back-- putting on more of a lawyer hat and less of an economist hat-- to think about the debate that went on when the COPPA rules route, and thinking about what does contact a kid mean? You can't collect PII if something can be used to contact a kid. And is a behavioral ad contacting a kid?

I thought it was wrong then, I still think it's a wrong interpretation now. And I think as you go back to the drawing board, maybe that's something to reconsider. So anyway, I'll leave it at that for now.

KATE O'LAUGHLIN: James, I'd like to disagree a little bit with the idea that collecting a persistent identifier on a single website cannot be connected back to other bits of PII which are more sensitive. It's one of the big differences between what the environment was like, the ecosystem was like in 2010 and 2011 to what it is today.

The invention in the adult side of advertising technology has really leapfrogged in terms of the ways that a single person can be identified and re-identified, in their data connected together. Back in 2011, there weren't things called customer data platforms, customer management platforms, data management platforms, which are all places in which disparate pieces of information that seem innocuous alone are now combined together. And they are prolifically used across all content monetization platforms and across all advertisers.

So even though it might seem a bit innocuous to drop a cookie on a kid when they're on a single website or from a single advertisement, do know that there are many, many systems out in the ecosystem that can connect that cookie back to precise geolocation, or can connect that back to a user screen name, that then can be connected to people's preferences.

JAMES COOPER: I was going to say, otherwise COPPA compliant. User screen name and geolocation would not be COPPA compliant if those had already been collected. So if you're otherwise COPPA compliant but for the cookie, that's what I-- I will grant you, I don't know the tech space the way that you and Jonathan do, so that's what I was saying. So I think if you add either one of those pieces of a kid, it would have been non-COPPA compliant unless there was parental consent.

KATE O'LAUGHLIN: I think my point is that a single site or a single advertisement might think that they are innocuously just setting a single browser. But when they connect it to a third party or they let that be used in some kind of internal operations allowed environment, that that is going to be prolifically sent out to a hop, and another hop, and to another hop, to another company that can connect it back to something more sensitive. And what we've seen since 2011, 2012, that some of the mechanisms that we've tried to put in place to prevent that downstream or upstream connection haven't really worked. So some of the flagging mechanisms that are used in the advertising technology space, the things that we're hoping to send out as signals that this piece of data shouldn't be used in connection with anything else, haven't yet worked.

So as we look forward, we need to make sure that we understand that these systems are already in place and very widely used. And we have to make sure that we don't introduce additional exemptions that let them be exercised with even more collection and connection together.

HARRY JHO: I have a question. Do we know if that data actually is being used to target not children generally but presumably let's say children under the age of eight? Are they using that level of targeting in order to present ads to children under the age of five, for example?

KATE O'LAUGHLIN: I don't think you would find anyone who would that would raise their hand and say we are using it.

HARRY JHO: Just from a common sense perspective, there's so many ways to otherwise target children of that age. And if you are, for example, marketing junk food, you don't necessarily need to go to those links to provide that, to deliver an ad. So again, I personally don't know. I do not run an operator. But I wonder as we think through this and the FTC is doing its research, if that's

something that we should be looking at.

KATE O'LAUGHLIN: Yes. Sorry, I'll just jump in here one more time. Yes, it is possible to advertise to kids without it being data driven without using personal information for the good, not just the bad example of using an unhealthy food. And I think that earlier today, that was one of those frustrating things to be sitting in the audience and hearing is that if we don't let data be part of the equation then the entire kid's ecosystem is going to collapse on itself because data is the only way to make money.

That is not true. There is safe and effective advertising that can help great kids content creators monetize that do not have to be data driven. We do that, we see that every day in our technology. We are proactively stripping out data so that we can have safe ads, we can have safe engagements with kids. And it works phenomenally well.

The big kids brands, they want to talk to kids and they want to do that safely. And it can work data free.

JULIA TAMA: I think maybe that brings us back to the question of the pros and cons. And if I could jump in on the pros at the moment, I think that this is something that the COPPA role today actually recognizes. Persistent identifiers are defined as personal information. But there is also this important exception that's been mentioned about support for internal operations. And that exception is the piece that makes it workable to have persistent identifiers as part of the rule.

Because if we're talking about the pros, a lot of those are recognized in the exception. Persistent identifiers are absolutely necessary for a lot of functions in online services and websites today that make them interesting and engaging for kids. And the exception sees that. And the exception also recognizes, I think, that persistent identifiers are a bit different from the other types of personal information that are listed in the COPPA rule.

Persistent identifiers do have these beneficial uses. Other data also has beneficial uses, but persistent identifiers are allowed to be used for certain purposes without parental consent because of those beneficial uses. I think there are a lot of pros, and I actually think it's very helpful that the COPPA rule is recognizing those today.

And I think that it's essential to maintain that exception and to continue to work towards improving it and keeping it as clear and as comprehensive as possible so that it can continue to be used. And it really is for the benefit of kids to make sure that there can be engaging and

interesting online content for them.

LAURA HOSKIN: Julia, have you seen an increase in benefits over time since the previous rule review? Has this gotten more useful for internal purposes over time, or is it just the same? Do you see that?

JULIA TAMA: I'm sorry. Are you saying that persistent identifiers have become more useful over time--

[INTERPOSING VOICES]

LAURA HOSKIN: For internal purposes, yeah. For designing apps? Or maybe it's not something you've thought of.

JULIA TAMA: No. It's a little bit hard to answer. I think over time-- I think what is listed now is probably the minimum of what should be listed of support for internal operations. The challenges that I see as a practitioner are that there's still uncertainty. So there are services or functions that companies might like to use persistent identifiers for which are not behavioral advertising and are not profiling.

But if the rule is uncertain, companies are very risk averse. And so there is a chilling effect where the exception is not clear.

MARK EICHORN: Katharina, I know you had wanted to weigh in, and then Harry.

KATHARINA KOPP: Sure. Thank you. So I think with regard to the internal operations exception, we believe that the definition is way too broad and vague. That it really creates incentives for operators to claim that persistent identifiers are used for internal purposes even if they're not.

So for example, the content personalization exception, we believe that sometimes content personalization is similar to personalized ads, especially when ads are-- of for example, content on YouTube are really ads. So if you have branded channels, for example, on YouTube. If a child clicks on that it or likes that, and then the personalization would basically repeat sending that content to the child. And that a really amounts to more advertising for the child to be consumed.

And I also think that content personalization, we're going to probably see much more of that. I think you've been involved in research on dark patterns in e-commerce websites. I think dark patterns, so this attempt to have the design architecture so that certain default decisions are made by website users. We're probably going to see much more of that being personalized.

And so there's forms of manipulation that's going to creep into so the children are making choices that they might give away more information or that they will be manipulated in certain behaviors.

So this exception for internal operations, I think you need definitions for that. We need to understand what companies are doing with this data. So again, I think a 6(b) authority would be good here to really understand how companies are using this information under the exception. We also have concerns, for example, around the use of this data for attribution and measurement purposes because that would facilitate advertising and marketing. And I think that's not the purpose and intent of COPPA.

KATE O'LAUGHLIN: I just want to jump in on that for a moment and say that I think we have to be disciplined about this conversation because there's a lot of concern, of course, at all times about what advertising or what content kids are seeing online. That's an important conversation to have. But I don't think that's a COPPA conversation. COPPA is about data collection from kids. And then we've introduced use restriction in the form of the support for internal operations exception. So I think we can speak about it there but I do not think we should try to make COPPA into the vehicle for all policy concerns that might relate to ad content or content online for kids.

MARK EICHORN: Harry had wanted to jump in.

HARRY JHO: I'm not an expert on COPPA. But to the extent that when I looked at say where we sit with the data that we have access to for our audience, we get data from YouTube. We have an app out there, a subscription app that we have data from Apple. And then we have data from our website.

Apple and Google do not provide us with really anything that's even remotely at a user level. But there is important data there about the geographic locations, for example. So for example, we have a large international audience. Knowing that we have a large Latin American audience led us to create a Spanish channel. We wouldn't have known to do that if we didn't have that data.

I'm sure cookie level data came into play. But by the time the data got to me it was aggregated only at the country level, which was really all the data that I needed. So one element here, I think, is who is looking at [INAUDIBLE] meaning? There is operator level data at Google's level, and then there's the data that we get.

Meaning on my website I might get more data, but I don't necessarily need to look at data to that degree of specificity. But it is essential for me to be able to provide content to have access to some information other than fan email of what we are and who our audience is. Similarly, with Apple, where we have a subscription app, I would say that just anecdotally, going to the issue of harm, I would say the number one bit of feedback-- we go out of our way for our content to provide ad free experiences.

So yes, we're on YouTube. But we're also on pretty much all of the subscription video services. And we have a subscription app, which is ad free. And then we've removed all ads from our website.

And yet in spite of that, I would say the number one bit of feedback we get on our app is why can't we make it available for free? We don't really consider it an option. But I would say that our audience would probably want to have an opportunity to somehow opt into ads instead of paying the subscription fee.

As we think about how these identifiers are used, I wouldn't want the conversation to be about just one level of operator or that the audience for the data would just be only advertisers. But rather, there's many different audiences, and not all of them have to get that data. I would never want to have or would never need to have user level data on anyone.

We have millions of fans and that would just be not useful for us. And I think most people wouldn't have an interest in that. But certainly, we would need to have data. Going to one of the earlier panels, we worked, when we developed our app, with one of the app companies, Touch Press. And many of the other companies listed on that slide are no longer creating content for kids.

One of them was acquired. The other one went out of business. And that was the cream of the crop for content in the app space.

So when you look at the preschool app market, that is absolutely a market where you're seeing negative impact as a result of being able to have monetization options. The result then is that we all know that people have continued to stay on these devices. So they are now using apps and engaging with content that is less thoughtful, not created by people who are even aware of COPPA, et cetera.

MARK EICHORN: Jonathan, I know you had your hand up.

JONATHAN MAYER: Thanks. I guess I had to respond to a few points that have come out from a technical perspective. The first one being, why should we care about these identifiers in the first place? And I think often the conversation tangles the use of information with the collection of information. And those are related but distinct issues.

You might be concerned about behavioral advertising to kids. Or, not mutually exclusive or, you might be concerned about third party entities collecting information about what kids do online. The rule could get at one of those or the other or both of them. I think as currently drafted, it gets it both. As for why you might think it's not cool to have a company you've never heard of collecting your kids activities online, I'll maybe leave that to others to talk about.

The second point I want to address is this monetization issue and whether you can monetize an app if you need verifiable parental consent to do behavioral advertising. Or I should say, we don't accommodate quite a bit of-- I'm sorry. I should say, advertising with an identifier, third party advertising. And as a technical matter, there are a bunch of other directions you could go.

So there are other types of advertising outside of behavioral advertising. Some of it mentioned today. Demographic advertising, that's we think we know something about this kind of person at a very high level but not specific to the person.

So people who are playing in an app that is designed let's say for little boys or little girls. You might target based on that demographic information without knowing something about the specific user. You could have geographic targeting. Not precise geographic targeting based on GPS, but this user seems like they're in Washington, DC, so we'll advertise a kids club in Washington, DC.

Or you could have contextual advertising. So the kids in an app where you're at the dentist's office and there's some app related to some fun toothbrush. I don't know. The point being it could be based on context. So there are a bunch of different ways of targeting.

There a bunch of different ways of delivering ads. So instead of using identifier you could imagine an ad delivery that's stateless or that's uses some state stored in the device rather than using a unique identifier. You could use a session identifier, or a short-lived identifier. You could use first party identifiers that are persistent but not persistent third party identifiers. So

there's an entire spectrum of designs short of sharing persistent identifiers with third parties for all advertising.

And at the risk of putting too fine a point on it, Apple has effectively banned third party advertising that uses a persistent identifier in the app store. And clearly, the app store is doing fine in terms of having children's apps. The claim that an exception for that type of advertising is essential seems a little bit belied by the Apple experience.

The last point I want to make, and I recognize that I've been talking for a bit here, relates to this internal operations exception. The exception conflates a few things that might be going on. One is to say we're concerned about behavioral advertising so we're going to cover behavioral advertising then use the internal operations exception to exclude everything that's not behavioral advertising. So the only persistent identifier stuff we're trying to cover is behavioral advertising.

I don't think that's what the rule's trying to do. But that could be a direction some folks either want to go or conceive of it as. Another is the bare minimum for the app to function. And that is network level information. You have to be able to collect IP addresses in conjunction with the app loading otherwise the app can't load anything.

And then you've got this broad middle of stuff where I believe the term used in the last rulemaking is smoothing the internet experience, or something like that right. Where as a sort of accommodation to the ecosystem we're going to allow identifier-based contextual advertising, other forms of advertising, frequency capping, et cetera. And there I think is where the hard policy questions is. And I think it's a little bit of a misnomer to call it internal operations. Again, I think it's a concession to allow the ecosystem to run and query whether that form of concession is technically needed at this point.

MARK EICHORN: I believe Kate wanted to step in and then maybe we can change the discussion just a little bit.

KATE O'LAUGHLIN: Yeah, sure. The techniques that Jonathan described for delivering advertising without data are all right on. And what we see practically is that the ecosystem can thrive using those techniques. Those same techniques and those same paradigms can be also applied in measurement.

Some of the internal operations expansion ideas have been maybe around attribution. If you're not familiar with the term "attribution," it's connecting whether an ad drove to something

being sold. I think it seems a bit innocuous. And it is important to marketers. It might be one of these places where concessions, you might have a lot of pressure to concede. But let's remember that what is attribution or what is marketing measurement to some of the most active brands in the ecosystem might get us too close to data that we really think is sensitive.

If you think about Target, or Walmart, or Chuck E Cheese, what matters to them and measuring whether or not advertising works is did someone actually walk into a store. And so if we extend some of these internal operations to include attribution as a use case and measurement, we again are getting into this territory where we're connecting a bunch of data together that gets even more sensitive. And we can accomplish measurement, we can accomplish marketing effectiveness measurement, which is ultimately the job that many marketers want us to do, by using some of the same techniques that Jonathan described on the targeting side of advertising.

JAMES COOPER: I just wanted to jump in and just say something. We can look and say that advertising ecosystems-- or I'm sorry, app ecosystems are thriving, but what we don't have is the "but for a world." We're looking at it and I agree, you look at the app store and there's absolutely no dearth of children's apps.

Just from a good empirical standpoint, just to look at something and say there's a lot so there's no impact, I think there's clearly an impact. First, there's [INAUDIBLE] anecdotal. Harry talks about going behind a paywall. So that's one thing.

We know if you go behind a paywall versus ads or have a freemium type view, demand curve slopes downwards. So you raise the price, fewer people consume. That's just going to happen.

The second thing is the data, the empirical evidence is pretty clear that behavioral or interest rate stats, or whatever you want to call them, they do garner more revenue for the content creators. In fact, Garrett Johnson at Boston University, Catherine Tucker and Avi Goldfarb, they were actually down here last fall as part of the competition and consumer protection hearings. We had a whole thing about that.

There's somewhere between 2x and 5x, maybe 10x for the revenue. Now there is some evidence to suggest that maybe that's overpriced, that their effectiveness isn't what they are. But just as far as the revenue that's generated-- and in fact, all you have to do is read the commission statement in the YouTube case and look at the YouTube statement after that.

Knowing that it's going to harm-- talking one about how YouTube profited off of these ads. And then YouTube saying, look, we know this is going to be tough for some content creators.

So it is going to say that what would be good-- and maybe this is something we'll talk about later because I know we are going to talk about what the next steps, what are some researching to actually see what the impact of the 2013 rule was on kid's content. Again, we can look at it and say it's fine. I have kids and I think they have plenty of apps, probably too many.

But just from a good science perspective, to see have there been an impact? And the impact can be not just some disappeared, some may go behind a paywall. There's also content.

There's a good, very recent paper in the *RAND Journal of Economics.* Joel [INAUDIBLE] and a couple co-authors, and I apologize to the other two co-authors for forgetting their names. It's not exactly on point, but it's about ad blockers. And they find that for every percentage of your audience that has an ad blocker, your revenue goes down by about 1%. And then also, when you look at the sites with the heaviest ad blocker traffic, they have less content.

I think there is likely to be some impact. And again, maybe the world's fine. But I think that we can't just look at it and say that there is enough out there. And there are lots of ways you can monetize. But you are changing behavior.

And I'm not saying, again, and I just want to say, this is just something that needs to be weighed. Maybe this is the right equilibrium. Maybe there is a market failure. Maybe we need government intervention here. Maybe COPPA's the right balance. But we can't just look at the Apple App Store and say there are lots of kids apps so it's fine.

HARRY JHO: If I could, I would just want to quickly say, you can actually tell, at least in the preschool space, you can see the vision of the future of content where say five, six, seven years ago you had many independent companies developing content. So for example, when my kids were really young they played Toca Boca's apps. They loved them.

Now what you're seeing is the developers are focusing on brands that are basically using the apps really just to promote megabrands, so the Disney apps, the Lego apps. But those independent apps are pretty much largely disappeared, unless basically, there's a large group of we'll call it almost disposable apps are being cheaply generated at that scale.

But that very thoughtful, independent creator based in the app store has largely disappeared. And more likely than not, you might see something similar happen to YouTube. So there is actually impact. There's meaningful impact and will affect choice.

LAURA HOSKIN: So I think you guys got through several of our questions without seeing them.

[LAUGHTER]

KATHARINA KOPP: Can I just jump in here one second? Just in terms of framing, I think it's been bothering me a little bit this morning already. I think we're not here to do a balancing act. COPPA had an intent to protect children, to limit the contacting of children, to limiting the marketing to children because they are vulnerable.

There's a lot of research out there why would we care [INAUDIBLE]. As a society, we've decided we care about that. So we should not sit here now and decide what's the negative impact to businesses, and how do we trade this off against children. I think the priority is that we want to protect children. And that's why we have COPPA. So I think there are other times when I think it's appropriate to consider what the trade offs are, but not in this particular case.

KATE O'LAUGHLIN: I don't think it's businesses or children. I think it's businesses and children. Businesses are out there wanting to offer high quality content to kids, businesses of all sizes, as we've heard.

I'm a parent and I think we want kids to have online content. I think we want them to have access to this tool, the internet, that is going to shape so much of their lives. And the question is, how do we do that responsibly?

And just to tie that back to one particular aspect of the COPPA rule because it's just come up a lot, there a limited options for monetization to support publishers who want to offer that content to kids. And contextual advertising is a really important one that is recognized in the current COPPA rule. And so I would just say that one way to support businesses and children is to continue to recognize that exception for contextual advertising, including the activities that come with contextual advertising. I would certainly include ad attribution in there. And I'm sure there will be other ideas in the public comments in terms of things that should be considered part of meaningful contextual advertising that can support an app or services for kids.

LAURA HOSKIN: To that point-- I'm just going to interject right here. I'm sure you guys could take care of it. There is an open question as to whether or not behavioral advertising brings in significantly more revenue than contextual. I just wanted to hear from everybody what their experience

with this is. If you have no idea you can just say I've no idea. That's perfectly reasonable. James, you've already answered this question. So sorry.

JAMES COOPER: I won't talk.

LAURA HOSKIN: I'll start with Harry.

HARRY JHO: Sure. I would say, currently we get advertising from or revenue from quite a large number of sources. But I would say that behavioral advertising on YouTube constitutes the lion's share of our revenue. I would say the loss of it will require us and every other YouTuber in a similar position to dramatically change their entire business model, which we're in the process of doing.

KATHARINA KOPP: So I think the questions that were raised around this issue, also with the research [INAUDIBLE] Professor Christie, I think only points to the fact that we need more transparency around this and what the role of the platforms are in determining price around that. Again, I think 6(b) authority is called for here to look into that, what the really behind the scenes information is.

JONATHAN MAYER: I agree with the call for ideally the commission to do the work of its own. And certainly would encourage more work in this area. It's an area of research I've wanted to get into. It's essentially not possible because the entities that have the data are generally not really overly enthusiastic about collaborating with privacy researchers.

The work that has been done to date, I think, in many instances has some serious methodological issues. And I say that about the work that finds that behavior advertising is quite valuable. And the work that finds behavioral advertising is not so valuable. And so I genuinely do think we just need more research. And it is a little crazy that we're a couple decades into behavioral advertising driving much of the online economy and privacy conversation and we're really not super sure just how important or actually how necessary this stuff is. It's a little weird.

KATE O'LAUGHLIN: Our experience is that safe kids advertising commands equal prices that advertising to adults that's very data driven does. We don't see a gigantic discount to contextual advertising. And then when it comes to the changes that is going to be incurred for monetization by content creators with YouTube changes, I would just say, let's not muddle turning off data driven advertising with some of the more structural changes that they're making to declare kids content.

When they turn off comments and they turn off engagements, that's affecting their algorithm and how users are going to find that content. That's one part of the expected decrease in monetization, which is separate from just turning off the data in the targeting. So let's not conflate decrease in prices or decrease in revenue to kids content creators on YouTube just because the data is turned off.

HARRY JHO: Agree.

MARK EICHORN: Julia.

LAURA HOSKIN: Julia

JULIA TAMA: It's my understanding that there are plenty of studies showing that interest based advertising is more supported for publishers than contextual. I certainly think we can always have more research. It's a data driven industry. We can have more research on it. Certainly, that would be welcome.

But I do believe that there are plenty of studies showing that the results for publishers are better with the interest based advertising. And I think that's what I hear anecdotally. Of course, under the new COPPA rule, there's been a shift in that in the past six years. So that was more from the time that the rule came out that we were hearing those concerns.

MARK EICHORN: So I'll ask a question from the audience. It gives me an opportunity to address something I've heard earlier today, as well. So the question is, as Commissioner Phillips noted, looking at the intent of Congress, COPPA was about addressing contacting of kids. Does a persistent identifier alone allow contacting of a child, assuming it's not combined with other types of information?

So I just wanted to take this opportunity too, since we're talking about the intent of Congress. People have talked about the intent earlier in the panels, and basically talked about the online safety aspect of congressional intent. But when you look back at the FTC report that led to it and I think to the statute and the original rule itself, I think that it's clear that there's a couple of purposes. And one was online safety.

But I think the other purpose was to basically restore parents to the role that they used to have back in the day where the parent would be home. And if you wanted to reach the kid, you would be calling and probably the parent would be picking up the phone. Or you'd be sending

some mail that the parent would be reviewing.

From the legislative history, that was from Senator Bryan. And I think he was speaking for himself and Senator McCain. He spoke to this issue a little bit. He talks about the information being collected.

And then at some point he says, "Much of this information appears to be harmless. But companies are attempting to build a wealth of information about you and your family without an adult's approval, a profile that will enable them to target and to entice your children to purchase a range of products. The internet gives marketers the capability of interacting with your children and developing a relationship without your knowledge.

Where can this interactive relationship go? Will your child be receiving birthday cards and communications with online cartoon characters for particular products?" So that's just an excerpt. But it gives you a flavor. Online safety was just part of what they were after.

But anyway, I provide that as background. But the question is, going again to does the persistent identifier alone allow the contacting of a child? I think James is--

JAMES COOPER: Again, I think I've already answered that. I just think, I mean, you're right. And I actually reread the legislative history as well. And you're right. I think that there is this conventional wisdom that COPPA is about protecting kids from predators and that sort of thing.

But you're right. It's clearly in the germ of COPPA was also advertising and marketing to kids. But I still think if you just look at the statute-- and the statute says, [INAUDIBLE] under PII it could be any other-- and I don't know it verbatim-- but any other thing that can help contact-- I don't know if it says specifically contact a child.

I still think that it's a-- I agree. And again, this was all in the comments. You guys went through this and you've worked through 2011 or '10 through '13 or '12. And that view did not carry the day.

But I still think that it's a stretch of the statutory language because to say that a advertisement is contact. An identifier that allows you to send an advertisement is the same type of contact as the other things that are specifically in there, the email, address, phone number, name, birth date, those sort of things. So I would say just as a matter of statutory interpretation, I think it's a little bit of a little bit of a stretch.

But again, if you want to go back and rethink that-- in fact, recent case on net neutrality said it's OK. You can go back and rethink your rules just because you think you got it wrong the first time.

MARK EICHORN: The original definition that James is referring to for persistent identifier was "Any other identifier that the commission determines permits the physical or online contacting of a specific individual." Did anybody else have any thoughts on this? Jonathan.

JONATHAN MAYER: So let me just just quickly give-- again, I'm going to try to stick to the computer science here. So I'm not going to talk about Chevron deference. But from a computer science perspective, an identifier is how you contact people or devices online.

Ultimately, it's the reference to, again, whatever person or device you're trying to talk to. And then you resolve it through some underlying protocol. For email we have a suite of protocols like SMTP, and so on. For phone numbers there's all sorts of protocols like SS7. For a cookie we use HTTP.

But ultimately, these are just always a placing something in front of a person or getting some information to a person. And again, from a computer science perspective, I don't see any difference between these communication technologies with respect to whether one is enabling contact or another.

MARK EICHORN: Julia.

JULIA TAMA: From a practitioner's perspective, there's a very significant difference. And I think we see it. We've heard some of this earlier. Persistent identifiers are being added to more laws as a type of personal information. And it creates a tremendous amount of mischief for companies.

It's extremely difficult. It's very easy to say, it's an identifier like any other. But the fact is, it's a different type of identifier. It's a identifier that does not allow me to pick up the phone and call a child and speak to them in real life. It is an identifier that doesn't give the same ability to go back and engage in some of the activities that some of the new laws are calling for, like access, et cetera.

So it's just important to realize that persistent identifiers are categorized as personal information today under the COPPA rule. But they remain fundamentally different from the other types of things that are listed as personal information. And that exception on support for internal operations, that's why it's so critical and essential for it to remain in place is to

recognize that difference. It's what makes it workable to even have persistent identifiers in there.

And I would agree with the comments that I do think it's a stretch to have persistent identifiers in there. I don't think they allow contacting in the same way as the other items in the list of personal information. But if they were to be left in the COPPA rule, the exception is essential, and it needs to not only continue to stay there but continue to be improved and to offer more clarity and more certainty for the companies that are really relying on it.

LAURA HOSKIN: So we have another question from the audience. Most monetization concerns mentioned today are centered around advertising. What does COPPA have to say about paid subscription apps for businesses? Harry. You're the paid subscription guy.

HARRY JHO: Right. With our app, we use the service to make sure it was COPPA compliant. The irony there is-- and we actually have no direct relationship with our users. They subscribe through Apple Service, so they are completely invisible to us.

I would say that from that perspective, one of the issues that does come up is-- and it's been alluded to-- from a product design standpoint, you do want to consider if the original purpose of COPPA was to prevent that level of you don't want people to call people up in their homes, should it also prevent me from allowing them to have a playlist? I would say, nearly all of the product services that people would want are services that would require a certain amount of customization to their use. But for us, we'd either have to do it for everyone or not at all. And so the answer ends up becoming not at all.

In the digital ecosystem of today, the fact of the matter is that the users have been so conditioned to not paying for content that a subscription app is really almost something that-- we invested a lot of time and effort in it almost as a loss leader, I would say as a matter of principle. It's not a major driver of revenue for us. Almost all the major drivers of revenue for us are advertising based.

And that is because that's what the audience wants and demands. And I would say that we've heard the word, "equity" today. For most of our audience, they would consider that a very serious issue of equity. If I told them that the only way to consume our content was for you to sign up to a subscription service, I think most of our fans would consider that to be very offensive and outrageous.

I don't personally support tracking kids to that level of detail. I think that a certain level of specificity, from where I see it, why would you need to get beyond a certain point of information? But if the information is anonymized to certain point, why shouldn't you be able to use it to provide a better experience? Why shouldn't you be able to use it to also support ads if the advertiser and the users want that? It's the only way I can quite frankly afford a robust content environment to exist. Otherwise we would ironically end up in a situation where, thanks to regulation, you'd be creating content monopolies where only the biggest billion dollar content providers could deliver content to this audience.

LAURA HOSKIN: You want to comment?

JONATHAN MAYER: So I guess a point that occurs to me in response is I think everyone wants there to be free, awesome content available for kids. That's a lot of promise here. And one of the directions that strikes me as potentially promising and that I hope the commission will take the opportunity to explore, is addressing this issue of age gating and parental consent and oversight via platforms. So I think one of the issues we have now is if you want to be a content creator or a developer, the model is that the burden is heaped on you to figure out the age gate, to figure out the parental consent, et cetera.

And you could imagine a world in which platforms, especially as the data show, kids are overwhelmingly moving towards a small number of mobile platforms and they're using tablets on those platforms. If those platforms did a good job of implementing age flagging, age gating, parental consent, et cetera, it might take a lot of the strain off of app developers and content creators--

[INTERPOSING VOICES]

HARRY JHO: Yeah, absolutely. Yeah. I think there's a way that we're talking about data where there's just one pool of data and there's one group of people that want to use that data. That's not actually true. There is a wide range of data. There's many different constituencies that want access to some of that data.

I would say, I struggle to think of anyone who actually wants to get to that level of specificity for children. And certainly, we shouldn't allow anyone to get so much individualized data that they could actually call someone up in their home. But at the same time, between that and being able to give anonymized data to certain classes of people and allow them to support advertising, allow them to support app development, I don't really see a public policy interest

that's addressed there.

It's totally anonymized. It may not even be from people in this country. Especially if we're talking about YouTube or the App Store. There seems to be a wide middle that we can bridge as we look into this. I would just urge that as we do the research we do it somewhat quickly because starting Jan 1, a lot of us might not be around.

MARK EICHORN: Can I ask-- changing the conversation just a bit-- one objective to online advertising-- we've heard about it earlier today, as well-- is that really an objection to the content of the ads themselves or to the products advertised. I remember a few years back, there was erectile dysfunction ads appearing on the Super Bowl. There was a lot of talk about that-- or generally on football.

Is there any connection between that and-- if I'm a kids' site and I say, you can't do OBA on my site. Is there any connection between that and appropriateness of ads. Either am I more likely to get ads that are appropriate for kids or am I less likely to get ads that are appropriate for kids? Or is it no relationship there?

KATE O'LAUGHLIN: I think that it should be every person or every company in the ecosystem than the ad delivery chain's responsibility to make sure that a flag telling you that this is a kid should mean not just don't use or collect data here but also make sure that this experience is appropriate. What is the kid hearing, seeing, feeling should abide by the guidelines set up by the self-regulatory organizations. And that should just be part of the expectation.

HARRY JHO: Right. And part of that would require us to know that it's kid's content and that their kids watching it in order for those protections to work.

KATHARINA KOPP: The problem with behavioral advertising is not that it delivers inappropriate content. We've been over this. But the fact that it aims to manipulate children and influence them in inappropriate ways, that's what to ask the objection is. And I think the problem with inappropriate content, I think there's much more brand safety issues awareness around this. And there's many more solutions from a different angle to look at that would be prevented. But that's not connected to [INAUDIBLE] behavioral advertising.

HARRY JHO: I would just want to jump in there a little bit more to really go to the-- that's really almost an editorial question. What do we want our children to watch in terms of ad content? Which then also somewhat I think relates to what do we want our children to watch in terms of the content

itself?

The approach that we seem to be taking here is to regulate that editorial decision through the privacy angle. My personal view is that we should address that and we should address issues of curation. But we should do that head on and not necessarily just through privacy, but rather through a direct discussion of the question.

JONATHAN MAYER: I just wanted to echo what Harry said a little bit. We began this discussion talking about the privacy harms and the privacy aspect of COPPA, which I think COPPA is mostly about. But when you think about the ad side, I worry about undervaluing the information flows to kids.

Just to say, well, they're advertising to kids, we need to stop it all. Experience from my life, my world was changed when I was watching an ad and I saw Cookie Crisp. I'm like, wow, they're cookies, you can have cookies for cereal for breakfast. It was a game changer.

But the point there is, if my parents would have seen that we never would have had Cookie Crisp. That's all I wanted to say. No. I'm paid for by Cookie Crisp.

I would not want to say, oh, you're under 13 so the decisions-- again, we're getting more into the realm of bigger picture policy of who should have control over what you're-- is this a parental issue-- but to devalue the information that flows to kids and say it's just completely valueless.

The Supreme Court in Brown vs. the video game case-- I can't remember--

HARRY JHO: Entertainment Software Systems.

JAMES COOPER: Yeah, OK, yeah. A couple years ago. They said that, look, the kids, except for obscenity-- and obscenity is usually defined in pornographic terms or sexual-- that the information flows to them, that kids shouldn't deserve any less First Amendment protection than grownups. That they're a vulnerable population but they shouldn't deserve any--

So I think that we need to be careful. And again, we're getting far afield from where COPPA is IN the privacy issues. But once we start thinking about using COPPA as a tool to restrict advertising to kids then I do think we're getting into First Amendment land. We should think about, is COPPA the right tool for that?

And we've had this debate. Again, we're at the FTC, which is the best place in the world to be

to talk about restricting advertisements to kids. There's a rich history here, not a good one. Eventually turned to a happy ending, I think.

I was here at the commission in the early- to mid-2000s when there was a big push to do something with advertising for kids for obesity reasons, again. And that was resisted a lot. And I know that there's research to suggest that kids don't get advertising, so everything's inherently deceptive. So that gets you out of the First Amendment. As far as I know, no court has adopted that.

The point being is that I don't think we should just give short shrift to information flows to kids and say that it's OK to have a rule that restricts information to kids. That's on the cost side. So when we have less valuable ads going to children, meaning-- and I don't mean just the monetization-- the reason that they make more money for the publisher or the content providers is because they're more likely to lead to action.

To the extent that kids are seeing fewer Cookie Crisp ads, or things that they really could act on-- and again, their parent is typically going to be the gatekeeper to this. This is something that should be valued. It shouldn't just be given short shrift.

MARK EICHORN: Thank you, James. Can I turn to one last question from the audience? I think we just have a few minutes left here.

But the question is about persistent IDs. And it says, "Persistent IDs may be part of a child directed site app but maybe on the device of the parent. So there may be multiple people using a shared device," and how to address these types of identifiers. And at the same time, I wanted to bring in both Jonathan and his presentation.

And Dr. Radesky had mentioned that more and more kids now have their own device. Certainly it wasn't true when the rule was revised. So if you can meld those two together. Any thoughts welcome.

JONATHAN MAYER: Sure. So I see, again, trying to focus on the computer science perspective, a great opportunity here for the commission to maybe encourage a new direction that addresses a lot of the issues that have thus far come up in COPPA implementation around kids have their own tablets, or maybe when they share a tablet now. Android or-- I guess as of a month ago it's now called iPad OS-- so iPad OS have the ability to set up a profile specific to a child. Were the world to move towards the operating system, for example, telling an app-- and this is

technically trivial-- the user who's currently on the device has a profile that their parent has configured as a child. And if the user is using your app or sending some sort of persistent identifier via your platform, or so on, you should be COPPA compliant. And if you want to, in your exercise of editorial discretion, have child friendly advertising and so on, you could do that too.

I think that could get at a lot of the issues here. That of course, does not solve shared devices, shared profiles on devices. But I think, given that that seems to be where things are going, here's an opportunity to take advantage of the trend towards mobile devices and maybe solve some problems.

JULIA TAMA: My opinion is that keeping the conventions of child directed and actual knowledge is a cleaner way to recognize who is the kid instead of giving a more liberal look at who could be using a device. In practice, we often hear from an advertiser saying, well, we were trying to reach the family. The same of them winking at you and saying, well, can't we get around this by just saying mom's probably in the room somewhere. That's how they try to get around COPPA. So if we loosen this up and say, well, a shared device with a shared persistent identifier is allowable, I think that gets us further into the gray than relying on what is good and more clean-- we've talked about it already today-- that could be even more clear but child directed and actual knowledge.

LAURA HOSKIN: So I want to bring up a point that was made in a previous panel. How do you think these issues apply when you're talking about minorities and low income families? Is it going to be just as easy for them to hit that button and say, oh, this is my child's device? What sort of issues do you see surrounding vulnerable populations?

KATHARINA KOPP: So if I may jump in here. I think COPPA, when it was written, it was thought written in this tradition of privacy self-management, the idea that individuals make decisions. They are rational decision makers. If they have enough information they can make this decision.

And I think today we are much more aware, and we have growing evidence of the fact that predictive and classifying analytics really lead to a distribution of harms that look at groups of users, and that the distribution of harms is uneven, and that some people are more harmed than others, or groups of users, as particular people of color and low income. COPPA identified children as particularly vulnerable. But I think even within children we need to understand that there are different populations affected differently.

And again, this is an area I think we need much more research on. We know this from the adult population. We have had some great research from Facebook, and advertising in housing and employment, where an advertiser wanted to reach a diverse audience. It ended up creating disparate impact.

We think that, again, we mentioned the junk food marketing, but it could be problems the same in education and other sort of areas where we need to look at the disparate impact. And I think, again, this is something for the commission to look at in terms of 6(b) inquiry. Because we cannot always see which ads are delivered to which populations in the aggregate and where the disparate impact is.

We need to do a better job in representing these groups at this panel, in these conversations. If I look around the room at these panels, we're not doing a good job. We had one person this afternoon. And really, we are much more diverse.

And we have in this country a growing problem of discrimination and increasing inequality. And we need to figure out to what extent the practices that we're talking about today contribute to that inequality. And so we need to look at that.

HARRY JHO: On the issue of you have one device for a wide range of users, I would think that it would not be in our interests to disregard the signals coming from the child user. Because I think this is how the scenario where the erectile dysfunction addends up getting shown. It's hard to imagine now, but when we first got started on YouTube there was very little information regarding anything on YouTube.

It was the earliest days. We were one of the first channels. I uploaded my videos because I just wanted to email them to people. The concept of having a YouTube channel and publishing or developing on YouTube was in no one's imagination.

One of the reasons why we became active users of the platform was that in that environment where there's very little content on YouTube, for many of our videos, the sidebar thumbnail that was next to our videos when we first uploaded was a video about an exorcism. OK. So I was using YouTube to share our videos with potential partners. And they would open it up and you'd see this thumbnail of this picture of an exorcism on it. And it just annoyed me to no end. How could they possibly put this exorcism video against my video?

I had no one to complain to. I had no recourse. One of the things that we realized that the only

way we could get rid of it was by uploading more content in the hopes that one of our new uploads might replace that video. And it took us like-- and that's the only reason why I started to upload more content and start managing my channel.

Obviously, that would never happen today. But part of that is because they know that my content is kids content. If they didn't know my content was kids content, what would-- there are enough problems, as we know, with some of the algorithms. Yes, I think we do want to consider those signals to help protect the kids.

MARK EICHORN: Jonathan, did you have a comment? Just to be extra clear on the issue of shared devices, I guess the direction I encourage the commission to look at of potentially doing better with platforms enabling age gates, and VPC, and ongoing parental relationships would have to be alongside dealing with the reality we all know exists, that parents hand their kids their smartphones and their tablets. For some kids, that's going to be the primary way in which they engage with devices.

So absolutely, you're going to have to look at other signals in those circumstances. If someone installs an app that is clearly a child directed app, the fact that the profile is not marked as a child profile is one piece of information. But maybe if it's just so obviously a child app you can be confident that that's actually still going to be a child audience. Anyway, that is all to say there are issues that will exist alongside one another.

JULIA TAMA: And I think more options can always be helpful, but I do think the current legal standard that exists today encompasses a lot of this and should stay the same because it's been workable that you have actual knowledge, as Kate mentioned, either of the child's age, or you have child directed content. And I think that standard is important to continue maintaining because that has proved workable. And expanding it to require companies to guess or investigate more would really not be workable.

MARK EICHORN: Well, with that, I see our time has expired. I will ask for a quick hand for the panel. But then, if you all would stay here, I will just give some closing remarks quickly. But thank you all.

[APPLAUSE]

So this is a signal that the closing remarks will be short. But I just wanted to thank everyone for coming today, and for those of you viewing from the office or home. It's been a good day.

We still have our comment period open. I believe it closes October 23. So get those comments

in. We appreciate them and we read them and take them into account.

There's a lot of people who made this event possible today. First, I want to thank all of our panelists over the course of the day for some great presentations and for your time and expertise. I really appreciate it. We really appreciate it.

I want to thank our colleagues in the Office of Public Affairs for manning the Twitter, and handling our press release, and all the other work that they do; our colleagues in the Division of Consumer and Business Education, the honors paralegals, who helped out with comments and making sure everyone got in the door; our colleague in DPIP, Alex Iglesias; and legal interns Nomi Conway and Shannon Silvester; Our colleague Rob [? McGrewer; ?] the events planning team; and in DPIP, Jim Trilling, Peter McGee, Kristin Cohen; my boss Maneesha Mithal, Laura Hoskin. And that's it. So thank you all for coming today. And again, get those comments in. Thank you, very much.

[APPLAUSE]