critical for determining whether we have the evidentiary basis for proceeding with the rule making and whether we meet the legal requirements needed for crafting any particular type of rule.

So it's really difficult to overstate the importance of public participation in this process, as what we hear and learn as part of this process will be the basis for what we are able to do or not able to do. When we launched this rulemaking proceeding last month, we issued an ANPR, an Advance Notice of Proposed Rulemaking, which lays out scores of questions on which we are particularly eager to receive your feedback and input. Your comments can help us gain a deeper understanding of prevailing commercial surveillance and data security practices, and you can do this through sharing research or reporting that you've done or seen, but also through sharing your own personal experience and perspectives. Expertise comes in many forms, including through day to day experience living with a particular business practice, so please don't be shy about sharing your views. We are so encouraged by the significant amount of

All right.

Josephine Lui:

Thank you very much. Next slide, please. The Advance Notice of Proposed Rulemaking, or ANPR, was published in the Federal Register on August 22nd, 2022. This is just the beginning of the rulemaking process. The FTC is accepting public comments until October 21st. The entity will then analyze all of the public comments. If the Commission decides to move forward, the next step is the publication of a Notice of Proposed Rule Making. There will be several more opportunities for public participation if the Commission decides to proceed. Next slide, please.

62 comments on the ANPR have already been posted and more comments are coming in every day. Public comments are an important way for the FTC to hear directly from you and anyone else who would be affected by the potential rule. Everyone is welcome to comment. Individuals, workers, entrepreneurs, parents of youn

Commissioner Rebecca Slaughter:

Thank you, Josephine. I'm sorry, and I'm going to apologize in advance that it's not clear how stable my internet connection is, but I'm hopeful it'll hold up and I will t

Following that discussion, Rashida Richardson will moderate a panel on consumer advocate's perspectives. And now, Professor Sylvain.

Professor Olivier Sylvain:

Thank you very much, Commissioner Slaughter. It's a great pleasure to be here and grateful for your leadership in this area. My name's Olivier Sylvain, I'm a senior advisor to the Chair and I'm on detail at the Bureau of Consumer Protection. I will be moderating our first panel on industry perspectives, and I think at this point it'd be great to get the panelists up on the screen, their videos up on the screen. Oh, let me say quickly here as they are joining us, that we will not do full biographies for all of these impressive folks. Their biographies are long enough and would take up all the time that we have, or take a large chunk of it at least. I refer you to the event materials on the forum, the public forum on site where you can see their respective biographies.

We will be joined today in this first panel by Jason Kint, Chief Executive Officer at Digital Content Next, Marshall Erwin, the Chief Security Officer at Mozilla, Paul Martino, the Vice President and Senior Policy Counsel at the National Retail Foundation, and Rebecca Finlay, the Chief Executive Officer of Partnership on AI. Before we turn to our panelists, I will just set out basic rules for our discussion since we are limited in time. All the panelists will have an initial three minutes to say a word or two about the theme of today's forum, and we will then open up Q and A session among the panelists.

I've asked the panelists to speak as succinctly as possible on four general areas that I will ask about. They will have about two minutes to answer, and we will hopefully have a way to allow the panelists to engage each other in conversation after they've given some initial answers, but we will limit that in time. I've asked the panelists to limit their reactions to about a minute. My objective as a moderator is to not get in the way, but also to ensure that we equalize time across the panelists. Our plan is to finish at 3:30. I think we're a little ahead of time, which is amazing, so let's see how things go. We might want to leave time for the second panel too, given the earlier start, but let's just shoot for 3:30 for now.

I will also let you all know that I've asked moderators if they want to weigh in, that they will raise their hand, they'll use the digital hand and I will call on them accordingly. So there are four areas that I hope

ensaq-3(h)3(10(l)14t)6)4(tu9(513(rai)2r)12(-)easqti p00000912 0 612 792 reW*nBT/F2 11.04 Tf1 0 0 1 72.024 330.41 Tm0 g0

which again brings me to my number two. Many in the industry will claim that behavioral advertising is

there's some abuse and misuse and that it is possible to protect against it, what are the best practices that companies are employing?

Rebecca Finlay:

Yeah. Thanks very much. I'm happy to jump in there. I think there are many approaches underway, but I think the approach that has perhaps the most consensus that I'm aware of and that is also well-researched and widely deployed is the use of documentation and benchmarks across the AI or machine learning life cycle. This is work that's been underway at PAI for several years, but it's really a field that was pioneered by the early work of many well known AI researchers, including Doctors Gebru, Mitchell, Rossi, Varney, Wallach, Wortman Vaughan, many others. It really is a well-established field of learning.

The guiding principle behind this particular best practice is that the process of documentation can support the goal of transparency by prompting processes and critical thinking about the ethical implications of each step in the machine learning life cycle, and ensuring at the same time that important steps aren't skipped along the way. You can understand why this is particularly important for consumers and citizens when AI is deployed, for example, in high risk settings such as healthcare or hiring, where we've seen assumptions and biases being built into models in real world settings with adverse effects, particularly for underrepresented or marginalized groups. So, well-functioning internal organizational processes that support systemic documentation across each stage of the machine learning system and the data set creation and made important.

This can also be a foundation upon which companies build ethics review processes, external auditing measures and assurance and accountability efforts. This is not just about creating a checklist of characteristics or even potential sort of mathematical or technical models. This is really about creating management systems and processes that stretch right from the design, development and deployment of the machine learning system being considered. Part of that is thinking about what is the potential impact of that system and what are the appropriate accountability mechanisms that need to be in place.

Clearly, this is not trivial. This is something that an organization needs to take on with senior leadership. It needs to have all sorts of institutional support, but it really is a foundation upon which many other measures like privacy impact assessments and other efforts can sit to provide both that internal and external assurance transparency and actionable responsibility. So, we're continuing to work on this. We've got a set of open source resources online that are available, and really look forward to continuing to advance this work.

Olivier Sylvain:

To be clear, Rebecca, I hear you talking about internal documentation, but you're also talking about public facing documentation as well.

Rebecca Finlay:

That's correct. I think once the notion being that with this set of clearly documented sets of questions that are asked throughout the process, not only is the organization bringing an external perspective to the question of impact, but also allowing for measures like external auditability and future assurance with regard to those processes.

Olivier Sylvain:

Thank you. I don't see another hand up, but Marshall, I'd like to turn to you on this. Many people have known about Mozilla's work browser level. Clearly, you all have been thinking about this in the context

California, Colorado, and I think Connecticut. That's a single one click opt out to say I don't want any tracking across the board. That makes it really easy for the user to have a persistent opt out from having parties, that they're not intending to interact with, have access to their data and then use it for purposes that they didn't really want or intend to.

And so, I just highlight that global privacy control as a simple one click signal. In some cases, the user even installs a product and has it by default. It's all about aligning with the consumer's expectations, and I think that's a positive development.

Olivier Sylvain:

Thank you Jason. Paul, you're next, but I want to just float out there for maybe a followup when you all go through and the possibility of talking about best practices regards to retention and access of sensitive data. But let's hold that off, and maybe Paul, you were going to mention that anyway. Paul, go ahead.

Paul Martino:

Yeah. Thank you. I just wanted to followup on what Marshall and Jason said, and I'll cover just data security and privacy briefly. But as I mentioned in my opening, retailers' primary business objective is to establish and build long-term trusted relationships with their customers. So, they view data privacy and data security as critical to doing that. With data security, the industry has invested, I don't have the exact number, but hundreds of millions, let's say, in developing and establishing dependable business practices that mitigate the risk of data security breaches, whether those are from external threats or internal threats, and to also ensure that the only authorized users of consumer data are those permitted by their customers. But there isn't a one size fits all. If you think about the breadth of the retail industry, from the smallest mom-and-pops all the way up to the largest companies, that there isn't a one size fits all approach when it comes to standards.

I do think that what Marshall talked about in baselining things that you do for data security are exactly right. But in addition to those, I just mentioned a few specific practices that retailers employ. This won't

Paul Martino:

Well, I will go first. Thank you. I was only going to mention on the data retention. The word I had forgotten was ransomware, and backups are important to be able to not have to pay a ransom if your system somehow gets invaded and locked up. And so, that's just a best practice for that.

But let me answer your question about what the FTC could do short of a regulation. Well, look, the FTC has done a great job over many decades holding public for like this and doing public workshops and engaging and inviting the different perspectives from industry, academic, and public interest stakeholders. I think that informs the FTCs reports. I think that service where they flag an emerging issue rather than go right to regulations or enforcement and gathering views across all stakeholders and then preparing a report. I mean, this is something the FTC has done very well for many years, and I think that very much informs the process of whether or not a regulation is necessary or if industry is developing best practices to address emerging concerns.

So, I would say, start with that short of regulation. I mean, just mention if they do do a regulation though, I think there's some things that they should put in place to help guard against emerging data practices where there might not be clear answers for compliance. I think one tool they can use that has been used very effectively in the state privacy laws is a notice and choice mechanism. I'm sorry, I didn't say notice and choice. I meant to say a notice and cure mechanism. For example, if there's an emerging data practice evolving business model, and it isn't clear whether or not those harms are being addressed, the FTC providing a notice, like the California AG has done, in instances, and then giving businesses an opportunity to come into compliance within a certain period or cure that alleged defect.

It's very important, and the reason is, it creates a very good incentive for businesses and the FTC to actually engage in a dialogue to figure out the best way to come into compliance. If we presume that consumers are best protected when all businesses are complying with the rules and regulations, then I think driving compliance is a very important factor. Incentivizing businesses and the FTC to engage in conversations before a regulation, before an action could be very helpful. We think that was important mechanism was the notice and cure. Thank you.

Olivier Sylvain:

Thank you, Paul. Yeah, very helpful. Rebecca, can I bring you into this? I mean, I think this is suited to the sorts of things you were also describing. I mean, how do you build partnerships? How do you bring people along? This is part of the question, but really what can the commission do given the tools it has, including but really a question's not just about rule making right now, to get companies compliant, as Paul says?

Rebecca Finlay:

Yeah. Thanks very much. No surprise, based on what I was saying about PAI and the importance of consultation and convening cross sectorally, but I do think that public consultations such as this are very important in terms of incentivizing action and change, both in industry and more broadly with regard to, and particularly, in environments where we're dealing with new and fast moving technologies like AI. I do think, to come back to the point that I made previously, that there is an important piece about better understanding the international context within which this rule making will occur. Just one example I know that as part of the notice, there was an expression of interest regarding how to protect children and youth online, which is just a critically important question.

As you probably know, the UK has released a child code or children's code regarding age appropriate design. This happened last year. It's a statutory code. It sets out audible standards which apply to online or connected products or services that process personal data and are likely to be accessed by anyone

being used in that same exact context. It's not some other party that you are not choosing to interact with that is collecting that data or informing its algorithmic recommendations. The problem that sits there that I just need to continue to call out is that without heightened... This goes back to your second question. Without heightened limitations on massive companies where the user doesn't really have choice, is it truly consent? Do you truly provide consent if you're using a search engine? And then, also, you're providing consent for their ad business and their ad tech business?

Somehow, you have to have heightened limitations on companies that have dominance across browsers and operating systems and search engines, et cetera. Because the problem is the digital ad market, and I'll cut off here, unpacking all I know in here, the digital ad market is a little bit like a water balloon. If any individual actor via retail site or a publisher moves forward with higher level of standard, the advertising market will just shift to where they can find those users and target them. And so, everybody has to play by the same rules, and the rules have to be heightened for the companies that have dominance.

Olivier Sylvain:

Thanks, Jason. Marshall, I'm going to bring you in. The language you used in your opening remark was creating costs for companies. Jason talks about heightened obligation or some kind of heightened attention. In your mind, Marshall, how do could rule... Listen, we're being generic here. It'd be nice if we can be a little more specific. I gave some categories. How could rules engender or create a sense of cost?

Marshall Erwin:

Let's start high, and then go into the specificity. I do think the lack of cost is really fundamentally a

online. That is an area where I think the rule making process needs to address. It should be one of those fundamental harms that we need strong, smart rules about. I think one thing that we are a little bit weary of here though, so we think about the right way to tackle this is, what we don't want to see is a set of rules that create what I think of as child safety theater, sort of a compliance obligation for systems or tools that are targeted specifically for kids.

Companies already comply with COPPA. They already comply with these baseline requirements, yet we know kids are incredibly innovative uses of the internet. They're going to use the platforms intended for adults, not just the platforms intended for kids. And so, we need rules that put an affirmative obligation on major platforms to do something when they have a reasonable basis to believe kids are using the platform, even if it isn't targeted against them. We need, again, an affirmative obligation for, just to give you an example, YouTube, not just YouTube Kids. That way, we can avoid the sort of kids' compliance theater that we do worry about a little bit. Some of the elements of what we mentioned, the sort of the UK Child Safety Law, we think are really promising, but there is an element of theater there that we worry practically. It isn't going to benefit kids as much as we would like. And so, that's one thing that should all be thinking hard about as we craft [inaudible 01:07:49].

Olivier Sylvain:

Thank you, Marshall. This actually does pick up in something Rebecca was saying as well. For its worth and just to be clear, COPPA is addressed to children under 13, and what the NPR puts out there is the possibility of talking about addressing problems associated with these more sophisticated children, teenagers who are able to navigate to adult sites. Paul, I think you're muted.

Paul Martino:

Thank you. I do want to get to the other issues that you're highlighting. I do have to respond to one thing that Marshall said. I want to bring in some of what Jason said here. I don't think that the internet is a consequence-free zone for all business models. I mean, certainly the context matters. Retailers, if they do not handle data responsibly, they're in a highly competitive industry. If they, for example, have suffered or have been victimized by a breach from a criminal organization or a nation state actor, they're going to suffer brand damage, they're going to lose customers, and there's real world consequences in terms of their market. We've seen that in the past.

Context matters because also it's not just the website you're on, as Jason was talking about. Yes, I agree wholeheartedly with Jason that if your data is being used to provide recommendations and you're on the website where the recommendations are coming, that to me is, and I highlighted in my opening statement, is lower risk. This is meeting consumers, I think, expectations that if they're looking at a product and get a recommendation on that same product, on that same website, that is not the same as, let's say, they're traversing the internet, and based on other data collection or online behavioral advertising, they receive an ad for something that was four or five websites ago. I think that's a different level of context. But another part of context is competition. So, I think

Paul Martino:

Commissioner Slaughter talked about this. There are maybe some online services or apps where they are dominant and there's a feeling from consumers they must use that service, but that's not the case for certain industries. I think the one I'm representing is one of the most competitive, and there are real world consequences if you don't EMC /P <MC0 g50.62 Tm0 gb9rss[(Co)63.74 6.0 g0 G(o)7(s0 G2r7rss[(Cs3)(y)3(An)6(d)3t)9(we

that are being proposed for ensuring privacy and security of sensitive attributes. But most of these are very experimental in nature. And just even assessing alone, the question of fine and fairness or discrimination under privacy constraints remains experimental today. So really concerned about collecting data on individual group membership and the range of risks associated with privacy therein. And it's important that we keep an intention to that work as we move forward and there's work happening around prescribing statistical definitions. These are all questions that we think really need additional work and additional clarity, particularly when we think about the power asymmetries and information asymmetries that exist within the market as well for consumers as they interact with these systems as well.

So focusing privacy regulation on the individual without understanding some of these other pieces is clearly going to have to be an important area of work moving forward. So I'll leave it there in terms of just sort of setting out the stage and some of the complexities, but look forward to continuing that work.

Olivier Sylvain:

Jason, can I draw you in, I mean, you started in your opening remarks talking about business models and this basic idea. I mean, I do want to observe if you don't mind, some of this is experimental, I assume right? I mean, that's part of what we're kind of interested in how we do the risk assessment, but some of

ANPR, so we've touched just the surface really. But again, thank you very much at this point. I'd like to transition now to our second panel and my wonderful colleague, Rashida Richardson will moderate that conversation, thanks.

Rashida Richardson:

Thanks Olivier, and hello everyone. My name's Rashida Richardson and I'm an attorney advisor to Chair Khan and I'll be moderating our second panel on consumer advocate perspectives on commercial surveillance and data security. And I'd like to invite the panelists to come on screen and join me. This panel is focused around two key themes, first we'll explore consumer interests, concerns, risk, and harms related to commercial surveillance and lacks data security practices. Then we'll explore interventions that can help mitigate consumer harms and protect consumer data, including actions the commission can take whether in the form of rules or other actions.

This panel includes Katrina Fitzgerald of the Electronic Privacy Information Center, Harlan Yu of Upturn, ambassador Karen Kornbluh of the German Marshall Fund, Spencer Overton of the Joint Center for Political and Economic Studies and Stacey Gray of the Future of Privacy Forum. If you want to learn more about these panelists, you can find their bios on the public forums events page. We've asked each panelist to offer brief opening remarks and they will proceed in the order I just introduced them. So over to you Katrina/

Katrina Fitzgerald:

Thank you, Rashida. Chair Khan and members of the commission thank you for your leadership on commercial surveillance, data security, and for the opportunity to participate today. I'm Katrina Fitzgerald, deputy director at the Electronic Privacy Information Center or EPIC. EPIC is an independent nonprofit research organization, established in 1994 to protect privacy, freedom of expression and democratic values in the information age. Over the last 25 years, EPIC has advocated for the federal trade commission to safeguard the privacy of American consumers. Unfortunately, the US is now facing a data privacy crisis because powerful technology companies have been allowed to set the terms of our online interactions. Without any regulatory or legal checks, these companies have deployed commercial surveillance systems that track us across our devices and all over the internet to build detailed profiles about us at the cost of exposing us to ever increasing risks of breaches, data misuse, manipulation, and discrimination.

These pervasive commercial surveillance systems are far beyond what internet users expect and they operate in opaque ways that users can't see or understand. Cross site and cross device tracking has become unavoidable for consumers. Trackers collect millions of data points about us each day that are then sold or transferred to third parties who combine them with other data sources linked to us to build invasive profiles. Sometimes these profiles are used to target us with ads. And in other instances, they're fed into [inaudible 01:25:46] algorithms used to determine the interest rates on mortgages and credit cards or to deny people jobs, or housing. The impacts of which often disproportionately harm marginalized communities, this tracking assaults long held norms surrounding privacy. Think about communications letter writing the contents of our phone calls, these have long been private activities and we have legally protected their confidentiality. Why should the rules change when it comes to email? But Google's implementatireW*nBTg nrotect

even when a user seeks information about sensitive topics, such as health conditions or religion. Users cannot configure their way out of these problems, opt in and opt out frameworks are flawed in practice. Both approaches place the burden on individuals to safeguard their data. These are systemic problems that need systemic solutions. The best way the FTC can reign in commercial surveillance under current law is to use the commission section five authority to issue an unfairness rule that limits wide scale tracking and profiling of consumers. Data should only be collected, used and transferred as reasonably necessary to provide the service requested by the individual, that is what people expect when they use the internet.

A strong data minimization rule would also improve data security, data that's never collected in the first place cannot be breached. Data that is deleted after it's no longer needed, is no longer at risk. Just because industry is grown accustomed to operating without any data protection rules does not mean we should continue down that path. It's time to change the business practices that are harming people online every minute of every day. So the FTC must act to change the course. Thank you for the opportunity to participate today.

Rashida Richardson:

Thanks. Harlan.

Harlan Yu:

Hey, thanks for having me. My name is Harlan Yu and I'm the executive director of Upturn. We're a research and advocacy nonprofit organization that focuses on technology, equity, and justice. I'd like to highlight today the important role that the FTC needs to play in rooting out commercial practices that are biased and discriminatory, particularly against historically disadvantaged communities and the most vulnerable consumers. In our work at Upturn, we've seen commercial practices that drive housing insecurity, discrimination and conditions of poverty do in part to how landlords and tenant screening companies collect and use eviction, credit, and criminal records that are products of unjust and racist systems. We've seen commercial practices that amount to insurmountable barriers to employment for certain jodun-2(i)14)(c)-2(n)4(6d)3(ue5(p)0002tco)4(m)(3612 792 aic>srt . c)-2(n)4(6d)(c)11(9(t)-3(o)14(m)-44 0 0 1 0912 ee)-3(2 792

that's not enough. Discrimination exists everywhere in our society, it always has. It is often reflected, often unavoidably in the data about us, which is now widespread. And because data is now endlessly collected, bought and sold within and across virtually every sector of our economy, commercial practices that cause a disparate impact are prevalent. And that's why this rule making is so vital for the FTC to pursue. I'd like to thank Chair Khan and all the commissioners and FTC staff for all your hard work on this ANPR. And I look forward to continuing to engage as this rulemaking process unfolds, thanks.

Rashida Richardson:

interest. And at the very least children and their parents should be able to delete minors data and to reset the algorithms feeding them content.

To address the national security loophole I talked about due diligence to be required for whom companies sell or transfer personal data to and require recipient companies to commit not to conduct... To conduct similar due diligence that they're not selling or transferring the data to known bad actors. And they should subject themselves to enforcement to keep that promise, a kind of know your customer system. And lastly, to address the criminalization of our private lives, even when users have consented to data collection at the time when sensitive data is implicated, like in an online search for or tracking geolocation to an abortion clinic or other sensitive location, these searches should be deleted promptly. Or again, if the user wants to search anonymously, more generally collection of sensitive data could be subject to opt in consent. So these are just a few ideas and thank you for allowing me to present them.

Rashida Richardson:

Thanks, Spencer.

Spencer Overton:

Yes, thank you so much Rashida, I appreciate it. And Chair Khan and other FTC officials, thank you all so much for holding this public forum. I lead the Joint Center, which is America's black think tank we focus on tech and economic policy issues. For years platforms like Facebook and Google have collected data on users and developed algorithms to deliver content. Users often get content customized to their interests, businesses can arguably more effectively spend their advertising dollars, but as Harlan mentioned, these processes can facilitate discrimination. Ads for employment opportunities can be steered toward male users and away from women and ads for new housing can be steered toward white users and away from black and Latinx users.

So one recent example in June of 2022 Meta settled a housing discrimination case with the justice department, as you all know, Meta collects and infers demographic data when users are required to indicate their gender when they, for example, sign up for Facebook, when users join Facebook groups like single black mothers and users create avatars of themselves with skin color and nose and lip and eye shape, and when users post, comment and like particular content. The Justice Department alleged that Facebook allowed housing advertisers to target ads by protected categories. And that Meta developed other tools like a special ad audience tool and ad delivery personalization algorithms that facilitated discrimination. DOJ, as I mentioned, and Meta settled the case while Meta denied liability, the company did agree to stop using the special ad audience tool for housing ads and also to develop a system to detect and reduce bias in housing ad delivery. It also agreed to pay a civil penalty of $115,000, which was the maximum available under that particular statute.

Now, this problem is not specific to Meta or one company, a study of Google AdWords, for example found that Google's machine learning steered employment ads away from women and toward men. Also litigation on a case by case basis is an important tool, but it's not always the best way to prevent

Thanks, Rashida. And thank you to the commission and Chair Khan for hosting this event. FPF is a global nonprofit supported by leading foundations, the National Science foundation, and 200 plus companies across sectors. Our core mission involves researching, educating, and developing best practices at the intersection of emerging technology and law. So first, urge the commission to move forward with this rulemaking, the rapid adoption of mobile devices, wearable technology, connected vehicles, smart homes, all of this has brought an exponential increase recently in the benefits and the harms of data collection in daily life. And because the use of data now informs every consumer facing business model, it's exactly the right time and a very important for the FTC to establish national rules for what constitutes an unfair practice.

Given that the harms related to invasion of privacy and failure to protect data have been so well

advanced notice of proposed role making. But collectively you all represent in our informed by different consumer groups and interests. So to kick this off, I'd love to hear from each of you about what data security and commercial surveillance practices are most concerning to you, how they affect your stakeholders and whether there are any groups or factions in society that are more susceptible to commercial surveillance practices and their intended risks. Sorry, I'm going to ask a lot of multiple questions, we'll start with you Katrina.

Katrina Fitzgerald:

Sure, thanks Rashida. I touched on a lot of them my opening statement, but basically the widespread surveillance of general internet browsing and app activities is the most problematic thing we see. It's unavoidable, it's beyond what reasonable consumers can grasp or understand. It reveals their most sensitive characteristics, health conditions, sexual orientation, sexual activities, political affiliations, et cetera. And it's transferred to hundreds if not thousands of different companies, typically without users knowledge or consent, the harms in that are data breaches, data misuse, unwanted secondary uses, inappropriate government access and it can have a chilling effect on consumers' willingness to adopt new technologies or engage in free expression. In addition to that, we have the problem of data brokers,

Katrina Fitzgerald:

Thousands of data brokers in the US that buy, aggregate, disclose and sell billions of data elements wit

than what that person actually did, particularly when we're talking about non-conviction arrest records. So yes, in the use of data and technology and these commercial surveillance practices, these risks and harms often do manifest in very different ways, often to the greater detriment of Black and brown people, to women, those who are LGBTQ people, with disabilities and others who have been historically disadvantaged.

Speaker 1:

Thanks. Karen?

Karen Kornbluh:

Yeah, I just want to underscore data brokers and the buying and selling of data in ways that folks don't understand and to entities, that they might not want to have their data. And the use of this data to fuel social media algorithms that can put people into silos and that can pose dangers to our democracy. One of the, leading into your last second part of your question and into, I think your next question's about

security. And that approach avoids the problems raised by opt-in frameworks, the consent fatigue, the cookie banners approach we're talking about, and dark patterns that nudge people into granting permission for data use. Because it takes the burden away from the user and it puts the burden instead,

In addition to Spencer's comment around not being colorblind. Yeah, I do. I would like the FTC to think about what a company would need to do to show good faith efforts to root out disparate incomes, disparate outcomes. Has it tested its own products? Has it pursued less discriminatory alternatives?

Karen Kornbluh:

Yeah, agree with all that. And then I guess, what other things I would say, is that in Europe they've deemed that you shouldn't be, that access to the service shouldn't be

Speaker 3:

... be contingent on consent. And so, I think that's an interesting thing to think about, but of course, that

Yeah, I already spoke on this in my last [inaudible 02:23:18], so I'm not going to repeat it. I just wanted

And I think just as my final point here, we should be clear that yes, company self-policing is important, but it's not enough. Yes, it's great Meta did an and independent civil rights audit, it's building out civil rights infrastructure,

statements, and material emissions in stated policies. Third, the commission should address data brokers and transparency. Brokers require sensitive data and complex profiles without having any direct relationship with the individuals whose data they profit from. Thank you for your attention, and the opportunity to speak today.

Peter Kaplan:

Thank you, Andrew. Our next speaker is John Davidson.

John Davidson:

Thank you, Chair Khan, and members of the commission. I'm John Davidson, Senior Council at EPIC. I want to second the comments of my colleague Katrina, and say that EPIC is eager to work with the commission to ensure that this process yields the strongest rules possible. I'd like to add another point though. Since the FTC announced this rulemaking, some have argued that the commission is overreaching, that even just by asking for input on how to protect the public from abusive data practices, the commission has somehow gone too far. I want to say that nothing could be further from the truth. Congress established the FTC over a century ago, for the exact purpose of taking on industry-wide business practices that threaten the general welfare. The commercial surveillance practices we're talking about today may be relatively novel, but the commission's authority and responsibility to address them is clearly not. This rulemaking stands on rock solid ground.

Of course, there are statutory guardrails on the FTC's rulemaking power. In particular, any data practice that is declared unfair by the FTC must meet the unfairness test, established by the commission and ratified by Congress, but Congress's adoption of that unfairness test is proof that it expects the FTC to act when consumers face systematic and unavoidable harm as [inaudible 02:37:58]. The fact that the FTC has rarely used its rulemaking authority is just not an argument for further inaction, it is a confirmation that the commission has untapped power to address the root causes of the ongoing data crisis.

Finally, it is beyond doubt that the commercial surveillance practices at issue in this rulemaking are prevalent and demanding of an industry-wide approach. As recent legislative developments have shown, there was broad political consensus over the harms we faced from commercial surveillance, digital discrimination, and lax data security. EPIC continues to support legislative data protection efforts at the federal and state level, but the FTC already has significant authority to define and penalize the unfair practices at the heart of the surveillance economy. This is no time to let that authority sit idle, and we're heartened to see that the commission understands the urgency of this moment, and is moving to act. Thank you.

Peter Kaplan:

Thank you, John. Our next speaker is K.J. Bagchi.

K.J.?

K.J. Bagchi:

Oh, sorry.

Peter Kaplan:

That's all right.

prepared for the new regulation in New York City, taking effects in January. I worked on [inaudible 02:42:38] humanity, just saying.

Another thing is that privacy starts at the code, so we need to go all the way back there. Aggregation of data doesn't afford me the right to be forgotten, and so, those issues need to be addressed, as well as ethical issues all along the development process. Privacy by design is not a marketing term. Those are a set of principles that need to be applied as you're building a tool. Now, EdTech, that's a hot mess. You're talking a big game like you want to go after people. I encourage you to do so, and with all deliberate speed, talking to the school board officials is like talking to green beans, and they have no idea why I am so excited about this. So, the sooner you get on that, the better. Also, data-

Peter Kaplan:

Thanks, Heidi. Thanks a lot. Your two minutes-

Peter Kaplan:

Appreciate it. Our next speaker is Kavya Pearlman. Kavya?

Kavya Pearlman:

Dear Chair Khan, commissioners, and FTC staff members, we live in a time when the harms to consumers go beyond compromising personal data that harms credit, or even job prospects. Today, we must consider that the risks involve human beings, their welfare, their existence. For this reason, FTC efforts to protect Americans from practices of collecting, analyzing, and monetizing of data need to go from their protection of information to prevention of harm, and to further ensure safety by design. We're moving from a post-truth era to a post-reality era, with a constant reality capture. Seeing is no longer believing.

I'm Kavya Pearlman, Founder and CEO of XR Safety Initiative, XRSI. We're a standards developing organization with a mission to help build safety and inclusion in emerging technology ecosystems, like the metaverse. We build privacy safety ethics standards, such as the novel XRSI privacy and safety framework. On behalf of over 150 advisors and the entire XRSI team, we urge you to number one, introduce special data type considerations for inferred data associated with virtual reality, augmented reality, neurotechnology, and metaverse related technologies, to correctly identify data classifications and appropriate security and privacy stance. Number two, include anti-competitive data consolidation practices, and the use of privacy enhancing technologies as well. Number three, then coding for addictive engagement for all consumers, but especially on young people, for those under 18.

The FTC has an opportunity to address these risks proactively, and reduce the harm that cannot be compensated to Americans by building safeguards around these ubiquitous converging technologies. We're grateful for this opportunity to play our Part. XRSI will submit our detailed recommendations. We are the [inaudible 02:50:36] process, for your consideration. Thank you again for the opportunity. Thank you, Lina Khan.

Peter Kaplan:

Thank you, Kavya. Our next speaker is Jonathan Pincus. Jonathan?

Jonathan Pincus:

I'm Jonathan, Founder of the Nexus of Privacy Newsletter, where I write about the connections between technology, policy, and justice. As a long time privacy advocate, I greatly appreciate the commission's attention to commercial surveillance. My career includes founding a successful software engineering startup, and co-

Serge Egelman:
In the

Serge Egelman:
... process. Thanks.

Peter Kaplan:
Okay. Thanks a lot, Serge. Our next speaker is Christopher Oswald. Christopher?

Christopher Oswald:
Thank you to the commission and staff. My name is Christopher Oswald. I'm with the Association of National Advertisers. ANA is the nation's oldest and largest advertising trade association. I thank the commission and staff for the opportunity to speak today. The modern American economy is built on the idea that consumers should have a diversity of options when it comes to choosing what products and services they receive. Advertising is at the foundation of that economy, connecting consumers to businesses in evermore effective and relevant ways. The responsible use of data has helped improve these connections for well over a century. While the technology use in these practices has changed, the fundamental truth of connecting businesses to consumers remained central to the advertising industry.

In the modern digital economy, advertising's role has expanded from making connections to subsidizing a plethora of free and low cost services for Americans. Without advertising support, the internet would not have the equitable and democratizing effects it does. Consumers who would pay more and those without the ability to pay would be cut off from valuable news, entertainment and other services that better their lives. Advertising is not an unfair or deceptive practice, and the responsible use of data to engage in more relevant and better advertising is not an appropriate focus of the commission's efforts. What the FTC terms as surveillance is in large part, the everyday responsible collection and use of data to deliver goods and services consumers want and to connect consumers to their next favorite product or piece of content through effective advertising.

Throughout the ANPR, the FTC terms personalized and targeted advertising is forms of its broadly defined category of commercial surveillance. It also states that one of its concerns is that companies will use data to sell more products, which is exactly the core activity of companies that seek to turn a profit. The FTC should not allow this apparent prejudice against advertising to control its rulemaking process or inadvertently create rules that would fundamentally damage the consumer economy. ANA and its members have a stake in the responsible collection, use and sharing of information for effective advertising. We will work with the commission throughout this rulemaking process to show that our industry as a whole does not engage in the types of unfair and deceptive practices the FTCs statutory authority allow it to regulate through Section 18 of the FTC Act. Thank you very much.

Peter Kaplan:
Thank you, Christopher. Our next speaker is Lydia X.Z. Brown. Lydia? Lydia, are you available?

Lydia X.Z. Brown:
Hello, this is Lydia. Can you hear me?

Peter Kaplan:
Yep.

Lydia X.Z. Brown:

case of scammers is one of the most blatant examples of how data falling to hand, seeking to make a

expression, room stands and analytics when students take these laptops at home. Schools also upload sensitive student data into AI-powered learning management systems, like PowerSchool, Google Classroom, or even into immutable blockchain ledgers.

There are thousands of data points, like whether a student has been pregnant, whether they live, whether they are citizen, their medical and mental health conditions, student discipline history, criminal status surveys, income and disability data. Schools are also measuring student behavior using apps with

This is because obviously if you're a victim of domestic violence or stalking or sexual assault or some other different kinds of targeted crimes, it is incredibly dangerously, easily stupid for anyone to find and use public information to discern your home address or public information about you that can lead to additional harm. That sounds great, but I would also like to point out that due to the work of some truly monstrous criminals and negligence on the part of some government bureaucrats, we know of at least one instance where the government office in charge of one stage address confidentially program was hacked and the lists of hundreds of people who were participating in that Safe at Home Program, as well as many of their real addresses and as well as the identities and addresses of people who simply applied to the program were made public and are now available for anyone who knows where to look to download that information and use however they see fit.

Any data point that can be quantified and measured can be collected, and there are going to be people who are going to aggregate that data and make it available publicly. In practice, data sloshes around between consumers, the public internet, private companies, underground darknets, and eventually government agencies. So while it is incredibly important that we think about regulating the companies collection and use of data, if you're going to be addressing this issue, you have to take a really hard look and grapple with the fact that there are terabytes and terabytes of data that just exists in the public domain that anyone can collect and reshare and make directly available without-

Peter Kaplan:

Thank you, Chris.

Chris Weiland:

... interacting with consumers at all. Thank you.

Peter Kaplan:

Thanks a lot, Chris. Our next speaker is Rick Lane.

Rick Lane:

Thank you. I am Rick Lane, CEO of Iggy Ventures, a volunteer child safety advocate and advisor to REGO Payment Architectures, the parent company of Missoula, the only COPPA certified family digital wallet app and online pay buttons in the marketplace. Back in 1999, I was a member of the FTC's advisory committee on online access and security. A question asked in the ANPR is which measures beyond those required under COPPA would best protect children, including teenagers from harmful commercial surveillance practices? One area of child privacy protection that is often overlooked and was not even mentioned by any of today's panelists is digital payment apps and debit cards that target children and collect and exploit a shocking amount of their data.

The privacy space between COPPA and Gramm-Leach-Bliley creates a FinTech child privacy protection

This first of its kind study wil

with people who are fighting against an oppressor or a repressive system that they have become victim to. The voice of those who believe that life is more sacred than property must be heard now."

Peter Kaplan:

Thank you, Jacob. Thanks a lot now.

Jacob Dockter:

Thank you.

Peter Kaplan:

Okay. Yep. Thanks, Jacob. Our next speaker is Berin Szoka. Berin?

Berin Szoka:

I'm Berin Szoka, president of TechFreedom, a think tank dedicated to internet law. The federal trade commission has uniquely broad powers over nearly the entire economy, especially the power to decide what is fair. In the 1970s, the FTC's conception of unfairness had practically no limits. By 1980, the FTC was becoming an unelected second national legislature. Huge bipartisan super majorities in Congress imposed procedural safeguards to ensure that unfairness and deception rulemaking is focused on clear problems with no effective alternative to regulation. That's why past advanced notices and proposed rulemaking focused on discrete issues, such as impersonating government agents, negative option marketing and clothing washing labels.

By contrast, this ANPR is as broad as is the concept of privacy itself. Past ANPR has identified administrative orders or court decisions establishing the unfairness or deceptiveness of specific practices. This ANPR sites only complaints, settlements and news reports across a wide range of data practices. Any proposed rule must describe with particularity why the commission has reason to believe that specific practices are unfair and deceptive and any final rule must explain why prescribed practices actually violate the FTC Act. An unfair practice must, "cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

Some data practices certainly do cross that line, but the commission must prove its case regarding each practice it seeks to regulate by rule, just as in any enforcement action. The commission must also establish the prevalence of any practice subject24 13.lme6ie y explain why prescribed practices

digital identity systems. These are immutable digital ledgers that are being falsely marketed as a private secure ways to transfer data. Blockchain systems have been widely criticized by over 1,500 computer scientists and technologists in a letter to Congress this past June, documenting fundamental flaws in the design of the technology. That letter is published at the concerned.tech website. The append only nature of blockchain systems means that data can never be deleted, never be corrected, and that any information will forever remain on an individual's permanent digital ledger, including false information.

I'm currently seeing numerous attempts to put children's data from cradle to career on these distributed decentralized digital ledgers. COVID testing companies are related and egregiously overlooked area of surveillance data risk. A current FERPA loophole allows privately contracting companies to be named as a school official, in effect allowing many such vendors unfettered access to a treasure trove of educational health, financial and behavioral student data with zero oversight and zero consequences should they pull any data that was not part of their intended work. One such company, a DNA data basing firm that also openly contracts with a blockchain-based data sharing app, is among the largest vendors in California county and university systems, openly stating that privacy policies that they transfer data internationally. It is also currently under investigation by two federal agencies, the SEC for allegedly violating anti-kickback laws, and the Department of Justice for allegedly conducting medically unnecessary testing.

I urge the commissioners to join these two federal agencies to further investigate data vulnerabilities baked into third-party partnerships of data reporting apps used by this company and related firms. Our current lack of protections and regulations allow for the vast extraction of multiple forms of sensitive data from individuals who are required to test in order to access educational or public agency settings, given already discriminatory policies are most disenfranchised communities would be most subject to the greatest data harms and for the problematic use of these tests in our apps. Thank you for your time and attention to this critically important and underreported aspect of commercial surveillance.

Peter Kaplan:

Thanks, Roxana. Our next speaker is Hye Jung Hun. Hye?

Hye Jung Hun:

Thank you. I'm a researcher at Human Rights Watch, an international human rights NGO. Recently, we published a global investigation on the education technology or ed tech endorsed by 49 governments for children's education during the pandemic. Here's what we found. Children were and are forced to pay for their education with their privacy. In the rush to connect children to online classrooms, most governments, including the U.S., authorize the use of ed tech that surveil the children online outside school hours and deep into their private lives. The overwhelming majority of these 163 ed tech products harvested data on who children are, where they are, what they do in and outside of their virtual classrooms. Others digitally fingerprinted children in ways that were impossible to get rid of or avoid without throwing the device away in the trash.

In the U.S, we investigated nine ed tech products recommended by the California and Texas Departments of Education. Not only did we find that all nine surveilled children or were capable of doing so, most of them also sent or granted access to children's personal data to advertising tech companies that specialize in behavioral advertising or whose algorithms determine what children see online. Children and their parents were largely kept in the dark, but even if they've known, their personal data was extracted from them in educational settings where they could not reasonably refuse or opt out without opting out of school altogether during the pandemic.

of all personally identifiable information and user data, including photographs without explicit consent, separate from terms and conditions which includes a general ban on excessive non contextual data collection and tracking. We recommend a requirement to limit data collection to no more than is necessary for the management and notifications for consumer services and accounts including data minimization. We recommend establishment of a HIPAA style best practices for universal data security. We recommend the definition of minimal business size for the affected rule making so that this is not impossible for small businesses to comply with.

We suggest defining a scope of platforms that must comply, including websites, apps, databases, browsers and platforms. We suggest imposition of criminal penalties for failure to protect data and unauthorized sharing and disclosure similar to that under 21 CFR 11. We suggest a consumer right to full access and revocation of data use and collection authorization, in other words, a right to delete. We suggest a ban on states from sharing information or data under obsolete sunshine statutes without the individual's consent. We suggest a national do-not-collect data registry that consumers can opt out of across the board from unnecessary data collection for advertising and commercial or business purposes. We all...

Peter Kaplan:

Thank you, Tim. Thanks a lot.

Tim McGuinness:

Thank you.

Peter Kaplan:

Thank you, Evan. Our next speaker is Douglas Gastonguay-Goddard. Douglas?

Douglas Gastonguay-Goddard:

Good afternoon. Let me get my notes here. Thank you for the opportunity to speak here today. My name is Douglas Gastonguay-Goddard. I am a software engineer. My comment today is on commercial data aggregators who publish and sell our personal information. These companies could broadly be categorized as people search companies, where you go to a website, type in a name and city and retrieve an individuals name, address, age, phone numbers, associates and family members. The issue I would like to raise is that these commercial data brokers receive almost all of their information from public government sources. The California Department of Motor Vehicles, for example, sells information including your name, address, zip code, phone number, date of birth, and even your email address. Similarly, California voting records include your name, address, phone number, and political affiliation. The United States Postal Service sells your address when you file a change of address form. That address change information flows to insurance companies, credit card companies, and any other entity who had your previous address.

There are no restrictions on the further transfer or sale of this data. This data is some of our most private information, yet it is readily published and sold by our government. If we would like to stop commercial data brokers, we should address their biggest data source. The government should not, by default sell or publish your information without your explicit opt-in consent. This is not a system that users can opt out of. In addition to cutting off this source, we need a law for data providence such that a user can track through the chain of custody to the origin of their data and potentially sever that relationship if they so choose. That is the conclusion of my comment. Thank you very much.

Peter Kaplan:

Thank you Douglas. Our next speaker is Fred Janct. Fred?

Fred Janct:

Bring my notes up here. Thank you. My name is Fred Janct and I'm a privacy program manager in the insurance industry. Thank you for this opportunity to provide my individual comments today, and thank you to today's speakers for their input on this vital discussion as it relates to data privacy. Unfortunately, much of this discussion and much of the discussion around greater privacy has and continues to revolve around the ideas of security and control. As a consumer, are companies protecting your data, companies showing consumers that their data is being handled safely. However, when assessing commercial surveillance as it's being discussed today, the collection, aggregation, analysis, retention, transfer and monetization of consumer data, the idea of visibility is not being discussed enough. An average consumer under video surveillance can often see how they're being surveilled, the camera being visible to them often with an accompanying declaration from the business or organization alerting them to this surveillance.

The selling of a mortgage or the transfer of the servicing of it requires a notification to the consumer, often referred to as hello, goodbye letters in the mortgage industry. In this era of modern digitalization however, the average consumer is awash in surveillance in almost every aspect of their life, and yet in terms of data with commercial surveillance, there is little awareness by the consumer that they're even being surveilled. Even so how much surveillance is being engaged at any given time, and that is just on the collection end of the surveillance paradigm. Data brokers not only collecting massive amounts of public consumer data, but these companies are also maz-3(e)ials0 g0 G[b)3(ein7y6 1 sumer datai[b)

appreciate the significance of the data being collected unless they can see either their own data in full or a clearly explained example of a full data set.

I firmly believe that the path to continued technological success in this country is through ethical product design, and I believe you will find many allies in this effort. We are here to collaborate. Please help us to do the right thing. Thank you.

Peter Kaplan:

Thanks, Gene. Our next speaker is Stephanie Joyce. Stephanie?

Stephanie Joyce:

Hi, I'm Stephanie Joyce, senior vice president of the Computer Communication Industry Association, which has long supported comprehensive nationally applied privacy rules for the internet ecosystem. Digital publishers, advertisers and consumers want to know what are the rights, obligations and best practices for maintaining the online environment as a vibrant marketplace, while protecting sensitive data that can be linked to individuals in a manner that would cause them harm. Congress has revisited privacy this year in HR8152, the ADPPA. Several items in the notice including automated algorithmic decision making are addressed in the ADPPA. The commission might be served by relying on Congress to create a statutory framework to govern these matters, rather than attempting to adopt rules out of full cloth. The term commercial surveillance misapprehends what digital services do. The aim for CCIA members is always to enhance the end user experience. Digital services companies rely on the data consumers give them in order to make interactions and transactions more timely, seamless and customized.

Concerns about behavioral advertising can obscure the pro-consumer and pro ecosystem effects created by this highly evolved method of consumer outreach. As CCIA stated in comments this past January, behavioral advertising saves time and increases value for both sides of the online marketplace. To presume that behavioral advertising is a dangerous practice and adopt rules built on that presumption threatens to upend consumer welfare and online business models. CCIA agrees that bad actors must be dealt with. We are concerned that the rules as proposed would be too prescriptive. As the notice acknowledges, there is a risk of obsolescence when rules embrace prescription over normative guidance. In addition, X anti rules often cannot avoid having a technological bias rather than being technology neutral. Finally, new regulatory regimes can unintentionally create competitive effects. Overly prescriptive rules might inadvertently give advantage to firms by erecting barriers to entry. The risk should be factored into the balance between consumer benefit and marketplace competition. CCIA looks forward to submitting comments next month in this proceeding and thanks the commission for its time and attention.

Peter Kaplan:

Thank you, Stephanie. Our next speaker is John Byrd. John?

John Byrd:

Yes. Hello, my name is John "JB" Byrd and I'm president of Miller Wenhold Capital Strategies based in Fairfax City, Virginia. Our surveying, mapping and geospatial clients include the National Society Professional Surveyors, NSPS, US Geospatial Executives Organization, USGO and the Subsurface Utility Engineering Association. In 2014, then FTC chairwoman, Edith Ramirez responded to congressional QFR regarding the FTCs regulation framework on precise geolocation data and information by commenting that when it comes to mapping activities that, "Companies that collect and use geolocation information for these purposes do not need to provide a consumer choice mechanism." We respectfully urge the FTC to acknowledge that geospatial imagery and data collection used for Gen application is a valued part of

is, if your software is running on my device and that software collects data, you should show me everything that you're collecting and provide me the ability to verify you're not collecting anything else.

Transparency at the point of collection isn't enough. We also need public visibility into the data sharing between companies and the ulterior uses of data, but it's a necessary though not sufficient first step to enable public understanding of corporate surveillance and meaningful feedback and accountability. Implementation is going to take time and care. There's security issues to think about. We'll probably need exceptions for certain special cases. I think penalties should start with warnings and increase gradually over the course of years. Thank you very much.

Peter Kaplan:

Thanks, Doug. Our next speaker is Jodi Masters Gonzalez. Jody?

Jodi Masters Gonzales:

Thank you for having me today. I am commenting as a consumer, PhD researcher, open source intelligence investigator, board certified independent auditor of AI systems and founder of a small business developing privacy enhancing technologies. I'd like to address a model of shared responsibility

pernicious influence on children and teens and adult consumers whose marginalization and related trauma make the ads even more harmful. As a recent UC Berkeley study explains, ads promoting body ideals built on racial, gender based and other prejudices that stigmatize certain body types. In contrast, ads for critical opportunities have been targeted to consumers that tend to access those opportunities more often. A factor used to predict engagement.

Consumers who have previously had less access to these opportunities are less likely to get these ads and struggle to show that they would've pursued the opportunities if they had received the ads. Another example is data driven decision making systems for determining eligibility or resource allocation across sectors. Many of these systems can fail consumers because they're training data does not accurately represent the whole population which they're used. They're designed to evaluate data that functions as proxies or for protected traits or they're not built to be usable for all consumers. Such systems produce adverse outcomes because they're not designed to mitigate impacts on certain groups of consumers. For instance, tools that prevent disabled job applicants from advancing in a higher end process.

To pursue viable discrimination claims, consumers would need built transparency from companies about how and why algorithm systems process their data to pinpoint how they contribute to discriminatory outcomes. Platforms also update accountability for these harms due to a lack of consensus about applying civil rights laws to companies that are not traditionally considered to be covered by such laws, but increasingly fulfill functions of covered entities. We urge the FTC to consider impacts on all communities, including disability and LGBTQ plus communities not mentioned in the ANPR and harms that are particularly severe along intersections of marginalized identities. We look forward to engaging further in the commission's [inaudible 04:01:51] making process. Thank you.

Peter Kaplan:

Thank you Ridhi. Our next speaker is Jeff Chester. Jeff?

Jeff Chester:

This is the Center for Digital Democracy. Thank you very much. The pervasive role that commercial surveillance plays in the everyday lives of Americans and those abroad is due in part to the historic failure of the FTC to address the forces that comprise digital marketing. Commercial surveillance operations evolve because none of the many problematic practices that are among its fundamental features were never seriously challenged. The FTC looked the other way as disturbing practices were adopted industry wide, even in the children's market where there was a law. The FTCs big tech antitrust failures also helped deliver our far reaching surveillance system. CDD and allies file timely complaints,

identifiers, the key role of AI to generate real time personalized content designed to secure consent. Growing tactics to influence emotional and subconscious behaviors must be

both laws require that if schools are going to share student data with third parties without parental consent, it can only be done for educational purposes. And yet, there are numerous ed tech programs used by students that traffic in their personal data, either by using it to improve their products or create new ones, essentially using students as subjects in market research, or even more alarmingly selling the data and using it to target ads for their own benefit or that of third parties. Videos on YouTube, with its insufficient privacy controls, are commonly assigned to students as our countless free programs access via [inaudible 04:15:31] agreements that monetize their data in multiple ways. Data collected via surveys in schools are processed into algorithms used to steer even young students into particular careers in potentially discriminatory ways.

We recommend the following measures. Schools should be required to obtain parental consent for collection of personal student data, especially data regarding behavior, biometrics, geolocation, disability, and health conditions. The data collected should be minimized to only that which the company needs to perform its contracted services and deleted when no longer needed for those services. The sale or use of student data for advertising should be strictly prohibited, as well as it's used to improve products or develop new ones.

The FTC should reconfirm that parents have the right to access any personal data collected by ed tech companies from their schools and understand how it's been processed and/or redisclosed, challenge it if it's incorrect, have it deleted, and opt out of further disclosure. The FTC should use its authority also to audit the practices of these companies, including their security practices, their use of algorithms, and to ensure that personal data, student data, is not inappropriately redisclosed, used in discriminatory ways and/or repurposed for non-educational purposes. Thank you for the opportunity to speak to you today.

Peter Kaplan:

Thank you, Leonie. Our next speaker is Elif Kiesow Cortez. Elif?

Elif Kiesow Cortez:

Thank you very much for the opportunity. I'm a privacy scholar working extensively with the GDPR for over a five year period now. Since its implementation, we have seen a lot of interesting attention internationally also on the GDPR. And just to comment on some of the recent discussions here, it is great to hear such diverse opinions. And for myself, I would like to highlight that in the privacy debates, sometimes we might think that we are either going to argue for pro consumers or pro companies and guiding companies for a long while in implementing responsible technology. I have to say that I believe in responsible technology and it is possible also for the FTC to find a balanced approach.

So with all of these international developments, I think that this is also in light of the casual privacy law discussions at the moment. It's a great time for the FTC to work on tangible standards, guidelines, tools, that could be used to evaluate and perhaps even to audit privacy practices of companies, in order to protect consumers while incentivizing the companies to compete with each other, to do better than each other, in ethical product design and implementing responsible innovation.

Even if ANPR might not advance, we do know that the problems like algorithmic bias and dark patterns will continue staying with us and maybe even increasing. So through this a ANPR or not, we will be looking forward to FTC's active role in shaping this debate. Thank you very much for the opportunity to comment today.

Jordan Crenshaw:

Good afternoon. My name is Jordan Crenshaw. I'm the Vice President of the US Chamber of Commerce Technology Engagement Center. Congress with the ascent of the president, not the Federal Trade Commission, is the only government entity that can mandate economy wide policies for data privacy, security and algorithms. If the commission proceeds on the path of promulgating rules economy wide, as asked about in its ANPRM, it will trigger the Supreme Court's major questions doctrine, which requires agencies who have been given clear authorization from Congress in the case of rules that have breqdcamFTC.v major economic consequences.

A large scale comprehensive rule making will have a major impact on the economy. Data is core to business decisions of every company in America. We recently found at the US Chamber that small businesses using technology and data have a $17 trillion impact on the economy and support a hundred million jobs. 80% of small businesses say technology helps them compete with larger firms, and that same number says that limiting access to data will harm their business operations.

Congress has never given authority to the FTC to make broad rules on data privacy. If it did, it woul 1 7(4(-)6e) TJETQq0.0

compliant to this spirit of why this other team was penalized. And this helps. I think it gets business leaders really meaningfully engaged in the spirit of the law, not just checkbox and policies.

If I could change anything, I would actually encourage the FTC to be more frequent and more severe in these, because I can only imagine that, at least in the private markets where I work, so venture capital, hedge funds, private equity. If the FTC penalized a firm, like really, really severely penalized a firm, maybe forced them to liquidate, because of something as ambiguous as lax data security, heads will roll and people will look left and right and say, "Whoa, we need to get on board." It's not about checking a box with policy. How do we do the right thing? It is effective. I met my time. Thank you again, for all your good work. Thank you.

Peter Kaplan:

Thank you, Benjamin. Our next speaker is Jennifer Huddleston. Jennifer?

Jennifer Huddleston:

Thank you. My name is Jennifer Huddleston and I serve as a policy council with Net Choice, a trade association dedicated to free enterprise and free expression. Thank you for the opportunity to speak at today's public forum.

Data privacy is an important issue for many Americans, as well as for the development and improvement of products in the tech sector and beyond. As my time is short, I would like to briefly highlight a few key concerns with the advanced notice of proposed rulemaking. First, there is a threshold question about the FTC's authority to undertake this process. Without a clear statutory grant from Congress, this issues a broad sweeping rule as it relates to data privacy and data use. The FTC arguably does not have the authority to undertake this endeavor. In fact, Congress is currently considering data privacy bills and has not granted the FTC with the authority to enact roles on this particular topic. In light of the recent Supreme Court decision in West Virginia with the EPA, regarding the major questions doctrine, any rule making not tied to its specific congressional grant of authority will likely face further challenges.

Additionally, the framing of the rule making to address consumer surveillance wrongly vilifies beneficial data technology practices across all industries, not just tech. This is concerning and gives the impression that the FTC has reached a conclusion without first hearing the evidence. The ability of internet sites to recognize and quickly restore a user's preference has been beneficial, not harmful. The framing of the ANPR purports to protect personal data, but what it actually does is an attack on advertisement. Before moving forward, the FTC should do more robust economic analysis of the harms that could occur from this type of rule making, especially to low and middle income families as well as to those who will face many more ads, more paywalls and less content. Likewise, the FTC should consider the impact to creators and to small businesses from a loss of revenue.

Finally, the FTC should use its limited resources to focus on the privacy concerns that do clearly fall within its mission, rather than expanding to intervene in every facet of the American economy. This could include a focus on those cases where there are clearly bad actors and actual consumer harm ,rather than creating a burdensome regulatory regime that presumes innovative uses of data are guilty until proven innocent. I thank you for your time, and I look forward to providing further comments for consideration [inaudible 04:25:53]. Thank you.

Peter Kaplan:

Thank you, Jennifer. Our next speaker is Zubair Shafiq. Zubair?

Zubair Shafiq:
Thank you. My name is Zubair Shafiq. I'm a Professor of Computer Science at the University of California,

expect to fully engage a global dynamic data economy. The first of the FTC Fair Information Practice Principles globally recognizes the need for consumer notice and awareness. This, in particular, needs expansion and development to address the harms in the evolving cyber physical world.

To address these hards notices must provide sufficient transparency for consumers to understand who, where and what they're dealing with, ideally with a receipt and record created by and for the consumer. Without this, there is no security. Without this, there is no trust. And without this, there is no privacy for consumers. And this lack of trust, security, and privacy is a substantial harm, unavoidable, and under the commission's authority and requires actions. The FTC should require two factor notice and a requirement for measuring how performative the notice is for the consumer. The two factors of notice are, one, notice of risk and, two, proof of notice. Most of all, be offered in a meaningful way that consumers can understand, otherwise there is no basis for consent to surveillance and the interaction of identification and traditional security goals.

With two factor notice, the landscape for consumers changes drastically. It introduces decentralized data co-governance where consumers, as well as regulators, can enforce consumers rights independently. This reduces consumer risk and increases private, personal data value and the cost effectiveness of security, privacy and regulation. It also-

Peter Kaplan:

Thanks, Sal.

Sal D'Agostino:

One last bit, sorry. It can also benefit consumers organizations to the FTC with localized and decentralized objective open source intelligence that can account for the legal technical state of consumer surveillance and data protections. I will provide these in further written comments, including on this specification between factor notice. Thank you Peter, and the FTC.

Peter Kaplan:

Thank you, Sal. Our next speaker is Jan Fernback. Jan?

Jan Fernback:

Thank you to the FTC for this forum. I'm Jan Fernback, a professor at Temple University, and I research data privacy and surveillance. There's no doubt that sensitive consumer data are being used and abused by corporate and governmental actors, but current FTC mechanisms of enforcement, case by case measures, are well intentioned yet inadequate to combat such abuses. Consumers cannot opt out of using essential digital platforms that collect and monetize our data. In fact, based on my research, I go through ext

the domain of Congress. The problem is that Congress has failed again and again to pass any data privacy legislation other than KAPA and the Fair Credit Reporting Act.

The currently proposed American Data Privacy and Protection Act, ADPPA, is going to fail in the Senate because it exempts de-identified data which is easily linked to individuals. Some previously enacted state laws are more powerful than the ADPPA, so the situation has become untenable and the FTC needs to have some teeth in order to secure all of our data. Thank you so much for allowing me this time to comment.

Peter Kaplan:

Thank you, Jan. Our next speaker is Nicolas Dupont. Nicholas?

Nicolas Dupont:

Hi everyone. I'm Nicholas Dupont, the CEO of Cyborg, a cybersecurity and data privacy startup based in New York City. I'd like to start by saying that I'm gravely concerned about the threat to consumers posed by commercial surveillance. Today, technology platforms largely control what we see and leverage the insights they've gathered about our behaviors to advance their own agendas. By allowing these practices to continue unchecked, we're consenting to the extortion of our behaviors and preferences for their own benefit. What we once believed to be objective facts presented to us during an online search or while browsing the news are now the results of content suggestions, which are algorithmically tuned to the benefit of the platform. It's not difficult to imagine a near future where consumer choice is no longer an expectation, but a mere illusion. Where information we see is no longer objective, but rather delivered to us with the goal of guaranteeing desirable outcomes for technology platforms and their advertisers.

Now, not here to claim that technology companies are bad, far from it. In fact, I founded a tech startup focused on solutions to address these varying concerns. Innovation in the tech space has completely changed the world. Technology's made people's lives easier, made education more accessible, and generally brought the world closer together. However, unbridled innovation with little to no regulation can often have unintended consequences. I believe it is in government's responsibility to protect consumers from the side effects of technology innovation. While digital personalization has brought tremendous convenience to the masses, it has also created an era of commercial surveillance. It is only through the protection of data privacy rights, and the stopping of mass collection of consumer behaviors, that this threat can be controlled.

But privacy cannot be solely enforced through privacy policies. It needs to be enforced for technology. The requirement of end to end encryption for personal information will be a massive

Nicolas Dupont:

...enforceable and effective step towards reigning in commercial surveillance. It is the FTCs mission to protect consumers by preventing unfair and deceptive business practices, so it's my sincere hope that the FTC and the federal government as a whole will embrace this opportunity to continue protecting consumers. Thank you.

Peter Kaplan:

Thank you, Nicolas. Our next speaker is Vasuki Pasamarti. Vasuki.

Vasuki:

Hi. Thank you for letting me speak. My focus is on vulnerable groups. In protecting vulnerable groups from abusive data collection practices, there should first be consideration for the tautological alignment in due diligence and due process around defining and communicating terms, such as a person with a disability, across all US government agencies. For algorithms to effectively develop within their AI, legislation that sets forth definitions of a person with a disability seemed to be different across state, local, and federal programs, and the confusion remains where, for example, the legislation overseeing a federally funded program enforces non-discrimination at a very seemingly social, medical and demographic level, but the program itself defines a disabled person purely under the construct of being a Social Security disability recipient, and the data collection is incepted at every level, all the while, and used by private companies.

Due to these fundamental disconnects, as well as multicultural elements at play, lacks subjective definitions of other terms, such as human rights, bias, due process, could be conveyed, causing potential presumption, surveillance, and lack of enforcement in local government, as well as in the commercial area. A final note in the course of Roe versus Wade having been overturned, there should be added protection around mental health data poaching and against retaliatory surveillance for survivors of trauma. Thank you very much for letting me speak.

Peter Kaplan:

Thank you, Vasuki. Our next speaker is Cali Schroeder. Cali.

the purpose and means of processing, and maintain relationships with end users. Modern comprehensive privacy laws, including the GDPR and ADPPA, all recognize a distinction between controllers and processors, and that tailoring legal obligations to a company's role enhances privacy and data security for everyone.

Third, on topic of AI systems, getting governance right in this area requires a thoughtful, clear eyed approach that protects consumers and accounts for the state of the field. I encourage the commission to look to the ADPPA, which issues the premature third party audit requirements that instead requires companies using high risk AI systems to carry out impact assessments prior to use.

Impact assessments are a tried and true way for companies to document how they identify, test for, and mitigate risks posed by technologies. As AI technical standards continue to develop, impact assessments represent a pragmatic way forward to promote AI accountability and encourage the use of trustworthy systems. I will end by thanking commission for organizing this public forum. Workday looks forward to

and continue growing America's innovation economy. Thank you, commissioners, and all the speakers. We look forward to working with you further.

Peter Kaplan:

Thank you, Carl. Our next speaker is Nora Benavidez. Nora.

Nora Benavidez:

Thank you. Thank you, Chairwoman Khan, commissioners, and the entire FTC staff for hosting this forum. I'm Nora Benavidez, senior council at the nonprofit Free Press, where we work on media and technology reforms to advance a more equitable society.

Data about what we do, with whom, and where is in the hands of often unscrupulous tech companies,

Andy Jung:

Hello, my name is Andy Jung. I'm a legal fellow at Tech Freedom, a nonpartisan technology law and policy think tank. In question 26, the advanced notice of proposed rule making asks, "To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance innovation?"

from or even informed of the secondary sale of their data. As Ms. Gray mentioned, this secondary usage must be regulated.

I come from a background in the commercial surveillance industry, and can tell you from firsthand experience, the tracking and protection practices required for transparency aren't prevalent today by design. It's easier for these platforms and first party data collectors to say that once data leaves their silo, it's not their problem to protect the consumer. This is reflected in the typical privacy policies we see in the industry. These policies are simply there to provide legal cover for the data collectors, rather than truly informing the consent being given.

On top of that, these policies are rarely, if ever, set in stone, so platforms such as Facebook and Google have continually decreased consumer protection as they've grown and gained traction. They know full well that users won't read these policies, and they can put whatever they want in them. This is an anti-competitive cycle that Mr. Kent mentioned, but it's also a deceptive consumer relationship.

Peter Kaplan:

Thank you, Joshua.

Joshua McGrath:

Yep.

Peter Kaplan:

Our next speaker is Jean Ross. Jean. Jean, are you on? If Jean isn't on, then-

Jean Ross:

I'm here. So sorry.

Peter Kaplan:

Oh, okay. Gau 329.57 Tm0 g0 G[(Oh, o)5(k) TJETQq0.00000912 0 612 7920() TJ2 0 612 792 re0 6.04 TQah.04 TooouETehyyf5

2mOha1 638.3ID 5>BDC q0.00000912 0 612 792 reW*nBT/F2 11.04 Tf1 0 0 1 72.7s155.7F2 11.04 Tf1 0 0isn't on, then

are a lot of free options with little visibility to the third party that keeps that company financially viable. I have signed up for many of them. They take you to your patient portal where that portal gives you one final warning, and even as a nurse, I'm unsure where exactly my health data is going and how it is being used to profit that company.

And lastly, my intent of getting health data into one secure place for families will be to educate, predict, and connect health consumers to resources and recommendations to achieve their health goals. This will require analytics on health data, so clear guidelines from FTC and best practices on how to engage with consumers and cause the least harm will be so appreciated, recognizing the intent of most co-founders is to use analytics to provide value and grow their user base. Thank you so much for your time.

Peter Kaplan:

Thank you, Jean. Our next speaker is Janet Haven. Janet.

Janet Haven:

Thank you. My name is Janet Haven. I am the executive director of Data and Society, a nonprofit independent research institute. We study the societal implications of data centric technologies and automation, and translate that research into actionable just policy recommendations.

As multiple presenters noted today, transparency documentation is a necessary component of preventing unfair and deceptive practices in the data industry. To combat discrimination and bias, the FTC must push towards universal obligations for transparency reporting in AI and ML product development, exemplified by tools such as model cards and data sheets for data sets. Such documentation would ultimately enable the adoption of auditing practices that are common in other industries, but largely absent in data driven tech.

Yet, research at Data and Society and beyond has demonstrated that transparency is necessary, but not sufficient to bring about a fair and just data ecosystem. Transparency documentation means little if

dispersed society, which also need to be balanced. In any balance relating to privacy, it's important to what safeguards in place. Existing data protection regulations such as those referred to, things like