Commercial Surveillance and Data Security Rulemaking – September 8, 2022

Chair Lina Khan:

Good afternoon, and welcome everybody to the FTCs Public Forum on Commercial Surveillance and Lax data security practices. As you all know, last month the Federal Trade Commission kicked off a proceeding to examine whether we should issue rules addressing data practices that are unfair or deceptive. Today's public forum is a key next step. As part of our effort to gather public input, we have today invited industry representatives, consumer advocates, researchers, and the broader public to share their views and experience with us. This public input will directly inform our analysis and thinking as the Commission determines how to proceed, both with determining whether to proceed with a proposed rule as well as what form a proposed rule could take. We've received significant interest in today's public forum with a sizeable number of people signing up to share comments. I think this outpouring of interest really underscores how critical and urgent these issues are to people's day to day lives today.

We know that today's digital tools can deliver huge conveniences, but we also know that these tools and the business models that underlie them can also be used to track and surveil individuals in entirely new ways. Firms are collecting data on where we go, what we read, who we meet, what we buy, and research has suggested that many Americans have limited insight into what information is being collected about them and how it's being used, sold or stored, and that even when people do know, they may find themselves with no real options but to go along with these practices. As more and more sectors of the economy continue to become digitized, these practices are touching more and more of our daily lives, be it in healthcare and housing or in education and employment. The huge amounts of data that are being collected and stored has also coincided with a growing number of data leaks and hacks, security vulnerabilities that can leave people's sensitive information exposed, leading them to lose money, have their identity stolen or face discrimination or other types of harms.

So the stakes with these business practices are high and the FTC has a long record of using its law enforcement tools to combat these types of commercial surveillance and lax data security practices in instances where they are illegal. With this rulemaking proceeding, we are now seeking to determine whether unfair or deceptive data practices may now be so prevalent that we need to move beyond case by case adjudication and instead have market wide rules. In order for the FTC to be able to issue rules in this area, there are certain legal requirements that we will need to meet. There are certain legal tests that we must be able to meet in order to show that a particular data practice is unfair or deceptive and that it is prevalent. The public record that we build, both through the comments that we receive in our public docket as well as through the discussion and comments that we hear today at this forum, will be 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 public interest that we have already received in this proceeding, and so I really want to encourage anybody who could not join today or who's inspired by today's discussion to also submit written comments at regulations.gov on or before October 21st of this year.

Democratizing this process and structuring it to enable broad and wide public participation has been a key goal of ours, and so that's why we're hosting this virtual public forum that will be recorded and submitted as part of the official record for this rulemaking proceeding. Today's forum will start off with a brief presentation from our Office of General Counsel on the rulemaking process so that everybody is aware of what types of information and evidence the Commission is seeking at this stage of our rulemaking proceeding. We will also be hosting two panels, one with consumer advocates and one with representatives from the industry, to explore a variety of issues that we cover in the ANPR, including best practices, the impact of commercial surveillance practices on consumers, risk that these practices pose to specific groups, as well as interventions to address algorithmic discrimination.

We hope that these panel discussions will help spark broader public interest and discussion on the ANPR topics and help inform some of the comment submissions. We will also be hearing from my colleagues, Commissioner Slaughter and Commissioner Bedoya. I'm so, so grateful for the expertise and experience that they bring to this proceeding. Commissioner Slaughter has been a critical leader at the FTC for charting the path forward on crafting rules in this area, and Commissioner Bedoya, who joined us just a few months ago, has long worked on and thought about these critical issues, and so we're just really lucky to have their expertise and experience and leadership as part of this process. The forum will conclude with remarks from members of the public that have signed up to provide public remarks.

Lastly, I'm so grateful to the agency staff that have already poured so much work into this ANPR and into putting together today's events, as well as my colleagues across the Commission for their engagement and input. Working to protect Americans from unlawful commercial surveillance and data security practices is critical work and we're really looking forward to undertaking this effort with both needed urgency and rigor. So I will now turn the floor over to Josephine Lui, who is Assistant General Counsel for Legal Counsel in the FTCs office of General Counsel, who will provide a brief overview of what's known as the Mag-Moss rule making process and will share what the Commission is seeking at this stage of our proceeding. So Josephine, over to you.

Josephine Lui:

Ladies and gentlemen, thank you very much for joining today's public forum. My name is Josephine Lui and I'm in the FTCs office of the General Counsel. I will be speaking briefly on the rulemaking process for the potential commercial surveillance and data security rule. Next slide, please.

Chair Lina Khan:

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 young children or teenagers, advocates, small businesses, large businesses, trade associations, non-profit organizations, government officials, researchers, academics and so on. Having many comments from individuals, groups and businesses will help the agency make a more informed decision. Individual comments from a person or organization expressing that persons or organizations specific point of view are often more impactful than group comments signed by multiple people or organizations.

The ANPR lists 95 questions that the Commission is interested in. Even if the Commission ultimately decides not to issue a rule, the responses to these questions may help with the Commission's enforcement work and may be helpful for other policy makers too. I want to highlight three questions in particular. First, question number three asks which commercial surveillance practices are prevalent. Responses to this question may help the Commission focus on particular areas of concern, either in enforcement or in rule making. To move on to the next step in the rulemaking process, the Commission must have reason to believe that the practices that are the subject of the proposed rule making are prevalent. Second, question number seven asks in part, how should the Commission identify and evaluate these commercial surveillance harms or potential harms? Responses to this question may help the FTC identify and address specific and distinct ways that consumers are being harmed. Third, question number eight asks which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions? Responses to this question may provide evidence in areas where the Commission has less enforcement experience.

It is particularly helpful when comments include supporting material, such as empirical data, findings or analysis of published reports or studies by established use organizations or research institutions. You can file comments online at regulations.gov. You can also read comments submitted by other people at regulations.gov. Next slide, please. As I said earlier, the ANPR is just the beginning of the rulemaking process. The FTC will read and consider all comments when deciding what to do next. If the Commission decides to move forward, the next step will be a Notice of Proposed Rule Making, or NPRM.

The NPRM will include the text of the proposed rule, a description of the Commission's reasons, an invitation to comment on the proposed rule, and an explanation about how to request an informal hearing. The informal hearing provides people with an opportunity to present their views orally. The informal hearing can also be an opportunity to resolve disputed factual issues. To sum up, there will be several more opportunities for the public to weigh in, if the Commission decides to move forward with this rule making. Please file your comments on the ANPR by October 21st to ensure that the Commission has the benefit of your input when deciding what to do next. Thank you. The next speaker is Commissioner Rebecca Slaughter, who will provide remarks. Commissioner Slaughter, over to you.

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 try to be concise in order to spare you an unstable connection. So I want to start by thanking Chair Khan for organizing this public forum, and thanking Josephine and your colleague Austin in the Office of General Counsel and the staff throughout the agency for all the work that you've been doing to help lay out the substance, the substantive procedural steps that we need, and help explain that to the public. The kind of public engagement we're seeing today is vital to helping the FTC understand the state of commercial surveillance in our economy, the shape of the digital market for personal information, and the kinds of harms that people experience from data collection and the tools that are built from that collection.

Public consultation is an intrical part of the FTC rule making process, and I'm happy to see so much interest in this forum. As I said after the Commission vote on the ANPR, I support strong federal privacy legislation, but until there's a law on the books, the Commission has a duty to use all the tools we have to investigate and address unlawful behavior in the market. Kicking off our rulemaking process on data abuses and convening this first public forum shows we're taking that responsibility seriously. Our open comment period on commercial surveillance and data abuses gives us the ability to hear from the public about the kinds of harms they see in the market, how those harms affect their lives as consumers, workers and potential competitors to entrench businesses. As I hope you've all now seen, the ANPR asks questions related to data minimization and the unfettered data collection we see in the market, how digital tools may discriminate based on people's protected characteristics, especially with regards to AI and advanced algorithms, and it asks questions related to young teens, kids who have aged out of the protections in the Children's Online Privacy Protection Act but aren't yet able to make consequential decisions about their digital lives.

Public and expert participation today and throughout this comment period is important. It will inform whether or not the Commission eventually proposes rules, what practices those proposed rules may address, and the kinds of actions we may take to effectively deter that harmful conduct. I have not been shy in saying that where we see unlawful conduct, the FTC has a duty to act. This is a truly open inquiry and I encourage commenters to critically examine prevailing business models that may be the source of harm. I also encourage industry to constructively engage in this process and inform the Commission about how we may better deter unlawful conduct, protect people's rights, and ensure that any possible rules are effective and not just a burdensome compliance exercise.

Opening a record like this is important for the FTC as an institution too. The Commission is showing that we're no longer shying away from using all the tools we have available to deter unlawful conduct in the market. The work the Commission has done over the last year and a half should be read as a bookend to the long era of not appropriately exercising our rulemaking authorities. I'm so grateful to the Chair for launching this proceeding, and to her and my colleague, Commissioner Bedoya, for their particular vision, their perspective, and their expertise. It really is a pleasure to work on these issues with people who are so thoughtful and engaged and knowledgeable and in different ways. We really benefit from that.

And I want to echo the Chair's thanks to all the staff throughout the agency for their excellent work on this project, up to this point and on an ongoing basis, because as we all know, the work is just getting started. I'm looking forward to hearing from the public today and especially from the folks we rarely see before the Commission. We have a lot to learn from your experiences and expertise. And now it's my pleasure to introduce us, or segue us, into the next section of our program. Professor Olivier Sylvain will be moderating our first panel on industry perspectives on commercial surveillance and data security.

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 we touch on today. The first one is about best practices and business model. So actually I'm getting ahead of myself. I want to get to these questions, but I think we have to leave time for our panelists. So let's get, in order of appearance in the program, let's get Jason to start with his three minute introduction.

Jason Kint:

Great, thank you. Can you hear me okay? Good afternoon. Thank you for having me. I want to touch on three points regarding digital advertising. First and foremost, from the consumer perspective, not all data collection and use are the same. Consumers expect the sites and apps they intentionally visit to collect and use data about them, to remember their settings and tailor their services among other things. Using data in these ways where it's collected tends to meet with a consumer's expectation. If they don't like the way it's used, the consumers are likely to show this dissatisfaction by taking their business elsewhere, assuming they have choices, more on that in a second. However, collecting data in one context and then using it in another, such as the case with behavioral advertising that collects data over time across multiple sites owned by multiple companies, tends to violate consumer expectations.

Consumers may not be aware it's even happening, and even if they were, they don't have effective mechanisms for stopping it today. As much as we have antitrust concerns about Apple, we credit Apple for moving forward on tracking prevention in 2021, much to the chagrin of Facebook and its surveillance business model. Many of the harms to consumers originate from this kind of out of context data use, which again brings me to my number two. Many in the industry will claim that behavioral advertising is the golden goose which fuels the internet, but the truth is publishers only see a three percent increase in revenue, according to research from Alessandro Acquisti who extensively studied the impact on overall revenue. Automation, including the buying and serving of advertising, is good for industry and consumers as it unlocks efficiency and lowers barriers to entry for new players. But behavioral advertising fueled by commercial surveillance primarily benefits the dominant platform companies who can see across the web and our lives.

Third, there are many questions in the FTCs notice about what obstacles and barriers may exist in addressing the problems with commercial surveillance. From my perspective, the main obstacle is the advertising industry has a competition problem. In today's marketplace, the terms of data use are established by and for the benefit of a few companies which enjoy a dominant market position. Even when a new law is passed, how industry complies with the law is often driven by these dominant companies. For example, two weeks before enforcement of GDPR, Google announced how companies using their services would need to comply with the new law. In short, companies would need to get consent on behalf of Google, although Google would not share how they'd use the data, and any company using Google services would shoulder all the liability for any subsequent violation of GDPR by Google.

Or in the case of Facebook, their Cambridge Analytica scandal continues today to reveal eye popping discovery in lawsuits over how they mined data while at the same time poorly controlled third party use of it. No publishers received a dime of Facebook's $5 billion settlement for abusing data and consumers. As the FTC moves forward on privacy rulemaking, we believe special attention needs to be paid to the dominant companies in the ecosystem. Thank you again for including me on this panel. I look forward to discussing these issues in greater detail.

Professor Olivier Sylvain:

Thank you, Jason. Let's now turn to Marshall.

Marshall Erwin:

Thank you for the opportunity to speak and express Mozilla's views today. We think this is really a critical process that you've kicked off, and one that we hope to provide some meaningful comments and help shape the outcome. First, I want to talk a little bit about the role of web platforms and browsers in protecting privacy and what that means for the role of the regulator as well. So we think that strong privacy enhancing features and products such as those that we built into the Firefox browser are really critical.

Because to the extent that sort of web browsers or web platform to provide a permissive operating environment, what that does is it leaves consumers open to essentially to attacks by a huge diversity of parties that can really put consumers at risk. That's bad for consumers, but it also makes the challenging operating environment for regulators who are then going to be underwater by that large diversity of attackers. So we really sort of stand by and are quite proud of the work that we've done in the Firefox browser and applaud the work of some other browsers in the space as well. At the same time, we also know that a large number of companies don't take the approach that Mozilla does to privacy, and more than half of consumers today are using browsers that don't have strong tracking protections in place or strong privacy protections. At the same time, even if those browsers did have a strong set of privacy protections, we know that technical solutions really aren't enough. There's a set of problems that technology alone will not solve.

And so what we want to see is platforms like Mozilla working to protect privacy, but also in parallel, regulators taking action to create cost against bad actors in the space, and that's what we think is really necessary to make meaningful change here and protect people's privacy. A few areas that I want to highlight where we think would be really worth exploring and developing a strong set of rules. First I want to highlight dark patterns or malicious design patterns, which are really pervasive across the internet today and quite problematic. Scenario where consumers are essentially being tricked into handing over their data. They understand and intuitively know that this is happening, they feel like they're being abused, but because they're being tricked, they really aren't empowered to do anything about it. And again, at the same time, there's not much that a browser maker can do about this as well when our consumers visit a website and are tricked into handing over their data. This is just bread and butter deception that we feel like there's really room for a strong regulator to engage and do something about.

Another area that we want to explore is harmful uses of data once that data has been collected. So the core challenge we see online today is that advertising platforms have developed very sophisticated targeting technology. And that technology does have some benefits, but it also is clear it has real costs and drawbacks. What that technology does is it allows people to sort of segment their audience and channel messages and content, in some cases to the populations that are most vulnerable, and that is kind of the harm facilitation mechanism that we see happening on the web today, and a set of rules really need to address that harm, both the harm that happens when the data is collected in the first place and the harm that happens when that data is used in abusive ways.

And finally, we want to highlight that it's important that there be mechanisms to provide greater levels of transparency into what is happening on major platforms today. Because these are private platforms and what is happening on those platforms is so highly targeted, everyone has an individual experience, and so we can see this harm happening largely anecdotally, but the system is opaque and it's hard to show systematic harm. And as a result, what we don't want to see happen, for example, is a regulator like the FTC having the ability to bring an action based on algorithmic discrimination, but not having the degree of transparency to even show that that discrimination is happening in the first place, so it's really critical as part of this rule making to think about the mode of access to gain transparency into the harm that's actually occurring.

So I'll just close out by saying, in our view privacy on my online is a mess today. Consumers are stuck in this vicious cycle in which their data is collected, often without their understanding, and then used to manipulate them. We see this rule making process as a real opportunity to break that cycle and we look forward to the outcome of this process. Thank you.

Professor Olivier Sylvain:

Thank you Marshall. Paul Martino.

Paul Martino:

Thank you for inviting me to appear today. I'm Paul Martino, Vice President and Senior Policy Council for the National Retail Federation. NRF is also a founding member of the Main Street Privacy Coalition, a broad array of 19 national trade associations representing Main Street businesses that together employ over 34 million Americans and produce over one fifth of our economic output. We believe three key principles should shape the Commission's proposed rule if they proceed. You will notice that they are rooted in the retail adage, "The customer is always right."

First, consumers should be free to make informed choices about how their data may be used to benefit them. Retail customers increasingly want product offerings tailored by them and related to their past shopping activity to help them make choices about future purchases. Retailers should be allowed to respond to these consumer demands. On the other hand, consumers should be equally empowered to exercise rights to opt out of data driven services and retailers make these available to customers. Put simply, consumers should be free to make choices that suit them best.

Second, businesses should be permitted to use data responsibly to benefit and serve customers as they choose to be served. For example, the EUs General Data Protection Regulation, or GDPR, provides lawful bases to use personal data, including when a business has a legitimate interest in serving customers. Many American consumers value hearing from retailers who make them aware of new offerings that may be of interest. These data driven communications help retailers build trusted relationships with customers and earn more business. Third, federal privacy regulations should be both customer centric and risk based, and they should apply to all businesses that handle consumer data. Retailers directly serve their customers in first party relationships that present lower risk because they depend on trust earned and maintained over time. Retailers work to develop long term, mutually beneficial customer relationships because they want to meet their customer's needs now and serve them in the future.

Retailers need to maintain those relationships to succeed in the marketplace, which is the strongest possible incentive to use data responsibly and as consumers expect. By contrast, third party uses of personal data by businesses unknown to consumers creates a much greater risk of harm, especially if used for purposes consumers do not expect or approve. Third party businesses lack the incentives of customer serving businesses to use data responsibly and in alignment with consumer's interest, because they are not in pursuit of long term customer relationships with the consumers whose data they collect and process.

The Commission should calibrate its regulations to be proportionate to the level of risk from varying business practices that use consumer data. New rules should not unduly burden customer serving business models that use data responsibly and consistent with consumers expectations and choices, and they should not ignore higher risk third party data practices, especially those that leave consumers in the dark about who is using their data and for what purposes. We appreciate your consideration of our views and the opportunity to participate in today's panel.

Professor Olivier Sylvain:

Thank you, Paul. Rebecca Finlay.

Rebecca Finlay:

Thanks very much. It's a pleasure to be here. Hello all, I'm Rebecca Finley. I'm the CEO of the Partnership on AI. We are an independent nonprofit organization working to advance AI equity and responsibility in the public interest. We connect today about 100 partners in 14 countries that stretch across academia, civil society, media, and industry. And we were created to, in the first instance, identify the emerging trends in AI research and development, convene diverse groups of study and develop open source tools, recommendations, and resources to advance AI that centers people first. While I'm happy to be here today, I want to clarify we are not an industry or a trade group nor an advocacy organization. We aim to change practice, inform policy and advance understanding, and it's great to see some of our partners participating on both of today's panels. When I think about the questions and the notice provided by the Commission, there are three key takeaways for me.

First and foremost, the conversation is timely and it is important and it is urgent. Secondly, there is clearly no magic solution. This is going to require a whole of society, be it policy, practice and citizen action, as well as innovation and coordination at the international, national and local levels. And we need to get started, despite the uncertainties and complexities within which we're operating. There are two statistics in this year's AI index, which is based at Stanford, that I often find myself going back to when I think the context within which we're operating.

First of all, this year it was reported that private sector investment in AI grew to 93.5 billion internationally. And not only is that a large number in and of itself, in terms of the private sector, but that is both more than double and more concentrated than that reported in the previous year. So we are seeing a real acceleration of the use of algorithmic decision making systems based on training data sets across all sectors of the economy, and therefore evaluating both its potential benefit but its true and potential adverse effects and harms on citizens and consumers and workers is truly urgent.

And as jurisdictions around the world have discovered, as we've seen in the EU, most recently in Canada, and also now emerging in the UK, we need both better policy making to set guardrails and have clear rules of the road, and better practice in the design and deployment of AI in industry and in government to advance innovation and protect the human rights of all individuals. Businesses and regulators need to prepare for and respond to the different ways that AI systems work and the opportunities and risks therein, both in terms of how algorithms work when optimized for certain goals, as well as the data they are trained and deployed on and the potential biases and errors they're in, and the way in which AI systems both focus on individualization and also generalization across groups, and this is particularly noteworthy when we think about informed consent and privacy.

The work that we're doing is exploring how AI systems can be designed and developed, who is around the table amidst an information asymmetry, what are algorithmic fairness

Rebecca Finlay:

... fairness and privacy in an AI context, and how do we balance the need for both innovation and consumer and worker protections, and the implications in today's changing international policy context. We welcome the FTC's notice, particularly the request for comment on rules and jurisdictions outside of the US as a way to learn what has and hasn't worked and to support global interoperability. I'm really happy to be here to share some of the insights and recommendations from the work that we've undertaken with our partners, and I'm looking forward to finding ways to continue to support this conversation and that of the work of organizations and individuals in attendance today. Thanks very much.

Olivier Sylvain:

I'm grateful to all our panelists for very helpful three-minute introductions to basic ideas you all are thinking about. I think you've set the stage for a nice conversation and opened our own consideration in context of the rule-making proceeding very well. I already previewed where the first question was going, but what's interesting is that I think all panelists actually touched on this a bit in their remarks.

This first bucket of questions... I say bucket, this is the first question is, what are best practices? I mean, we can drill down a little bit, and I think actually Rebecca, I'll start with you. You know you've finished last in the introduction, but it's a good segue from what you were describing. What are best practices or potential business models that companies have developed to mitigate against consumer harm and protect data?

I offer this question because I think we all recognize that there's a lot of opportunity in the things that companies have learned, that industry has learned, over the past few years. I think all of you could speak to this. By the way, I use the language of harm in this question. We're not here going to evaluate how to measure that. I think we can have disagreements on what that is for this first question. We'll turn to that later on regards to potential rules. But right now, assuming that companies recognize that 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 of web browsers, but more generally, is there something you can share with us now with regards to the best practices or business models that help to mitigate against harm?

Marshall Erwin:

Yeah. I'll say, I want to take this question in a slightly different direction for a moment, because I think we're going to spend a lot of time expressing our views on issues like privacy and what we do as a company to protect our users, those best practices. But as chief security officer, I want to highlight, there's a number of questions that the FTC has asked about data security that I think are actually really critical as well. That's an area where we have seen a consensus set of best practices emerge that are important to call out and consider as part of this rule making. I'll just spend a few brief moments on those right now.

There has, like I said, been this sort of consensus set of practices emerged that are really, I think, universally accepted, although not universally adopted. These are things like having a basic security program, having incident response processes in place, having a basic set of security controls, having risk assessment processes in place. All of these are really critical to protecting data once it has actually been collected. I think these are fairly consistent best practices that you can see in a number of regulatory frameworks that have come in and do existence around the globe, consistent with the safeguard rules that I think the FTC already applies and should serve as a really good model for how the FTC should be thinking about rulemaking is specifically regarding data security.

I'd really encourage everyone to think about those requirements and how they might be mapped on onto this rulemaking. And then, finally to call out a few specific security safeguards that I think are worth highlighting, just basic sort of encryption in transit. Every company should be doing that. If the company isn't doing it, maybe you should think about not using their products. And then, basic access controls to govern data MFA, strong password requirements. Again, these are the baseline things that every company should be doing that can really buy down a huge amount of risk for consumers.

Again, if these things aren't in practice at a company, it's worth scrutinizing that company much more closely. I'll let somebody else-

Olivier Sylvain:

Yeah. Marshall, my connection has obviously been unstable. I regret that I didn't hear the end of what you were saying, but sounds like you were going to moderate in my behalf. I think I saw Jason, your hand was up next. Yep.

Jason Kint:

Yeah, let's jump in for a second. As context, DCN, who I represent, is a large group of premium publishers, thousands of brands across news and entertainment. But what matters here in terms of best practices, and I'll really speak to what I see as emerging best practices that are happening now. I mean, there's clearly a gap in reaching consumer expectations that's there, and now, we're trying to address it. All of our members have direct and trusted relationships with consumers, so they come to them and their brands to be informed or to be entertained, and they make that choice to intentionally interact with them.

With that in mind, the issue of tracking and data collection use by other parties that you're not choosing to interact with is a really important issue. I'm seeing a lot of emerging best practices coming out of the west, both from technology and policy. I mentioned Apple with tracking prevention in the browser, the operating system. I think Firefox also had it for a long time for Mozilla, Brave. You have tech solutions. You also have the global privacy control, which is in the draft rules that are being pushed forward in

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 be an exhaustive list, but I think these are things for staff to consider in terms of what our best practices. Let me just start with... Some of these might be obvious but they are innovations over the last decade, or I should say if they aren't recent innovations, they've been more fully subscribed to over the last decade. But enabling multifactor authentication for consumers to access customer accounts, but also for company employees to access key company systems, especially those with consumer data. Implementing antivirus and anti-malware software in business systems, developing and implementing strategies to consistently update and patch systems. We all remember the Equifax breach and what led to that.

Maintaining backups of data to restore systems if necessary. This is a best practice with respect to also being able to have some options if there's... I'm thinking of a malware attack that creates some kind of demand for information and I'm spacing on the name, I apologize. And testing the ability of employees to detect recurring threats with phishing simulations or tabletop exercises. Many retailers engage in these tabletop exercises on an annual basis to test the response systems if there's a potential breach. I'm sure Marshall, as the chief security officer, is very familiar with those. I do want to touch base on one thing. Jason mentioned the global privacy control. I do want to mention that there are some concerns we have with that, because there's the potential that the use of a global privacy control could actually frustrate consumer choice and frustrate business' efforts to serve their customers.

I'll just point out one example. The privacy control is like a setting in the browser. I know I'm simplifying this, and I apologize, Marshall, but it sends a signal that businesses are supposed to respond to and execute and opt out of various things, whether it's an opt out of targeted advertising or whatever in this case the state law requires. We have a concern that if customers have already opted into something, like a customer loyalty program, that gives them discounts or provides promotions, or if a retail business is looking at global privacy controls and they get a general signal and opt out from a browser signal that says, oh, take that customer off this list. But if they've already previously signed up for something, we're worried about how that is handled. I know that regulations are being considered in Colorado and more work is being developed, but we think one principle that should take a hold is that if there's a specific choice made by a consumer... Again, customers are always right, but if they've already chosen to participate in some way, we think that specific choice should override a general choice.

The general choice might be good as certainly as a default. Certainly, it's much less burdensome among consumers to be able to click one box in their browser and make sure that they're opted out of, let's say, targeted advertising if that's what they want. However, we're concerned about what it means if consumers have already made choices at particular brands or companies that they want to be more engaged with. So, I'm not the expert on the global privacy control, and I'll leave it to Marshall and Jason to add more to that, but I just want to raise that concern.

Olivier Sylvain:

Thank you, Paul. Marshall, your hand was up, and I will leave the global policy control question to maybe a little later. Paul mentioned backups and actually segues a little bit with a question I was setting up, and that is retention and best practices in that regard. I don't know if that's what you're going to speak to, but maybe since Paul was drawing you in, maybe there's something else that you might want to add in response.

Marshall Erwin:

I was going to comment on the global privacy rule, but I think we can avoid that. It's fine. Going back almost 10 years, we established what we called the Mozilla Data Privacy Principles. One of the key principles there was data minimization, which I think is essentially another way of talking about data retention. Data minimization being you only collect what you need, and then you get rid of it when you no longer need it. Really critical, I think. That's frankly the most important thing that Mozilla does as a company. We do collect data from our products. That data is really important for us to build a better product to know how people are using it and to actually build what our consumers want. But we work really hard not to overcollect that data and then to get rid of it once we no longer need it.

That's actually probably one of the most fundamental things that we have been able to do that minimizes risk, direct risk to our users from Mozilla zone data collection. So, I'm just a strong champion for data minimization, limits on data collection, when it's not going to be used directly to benefit the consumer. And then, data retention requirements such that the data isn't retained for longer than needed.

Olivier Sylvain:

Paul, I see your hand up, but in the interest of time, I want us to move to the next question. I promise we'll to the... I think I'm going to be able to get the global policy control question, and actually maybe with regards to the second question. Paul, you'll be to first answer to the second question. How's that? Rebecca, I haven't forgotten about you. You'll be up next. But basic question is how do we incentivize? How could the commission incentivize companies to mitigate against harms, given that obviously bad things are happening and the commission does a lot of different work as you all know, but are there things we can do, short of rule making, given the tools that Chair Khan mentioned that are available to get companies to make sure that harms aren't as rampant as they may be?

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 under the age of 18 in the UK. Of note, it applies not just to UK-based companies, but also to non-UK companies who process the personal data of children based in the UK. It was established, as I said, last year. They've already come out just recently with their first year report in terms of their impact to date and just some key elements around transparency and what does it mean to provide privacy information in a way which is understandable, concise, prominent, and clear in a language that is suited to the age of the child who is using the service.

There's also data minimization standards that are included therein. It came out of a consultative process that was done with many groups across the organization. So, understanding these dimensions, understanding what has worked, understanding the emerging legislation coming out of the EU right now and other jurisdictions is a critical role I think that the commission could play in participating and engaging with industry and other stakeholders around some of these questions.

Olivier Sylvain:

Thank you, Rebecca. Let's go to the third question, which gets to the rule making. This is where it gets harder, admittedly. The reason is because, in spite of the efforts, Paul, that you described, and Rebecca, you allude to. I mean, the learning that companies have engaged in. Harms persist. Again, we can have some disagreements about relative harm compared to benefits, but harms do persist. I think you all observe that and you all recognize that in your opening remarks. Are there rules that you'd like to see that would clarify what the FTC Act forbids? Here I think you can assume, you can talk about what the harms are in this context, right? Again, this is not about an agreement about it, but you expressing, based on your experience, whether rule making would be appropriate.

I just want to throw out here the question of choice and given that the consumer's always right. In some ways, is intention with an observation, Marshall, you made about the opacity of the ways in which companies make their decisions. Jason, you alluded to this as well. So maybe, actually, let's turn to you, Jason, on this. I mean, the commission and the NPR references data security as an area of interest in regards to rules, algorithmic discrimination, a couple of you have mentioned. Children's privacy, I think all of you have spoken to. We can also mention workers for what it's worth. So in the interest of predictability for companies and consumers and given that harms persist, are there rules here that you would like to see?

Jason Kint:

I guess I still would still focus on context and those sorts of activities within the choice of visiting a website or app are very, very different than when it's tapping out of context. And so, any sort of way to use the existing tools or new rules in order to limit that out-of-context tracking by parties you're not choosing to act with, which I've said before. I just would really amplify the heightened level of limitations or risks that go with it by companies that are able to see [inaudible 01:01:51]-

Olivier Sylvain:

Jason, sorry to interrupt. I think I know what you mean by out of context. But you're saying something, you're actually packing in a lot in that idea. Can you unpack that for us?

Jason Kint:

Sure. No, I appreciate you asking me to. If you're choosing to visit a website, whether it be a retail website or, in my case, my membership news and entertainment company's website or app, using that data in order to make recommendations on the product or to target advertising on the product, that's in the same context. The data's being collected while you're choosing to use that app or website, and it's 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 problem here when we think about what needs to be done to incentivize an ecosystem to move in another direction. That's the problem there is. Right now, the bad behavior is too easy and there's no consequences for it. Internet is fundamentally consequence-free zone. I think that's really where, when we think about the rule making and potential penalties that violations of the rules might entail. That's really where the value is here, and I think where the potential is to really move the needle in a meaningful way. That's where I think that cost piece really comes in.

A lot of what we do in the browser is sort of crack down on some of the behavior that Jason was describing. What we think of as cross site tracking, which we can, fundamentally, users don't understand it. It's opaque. It violates their privacy. What we see is clamping down on that, decreasing the benefits fundamentally of commercial surveillance. And then, if the regulator can increase the cost of that, I think we can meaningly move with the deal.

Olivier Sylvain:

Marshall, when you say increased cost, you're, you mentioned penalty. You're not just talking about penalty, right? I mean, or are you? I heard you initially talking about baking in obligations that make it costly to endeavor, engaging some kind of commercial practice.

Marshall Erwin:

Yeah. I mean, I actually am talking about penalty. I think that fundamentally is what moves the needle in a meaningful way. I think, again, how it work, which kind of increases the cost by making commercial surveillance practices less efficient. That's actually what we're doing in the browser, although that's not how we talk about it. I think that's what we are doing. But on the converse side, actually creating a real cost when there's bad behavior, and financial penalty is a meaningful way to move the ball.

I do want to go back to the child safety question, which was raised. We think about getting into a little bit more specificity. Kids right now are being harmed by this pressure cooker situation that we see 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 handle consumers data appropriately. And we think those market incentives, at least in our business can be even more powerful than say regulatory incentives because if your success is dependent on developing trusted relationships over time and maintaining those, then you have to use data responsibly, or you will suffer the consequences in the market, I'm not saying that what applies to retail is appropriate for everyone else, but I do think just going back to the previous comment about... Or my opening statement about risk based, the commission should assess the different risks based on different business models, certainly the context is important and certainly the level of competition is important to that equation too.

You don't have maybe the informed choice that I talked about if it's out of context or in a market that suffers from lack of competition, when you have much more competition and much more information for the consumer, then I think the choice is informed and works better. So thank you for the chance to explain those thoughts on this before we move on to other questions.

Olivier Sylvain:

No, great. And that's actually a segue for, I think our last bucket of questions, if you will, our next last question. And I'd like to talk about risk if you don't mind. And that is so one of the things the NPRM does is posit that potential consumer harms may flow from market incentives, namely that companies have the incentive to hoover up and monetize consumer data given the few limits there are. And a couple of you mentioned it, Jason, I think you mentioned it at the outset. And I mean, I think everyone has recognized that. And just to speak to your point, Paul consumers surrender their data. Sometimes they feel like they have to even the context of competitive environment for $0 in order to receive these services. But of course there's a transaction network that most consumers don't see. Collection monetization doesn't always or necessarily cause harm, consumers keep coming back. I think we all recognize that there are clear benefits in services and many of us patronize, but it potentially increases the risk of harm.

And actually, Paul, you talked about this regards to some of the things you said. Actually, Rebecca, I want to maybe just address this to you. I don't know if you've given some thought to this, but with regards to a rule, with regards to a rule, now we're not talking about rules now, if the commission was to pursue a rule addressed to business models, how could it assess the cost of the service being provided for free due to targeting, ads, given alternative business models that would allow these services to be free without that kind of targeting or in some other way? I've called on you Rebecca and maybe if you want to jump in on this, but I think everybody has probably given some thought to this. Rebecca.

Rebecca Finlay:

Sure, I'm happy to jump in. Can't speak directly to the rule just because that's not been our area of focus, but I do think the point you raised about risks and there's a question around the notion of algorithmic discrimination and algorithmic fairness. And one of the ways in that has been positive to try to deal with that issue is to collect more data and to collect more data about demographic groups who are inherent within data sets in order, therefore to create data sets that are potentially more fair. And we have definitely done some work in this area, really looking at and challenging the question of data being the solution to the question of algorithmic fairness. And it really is when it bumps up against the question of privacy, which is, I think also important to this conversation as well. So we've had several conversations with experts and with our partner [inaudible 01:14:35] to understand better, what are the risks and trade offs associated with the use and non-use of demographic data and algorithm systems and that directly relates to the question of privacy.

And the first concern really is about collecting or using sensitive demographic data and the risks from breaching individual privacy, because we know in the way in which those certain groups have been discriminated again, based upon that group level sensitive demographic data. And there are methods 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 it's plain and I mean, it'd be nice to know what the low hanging fruit is here for potential rule if we pursue that line. Jason.

Jason Kint:

As context, because I've talked a lot about advertising premium publishers still get most of their revenue from advertising or a lot of it, but subscriptions are super important, eCommerce, et cetera. And so I would just emphasize that whatever rules you're considering there's significant... Where I see the risk being is if you again, treat all data equally, all data collection processing equally, and so the low hanging fruit to me is really clearly going after tracking of users by the party you're not choosing to interact with and lining that up with something like the global privacy control that just allows the user to quickly signal, hey, I only want the party I'm choosing to interact with to have access to my data. That's really clean and simple and important because if you don't do that and you treat all data equally, you end up with where GDPR was mentioned earlier, which is a great... I think a pretty good privacy law framework, etcetera in Europe.

And it'll continue to evolve, but having have a popup come up every time you visit a site for stuff that's entirely in line with user's expectations like, hey, you're my subscriber and then you're paying money for the product is a disservice to the real stuff the user doesn't want to happen where the data is being tracked by third parties. And so if you're the party that they're choosing to interact with or a service provider of them, that data is very different. And I think any sort of rule would make that clear and that's within user's expectations, that's super important.

Olivier Sylvain:

Yeah. Thank you, Jason. And I thought Paul might raise his hand because this is something his opening remarks were about. So how about we'll close with these two because I've been told by more thoughtful people than I, that we could actually use extra time for the public if we end a little early. So Paul, you go and then Marshall you'll have the last word. You're muted again, Paul.

Paul Martino:

Too many buttons to push, sorry about that. I just want to agree with Jason. I do think that that kind of clarification is important, context is important. I'll just leave you with this thought, there may be other websites where you go to do lots of things that are free services and because you're not paying for it and this has often been used, the consumer is the product. What's being collected there is the data about the consumer's behavior and that's being sold. That's quite different from the retail experience, you're not going to a retail website, unless you're going to look at something that you might want to buy or hopefully for the retail industry, you're going to buy something and you're there to buy it. If you're not there to buy something and engage in a transaction, where the transaction is very apparent and clear, you're paying money to get something in return as Jason was talking about, it's very clear, you're a subscriber to a publication.

Those are instances where you shouldn't be bothering the consumer with incessant popup notices about things they already know, they're in context, you're meeting their expectations. I think it's where they don't know who has their data, they don't know how it's being used, where the FTC should focus its time. And so I think the FTC should just, and I'll make this my closing point, the FTC I think should be careful if they do pursue a regulation to not inadvertently craft regulations that are so broad or so broadly constructed as to interfere with consumer freedoms and choices, they have a right to make. For example, if they're engaging in commercial transactions with main street businesses, whether it's shopping with retail brands or going to a hotel, they should be respecting consumers choices and preferences there where in context, it's clear, these businesses are protecting their privacy, they're using innovative technology.

And I would say in the retail industry, we're using technology to just try to meet customers whenever, wherever, however they choose to shop today and that's the purpose. And so I think understanding the context is ultimately, I think a touchstone here if the FTC does move forward with regulations, and I just thank you again for your time, Olivier, I really appreciate it. The opportunity to share views with you and with the public here today.

Olivier Sylvain:

Thank you, Paul. Marshall.

Marshall Erwin:

Yeah, so just in closing, Mozilla, we may also make our money from advertising and I think we expect advertising to be the primary monetization of the mechanism for the web for the long time to come. But what we want to see is a shift away from is behavioral advertising tactics that are the predominant commercial surveillance tool in use today. That's driving a lot of the problematic activity on the web towards more benign methods of advertising, the ones which we think can be viable and can provide in meaningful monetization stream for the vast majority of companies. And those things like targeting based on first party data, contextual targeting some of the things we've already mentioned here, which again, we think can be viable, but we need a real shift away from those more sophisticated and problematic targeting practices. And to the extent that rules can really differentiate between those and force a shift towards the better set of advertising practices, we think that could be really helpful. Thank you for the time.

Olivier Sylvain:

Thanks very much. Thank you, Rebecca. Jason, Paul, Marshall for a conversation is too short, but you've helped us to air some of the important questions the commission will have to seriously wrestle with, of course, we have a bunch of questions. People like to say, remind people there are 95 questions in the

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 implementation of email sought to track both the content and the identity of communicating parties in a way that we wouldn't stand for and would violate criminal statutes if performed on postal mail or telephone calls.

Or a search, a librarian who would assist a patron in finding information owed duty of confidentiality to them. But search engines, turn this on its head, making information retrieval, a commercial transaction, 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 job candidates, such as individuals with disabilities because of how employers use certain types of screening and selection procedures at scale. In some cases, those seeking economic opportunities aren't even aware of the possibilities that are available to others because of discriminatory online advertising practices.

And although some of these practices are new due to the proliferation of digital data and predictive technologies across society, discriminatory outcomes are historical, they are longstanding and they remain essential story in today's economy and in people's everyday lives. The FTC needs to use all of its available tools, including this upcoming rule making to tackle the disparate adverse impacts that too often leave certain consumers systematically behind. Discrimination is often clearly unfair, particularly on the basis of race, gender, disability, and other categories that are protected under state and federal law. Protecting consumers against illegal discrimination is squarely within the FTCs section five authority. And the FTC can protect people in ways that may reach beyond traditional civil rights laws. Among them, ACOA, the FHA and title seven. Using its unfairness authority, the FTC can more easily reach certain market actors, such as data brokers, vendors of predictive analytics tools and others that existing laws may not.

The FTC can also reach other parts of our economy that aren't covered by traditional civil rights laws, but where there are discriminatory practices that cause certain consumers substantial unavoidable harms. For example, harms related to the collection of precise geolocation data. The FTC should seek to fill these legal gaps. The FTC needs to pursue these claims through aggressive enforcement actions, but 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:

Thanks, Karen.

Karen Kornbluh:

Thank you. Thank you, Chair Khan and commissioners Rashida for inviting me to provide comments. I lead the digital innovation and democracy initiative of the German Marshall fund of the US. We're dedicated to ensuring that technology supports rather than undermines democracy. And I'm the former us ambassador to the organization for economic cooperation and development. The Supreme Court's jobs decision clarified for many how vulnerable their online activities render their private lives. One company was revealed to sell data identifying people visiting planned parenthood clinics, heat maps could be used to trace clinic visitors to specific homes. Now, after the story broke about this particular company, it removed the sensitive data from its service, but reporters soon found other brokers selling similar information. I want to make three basic points today. First there's a national security loophole from the proliferation of consumer data, when we have so much information about Americans floating around the internet, in fact, there's a 12 billion surveillance for higher industry that allows foreign governments to buy data.

It can be used for counter espionage to manipulate voters, conduct ransomware attacks, target for harassment, et cetera, data brokers, market data, and current or former military personnel, including their web searches, family members, home addresses, and even GPS coordinates. It's difficult to trace where these data go or what they're used for. The director of US National Counter Intelligence and Security Center even said that China is using both legal and illegal means to collect bulk personal data of Americans, so we're making their job easier. Second, this data collection enables manipulation of consumers of citizens, personal and behavioral data power algorithms that show users content for reasons they don't understand. They don't know how much information has been gathered about them to determine what content they should see. Children especially are exposed to content, encouraging dangerous behavior for reasons they don't understand.

A young girl I know actually wrote a letter to one of the largest social media companies to ask them to clear her algorithm so it would stop sending her content that triggered her eating disorder. She of course received no response and had no recourse to stop the stream of harmful content in her feed. And third, very quickly as the [inaudible 01:33:55] decision revealed too many of these companies gather and sell sensitive information about vulnerable or protected groups. Recently, Kiwi Farms a notorious website that gained private information and that was used to swat and docs, trans people in very dangerous ways. They were taken down, but it's clear that this information floating about, about vulnerable people posed real physical danger.

So it's clear that the current consent framework is insufficient. The companies that we as users deal with online have an asymmetry of information yet no obligation as what a doctor or lawyer to strong professional ethical constraints and legal obligations to act in the user's interests with the extensive profiles they have. To empower users the FTCs deceptive practices authority can be used to combat for instance, dark patterns. These are user interfaces that trigger nudge users to do things against their own 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 and deter discrimination before it occurs. The FTC and other federal agencies can play an important role here. So I look forward to talking in more detail about these issues and potential solutions in our discussion period. Thank you.

Rashida Richardson:

Thank you. Stacey.

Stacey Gray:

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 documented, including by my colleagues here, I'd like to focus more with my time on solutions. At a minimum, the commission should surely codify the existing case settlements and consent decrees from the last 30 years requiring accurate disclosures and reasonable cybersecurity. In addition though, we'd hope to see the commission apply its unfairness authority to begin to reform the current market, I'm in full agreement with the comments of the other panelists today and to limit data driven discrimination and harmful secondary uses of personal data, it should do so in a focused way, prioritizing the most harmful or the most unnecessary practices. And in line of course, with its mandate to balance benefits to consumers and competition, but it should also recognize that this means establishing that many of today's current prevalent business practices in the United States are unfair.

So fortunately, even though the fairness prong of section five has not been applied frequently by the FTC in the past, the concept of fairness in data processing has a long and rich history in the United States. And so we have decades of commission, staff reports, workshops, guidance, for example, the commission has repeatedly emphasized that the collection of uniquely sensitive information such as the inference of a health condition in almost every case requires explicit awareness and consent. The commission should also seriously consider the extent to which incompatible secondary uses of any personal information, sensitive or not are unfair. This is a core principle of the 1973 US Fair Information Practices and most global data protection frameworks. The caveat is determining what is compatible and what is fair inherently involves balancing context and policy trade offs. Many secondary uses of data can, and perhaps should enable academic research support for public health fraud detection, perhaps even to a reasonable extent, advertising supported content. So as the commission engages in this balancing, I would just recommend keeping in mind a couple of practical ways that privacy risks are typically mitigated today and offer some comments on them.

The first is consent, consent ought to be a relevant, but not solely dispositive factor when it comes to fairness. We've seen empirically that giving meaningful opt in or opt out consent to hundreds of companies can be an impossible task. And the second is through decreasing the identifiability of data, which again should be a relevant, but not dispositive factor. The FTC has an opportunity today to using both its deception and unfairness authorities to essentially establish national standards for what the identification means and the use of privacy enhancing technology. So thank you again for the opportunity to participate and looking forward to the discussion.

Rashida Richardson:

Thank you all for your remarks, you already brought up a number of different concerns and solutions that I hope we can dive into a little deeper for our remaining time. And just so we can cover as much as possible, all questions that I pose for the remaining portion of this panel are open to all panelists. And I just asked that you use the raise hand function and try to limit your remarks to two minutes. And I'll moderate according to when hands are raised. So before our panel, we heard from industry representatives and partners about what informs their data practices and other views regarding this 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 with virtually no oversight at a great cost of privacy. And a particular problem we're seeing with data brokers is the mass collection of location data from individuals, particularly apps capturing your location information through third party software development kits or SDKs, which the pieces of code that data aggregators write and make available to app developers to easily add functionality to their apps. But it creates a data pipeline back to the data aggregator. And a single SDK can be found in 100s of different apps and that provides the data aggregator, the SDK developer with location data on potentially millions of individuals. So all this unwanted observation through excessive data collection and use is harmful in and of itself, I'd say, and needs a solution.

Speaker 1:

Thanks Stacy.

Stacey Gray:

Thank you. I actually agree with almost everything there. And I would argue that this is in fact, the most pressing and important if complex issue that the FTC can address, which is the legality of our current online and mobile advertising data ecosystem. And the reason is that we've seen repeatedly, in the last 10 years, examples of device based information originating sometimes for fairly benign purposes such as remarketing, ending up being scraped from real time bidding auctions, repurposed for micro-targeting, used to create highly sensitive profiles. In some cases, being used to infer identity and cause direct harm to people in the real world, in the physical world and being repurposed for, as was mentioned earlier, law enforcement and national security purposes. And one of the things that makes this so complex, is that there are of course major competitive implications to the steps that large platforms have taken to address this issue, specifically over the last five years.

So there's very little consensus on, well, there's a lot of consensus on the need to reform advertising. There's very little consensus on exactly where to draw those lines in this very complex ecosystem. And so I would only say that the EU, the European Union has been grappling with this question for many years, landed in some cases in really good places. And I would urge the FTC to engage as much as possible with EU regulators and to learn from both the successes and the failures of those data regimes. For example, the e-privacy regulation requiring individual consent on every single website through cookie banners that are, in most cases, sort of impossible to achieve meaningful consent and often a losing battle.

Speaker 1:

And I'll just add before handing over to you, Spencer, that we do in fact have some directed questions to our colleagues in other jurisdictions and we have done some engagement and hope that all of you also do encouragement, so they do reach out. Because since they are somewhat ahead of us on all of this, it would be very helpful to hear some of the details of how it's going. So over to you, Spencer.

Spencer Overton:

Thank you so much. I'm certainly concerned about trace based targeting that allows advertisers to exclude protected groups from employment, housing and lending opportunities. But I'm probably more concerned about practices that are less obvious to regulators, the public or even advertisers. Certainly, that would include tools that allow for ad targeting that are not fully understand by consumers and advertisers, like lookalike audience and special audience tools. But I'm also concerned about discriminatory ad delivery. So platforms use data collection, algorithms to determine which users are most likely to engage with particular ads, auctions, et cetera. And often advertisers, regulators in the public, they don't fully understand how these items work and whether ads are delivered in a discriminatory manner. So researchers try to do tests and study it, but it's not enough. Often it's on a case by case basis and often platforms object to the test. So these things that are really not transparent, concern me.

Speaker 1:

Thanks. Harlan and Karen.

Speaker 2:

Thanks Rashida. I'll actually address the second question you posed, which was, are there groups or factions of society that are more susceptible to certain commercial surveillance practices? And a whole dissertation, could of course, be written on this question, but I'll just share one example that's stuck in my mind. Which is understanding what it actually means, for example, for someone to have an eviction filing on their record, right? First, there was a study here in DC, that found that landlords executed only 5.5% of evictions that were filed in 2018, 5.5%. Similarly in Baltimore, 4.3%. So in a vast majority of cases of eviction filings, that filing doesn't mean that there was any wrongdoing by the tenant. It could simply reflect a landlord's threat of eviction as a power play to course a low income tenant to pay a rent on a more timely basis, or even a landlord's decision to terminate, to remove their property from the rental market. Here in DC, it was found that in 2018, there were only 20 landlords that were responsible for almost half of all the evictions filed in that year.

But once somebody has an eviction filing on their record, they will often be denied future housing opportunities due to those records. And we know too, that eviction disproportionately burdens Black and brown tenants and particularly Black women. On average, black renters have evictions filed against them at twice the rate of white renters. And crucially, Black women are also more likely to have a prior eviction filing that ultimately resulted in a dismissal. So a false eviction filing.

And of course, we could tell a very similar story about criminal records, where the record may often more accurately reflect a person's station in life, where they live or an officer's own behavior, far more 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 groups that are vulnerable and may be harmed. This particularly affects children who are, we think of as more vulnerable and less self-sufficient consumers.

And then right now, with what's going on legally I think, women, trans community, LGBTQ community, and minorities in general, where identities is being weaponized on social media. And then the one group that I mentioned that I do want to stress because I don't think we usually think of it as a vulnerable community, but it is very attractive from a national security perspective, is current duty military and former because they are such a rich target from a national security perspective. I think we have to think of them as one of the communities to worry about.

Speaker 1:

Thank you all. Discrimination and targeting has come up a lot, both in your opening remarks and some of your remarks to this. The last question and I ask, and I think it would be really helpful for the audience to get a greater understanding of why we are concerned about particularly, vulnerable groups or why certain communities don't have the same experiences online as others.

So again, with the twofold question for Harlan, I know you gave off a lot of different examples, but for others who want to chime in, it would be helpful to share your insights on how commercial surveillance practices may impact different consumer groups, especially those that have shared protected characteristics such as race, veteran status, disability, gender. But also, given that our kind of collective understanding of discrimination and targeting has become a little bit more nuanced, it would be helpful if any of you could comment on whether these practices also pose intersectional risk. Meaning people who share more than one protected characteristics may be exposed to greater harm due to their diverse status. And to the extent that you can, explaining a little bit about how those types of intersectional risk may manifest.

Spencer, you're already raising your hand, so over to you.

Spencer Overton:

Thank you so much. We all know about these existing racial disparities that have haunted us for generations. The big number is Black household wealth is 14% of that white household wealth. And there's several others. Online and discrimination and lending, housing, employment, they really pose the danger of automating racial discrimination and really broadening these existing racial disparities moving forward. Now, in addition with the economic harms and also these criminal record issues that Harlan mentioned, consumers who use platforms can be marginalized in other ways, such as voter deception, voter suppression, and diluting the voting strength of communities of color. That's actually kind of the way that I come to this as a voting scholar.

In the 2019, or I'm sorry, the 2016 presidential election. African Americans made up just 13% of the population, but they accounted for over 38% of US focused ads purchased by the Russian Internet Research Agency and almost half of the user click. You'll remember that the Russians set up social media accounts and built a following by posing as being African American operated and by paying for ads that social media companies distributed largely to Black users. And near election day, the accounts and the ads urged African Americans to boycott the election. So part of it is economic opportunity, but there are these other elements of life and liberty that are incredibly important as well.

Speaker 1:

Thanks for that. And also thank you for expanding our understanding of the risk at stakes. Katrina?

Katrina Fitzgerald:

I agree with everything Spencer said, but wanted to give another quick example. Online proctoring is an example of a technology where, with intersectional discriminatory effects and the facial recognition algorithms are less effective at recognizing Black faces. They're even worse at recognizing Black women's faces, as demonstrated by Joy Buolamwini, and to make everyone in gender shades. And then layered on top of that, the movement tracking algorithms can disproportionately flag students with disabilities, whose movements don't correspond to typical or expected pattern.

So I just wanted to flag examples because I think it's really important that the FTC makes sure that consumers in the rule include students because right now, the definition in there said that I think businesses and workers, including students would be consistent with, it's not just limited to individuals who buy or exchange data for retail goods and services. But I think students should probably be explicitly mentioned in there.

Speaker 1:

Thanks. Harlan?

Speaker 2:

Yeah, so I agree with Spencer and Katrina, that there are lots of downstream harms that stem from these commercial surveillance practices and just a wide range of abuses at the end of this, including voting, including proctoring. But I'd like to just make one additional, overarching point, which is that while many of these practices that are most harmful today, and those that involve technology and data aren't necessarily those that are the most new or the most complicated.

So many of the technologies and practices that we encounter in the course of upturns work, are actually quite easy to wrap our arms around. So for example, for a job applicant who is applying for an hourly job online, we're talking about how easy it is for any employer today to now plug and play a background check, or to put applicants through an online skills assessment or personality screening test that may reflect racist and ableist assumptions about who might be a productive worker. And so I can understand why we're drawn toward the new, fancier algorithmic machine learning tools, and this is not at all to dismiss their potential harms. But I'd also like to suggest that we continue to examine the many well entrenched technology and data practices that today continue to have adverse impacts on Americans everyday lives.

Speaker 1:

Thank you all. So I think before we move on into interventions, I want to focus on one other group of consumers that has come up, to try to unpack and understand the concerns and risk. Karen, you mentioned young people, which obviously is a group that comes up often, not only because there's tons of research that demonstrates they're more susceptible to certain commercial surveillance practices, but also because of their age, the long term harms can be great.

So it would be great to hear from all of you on how the commission should address the impact of data security and commercial surveillance practices on children and teenagers. Oh, I'll use the term young people to be more expansive, but also how the commission should evaluate the efficacy and impact of certain safe guards for young people in complicated home situations, such as foster care, emancipated minors, unhoused families, youth and detention are under court supervision. Because obviously, some safeguards like parental consent may not work for those groups. So just trying to get a gauge on how universal certain safeguards are in their efficacy for this group would be helpful for the audience. Karen?

Karen Kornbluh:

Yeah, I'll just rattle off two things really. One is, the use of dark patterns to manipulate young people into giving up data in ways that they might not want to, because it either looks like they don't have a choice, or because it's not clear that they're doing so, is one obvious one. And another is that, as I suggested, if a young person, and this is where I would answer your question about when they don't have parent, either the parent or young person, him or herself, I think there should be real thought to given should they be able to wipe the slate clean at some point? Should they have a right to push reset on the data that's been gathered about them, so that they don't go forward, carrying maybe mistakes that they made in the past or just not be allowed to change the data that's kept about them?

Speaker 1:

Thanks. Stacy?

Stacey Gray:

Thanks for the question, Rashida. So I'll just flag that there are some pretty complex jurisdictional issues here with respect to intersections between COPPA, which is our current federal statute, protecting children under 13 and FERPA, which protects students vis a vis schools and their relationship with schools. But young people are a uniquely important group and especially teenagers. So adding protections for teenagers would be in line with global trends, right? They're uniquely important group because they represent one of the fundamental reasons why privacy matters, why we care about it, which is to enable other values, in this case the ability to grow, develop, experiment, test new ideas, try on new identities, abandon them, learn, all while being free from the chilling effects of either being watched or having information from their youth used against them later, when they apply to college or apply for a job.

I will only flag, that at the same time, access to information is also incredibly important for enabling those values. It can be very easy in regulatory efforts to protect children and young people to, inadvertently, create a regime that requires, for instance, quite invasive forms of identity verification and age gating, that affect both children and adults and require the collection, the over collection of data. And data can also, of course be used to advance other socially beneficial goals that help children and young people, like educational opportunities, identifying bias in schools, identifying where to provide resources, ensuring safety, assisting children who are struggling or in danger. And sometimes these goals can be directly intentioned.

So the commission should scrutinize the use of data about young people very closely. The specific initiative around it, sort of in eraser button concept that Karen mentioned, is I think, an excellent one. The commission should scrutinize this closely and specifically for teenagers, but just sort of being aware that there's a tension there between those values and also a tension between children for whom it's the parents given data protection and privacy rights, and teenagers who are taking on greater autonomy over their own choices and their own information who ought to be afforded similar rights.

Speaker 1:

Thanks. Katrina?

Katrina Fitzgerald:

One reason it's important for the commission to set specific rules for young people, is that targeted advertising is particularly harmful to children and teens. They're much more vulnerable to commercial manipulation. They're still developing the critical thinking skills and often they can't distinguish between advertisements and non-commercial content, especially because online, digital media has none of the separation between advertising and entertainment content that TV has and young people can't recognize, for example, influencer marketing, in game marketing, as advertisements. Fairplay did excellent comments, sent them to a commission earlier this year, the stealth advertising comments. So I would point you to Fairplay's comments there for evidence on that point.

But because there's not that separation and because kids and teens are particularly vulnerable to commercial manipulation, the FTC should really declare targeted advertising to people under 18 to be unfair. And then to your point about young people in complicated home circumstances, I mean there's many reasons why families are not able to constantly monitor minor's digital media use, and that's why platform should be required by default to have the most privacy protective settings for young people.

Speaker 1:

Thank you. And thank bringing up Fairplay's comments because this gives me a great opportunity to plug the fact that we still have a open comment period for the kids stealth advertising. So if parents, students, anyone, has views on those, we'd love to hear from you because it's informing another process on this very issue Katrina just mentioned. And in some of your responses to this, you mentioned sort of like the race or right to deletion, but Katrina actually, and I may actually be confusing who said what in the opening remarks, but I believe you brought up data minimization in some of your opening remarks in that an issue that I know is sort of one of the major talking points of a lot of consumer advocates as a way to address and mitigate consumer harms because you're stopping it upstream.

But I think one of the looming questions we have and actually posed in this ANPR, is if we are to dig deeper into data minimization or even data transparency, what do those requirements look like and how can they address commercial surveillance practices and harm? So I know this is a little bit more targeted on a specific issue, but open ended, it would be great to hear from any of you about, I guess some of the more granular details of how do you think we should operationalize data minimization and transparency, and also what are the stakes with that type of intervention? Katrina?

Katrina Fitzgerald:

EPIC and Consumer Reports wrote a whole paper for the FTC on this, so, [inaudible 02:07:03]. We sent it over this year, we presented three possible approaches for how the commission should promulgate, a data minimization rule under section five. The approach we recommend is a data minimization rule that bans secondary use and third party disclosure while explicitly carving out certain exceptions, like data 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, on companies to minimize their collection of data to what's reasonably necessary to provide the service.

Basically, it better aligns companies collection and use of data, with what consumers expect when they use the internet. It allows them to use it with their privacy protected as the default.

Speaker 1:

Great. And I'm going to do something that's a little unfair, but I hope you will just go along with me. Harlan and Spencer, you both talked a lot about different ways that discrimination manifests either at stemming from commercial surveillance practices or replicating broader problems in practices in society. And to this related question, I'm just wondering if you have any thoughts on the relationship between data minimization, or even transparency in relation to some of the discriminatory harms we're seeing? Is collecting less data going to reduce the likelihood of amplifying discriminatory practices, or is there something else that we're missing there? With this question, I'm also asking you in some ways, to unpack that relationship and how maybe or not some of these safeguards may good for consumer but may or may not actually address this issue around discrimination or disparate outcome?

Spencer Overton:

I will let Harlan kind of build or magnify on this. I do think that minimization, as well as transparency are important and Katrina own mentioned this notion of moving the burden away from individuals to structural rules in terms of meaningful transparency, in terms of regulators. Kind of the traditional notion of consumer consent cannot address harms like economic discrimination. Like a Black woman does not know she's not being shown ads about a lucrative job posting or a house for sale in a community with great public schools.

And so this concept of transparency and shifting to government and shifting to companies in terms of obligations, I think are important. Definitely if there is a unintended consequence with the whole minimization piece, I think that there's just the point that color blindness alone here is not the answer. Yeah, we've got to fight the improper use of trait based ads and housing, employment, financial services, voter suppression, But we also have to recognize that digital advertising can play an important role in building community, mobilizing voters from underrepresented groups, disseminating essential health information on breast cancer, sickle cell, Gaucher disease, to groups that are most likely to be affected.

So definitely, data minimization is definitely good in terms of a concept. I also want to mention though, that kind of mechanical colorblindness is not always the answer because sometimes the data can be used for good.

Speaker 2:

Yeah, I'll just riff on both of Spencer's comments. As it relates to data minimization and connecting to my earlier comments, sealing eviction filings at the point of filing, before they can fall into the hands of data brokers, is an important intervention that I think would stem at least some of the discriminatory impacts of landlord actions and tenant screening activities. Similarly, for criminal records, especially non-conviction arrest records, sealing those records from public view in a way that will influence people's housing opportunities and job opportunities, has an important role to play. And limiting the use of background checks, writ large, because a lot of the data, as I've already mentioned, stem from systems that are racist and unjust.

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? How far can they actually move the needle in avoiding discrimination? What are those outcomes? As Rebecca Finlay from the Partnership on AI pointed out in the last panel, this kind of work does come with risks and it needs some guardrails. But in general, we'd like to see more companies do this and to show their work publicly. Because if companies are to take the problems of racial and other discrimination with any amount of seriousness, they can't be scared to look into measure and to make good faith efforts to address the disparate impacts that they see. And so yeah, I think the FTC has a major role to play here to get companies to do just that.

Speaker 1:

Thank you.

Karen Kornbluh:

Can I add one thing to that? Yeah. Just having been at a company recently, I also think it's so important that the FTC speak to these issues with rules. I think there are a lot of ethical guidelines floating around, but often those just don't serve the same educational purposes to companies that aren't thinking of all their new innovative products based on the data. They're, look, this data that we have over here in a drawer, what can we do with it? They often need a lawyer telling them, these are the guardrails, this is what you can and can't do. These are protected classes that you need to worry about. And so I just, following up on Harlan's great point, for them to start collecting that data and doing that kind of work. I think they really need some kind of clear incentive from the government.

Speaker 1:

Thanks for adding that. Stacy?

Stacey Gray:

I agree. And just a quick word on the transparency piece. The FTC should consider it potentially, as part of its unfairness authority and not just deception authority. Because despite the relative ubiquity of privacy policies, there's really no federal standard requirement for having them or standard about what they are to contain. And even though we have sort of a mountain of evidence that most average consumers do not read privacy policies, and even though we know it does not solve for these other unfairness issues. It's still the fact that disclosures of databases and disclosures of data processing, are something that ensure a baseline of information in the marketplace and help enable all of the other rights and obligations that we talk about in data protection. And other people do read privacy policies, specifically journalists, researchers, competing businesses and regulators. So this is something that the FTC could consider codifying, for instance, that the absence of adequate disclosures is an unfair practice and of course, not avoidable by consumers.

Speaker 1:

Thanks. That's actually a great segue into another sort of prevailing intervention that I was hoping you all could chime in on. And that's notice and consent. And I know the chair has been quite vocal in questioning whether notice and consent is continuing to be in effective framework for protecting consumer privacy. So it would be helpful to hear from you all on how the commission should evaluate the effectiveness of consumer consent? And to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? Stacy, you helpfully distinguished between the two, and that section five has two major parts and we tend to focus on the deception part, but sort of hearing from you on where it fits within our authority and how we should evaluate the effectiveness would be very helpful. Stacy?

Stacey Gray:

Absolutely. So like I mentioned in my opening remarks, I think it's becoming widely accepted that consent, opt in, opt out, whatever it is, individual choice, is relevant, but ought not to be the soul or the dispositive factor in these sorts of balancing tests when we talk about fairness. Lots of reasons for that. One is practicality. If you look at, for example, the current data broker registry database of companies based in California that are required to register with the state of California, stating that they collect and resell personal information that they did not obtain directly from consumers. Those companies are obligated to comply with opt out requests. But as you can imagine, 500 plus companies, most of which most consumers have never heard of, have never interacted with, the practical impossibility of submitting opt out requests there, just makes it an almost meaningless, if not actively harmful because it's a legitimizing factor in the question about privacy in California and those companies.

And it's one of the things that's motivated all of the discussion, of course, about the global privacy control, which the last panel discussed, I think, in a really helpful way. But aside from just the practicality, my only other note about consent is that we would not want the FTC to limit itself to current technology and to current technology that can be designed for consent. So we're increasingly entering a world involving voice enabled devices, smart city devices, connected vehicles, and in all of these contexts, you face a situation of consent, either not being possible to obtain, for instance, with external facing cameras on a mobility device, not being able to get consent from passers by. Or where it's simply a bad idea to try to give individual choice, for instance, with respect to data being used for safety in a connected vehicle. So we need other safeguards, we've got to expand outside of that notice and choice framework. We need to be talking about minimizations, pseudonymization, de-identification, all of these other ways to mitigate risks without placing all of the burden on individuals. So those are my two high points on consent.

Speaker 1:

Harlan?

Speaker 2:

Yeah, I'd say in general, I don't think consent is a particularly useful framework because we need systemic and not individual interventions. But particularly as it relates to discrimination into core areas of economic opportunity like housing, employment, and credit, consent means very little because we need a power analysis here. When people at the margins are seeking housing security, or stable employment, needless to say, they often don't have the choice in practice not to pursue opportunities that are in front of them. And of course, in that position, this makes those folks particularly vulnerable to giving consent, in ways that are not truly voluntary. So what ultimately matters here is outcomes. Is there a disparate adverse impact at a systemic level due to these commercial surveillance practices? And that just won't be answered by looking at individual consumer consent.

Speaker 1:

Thanks. Karin?

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 can be subverted by these dark patterns that we've talked about where there's technically, you can deny consent, but not actually. So, I think these things are wrapped up in each other.

The second thing that is something that I mentioned in my opening remarks, which is just, and other people have talked about it too, this power imbalance. So, even if I give consent, the lack of obligation to look out for my interests on the other side, which is just not something that we have in other areas of our lives, where there is such a asymmetry of information and a power imbalance, there would be some obligation, ethical, professional, legal, and so on.

And then the third thing I would just say is that I think consent, a global consent is problematic when it gets to sensitive information. So, I think again about I've given consent, but now I'm doing a search for the location of abortion services, and it never enters my mind that that information would be collected. And so, I think at that point, there should be an option to go into anonymized mode, or to have to get your consent again, if there's that kind of sensitive information.

Rashida:

Thanks. Stacey?

Stacey Gray:

So, I can't be on a panel without plugging my friends in the EU and the GDPR. Two very quick ways that the FTC can really learn from what's been happening there. The first is it's a common misconception that the GDPR requires consent for all data collection. Absolutely not the case. The GDPR has different lawful bases. Consent is one of them, which I think is putting consent kind of in its appropriate place where it can be used effectively, but is not the only, or the necessary, or the sufficient way to collect data. They also have a very effective legal framework called legitimate interests, which in some ways, is very similar to the FTC's unfairness authority, in the sense that it requires a balancing of a company's interest in collecting the data, with the impact on the rights and freedoms of the individual, or the harms to consumers and competition.

And the second piece is that the EU has acknowledged in a way that we'd love to see US regulators do more of, acknowledged the power imbalances inherent in consent situations. So, for example, consent is not considered a valid legal grounding under the GDPR, in employment situations. So, other legal bases can be used, for instance if a contract is signed, but the idea is that employers vis-à-vis employees have inherently far more power to nudge, to manipulate, to coerce, and that a person starting a job isn't in a position to be able to meaningfully consent to, for example, worker productivity tracking surveillance tools. So, two lessons that I think US regulators should absolutely think about adopting in this process.

Rashida:

Thanks. And Spencer?

Spencer:

Yeah, I already spoke on this in my last [inaudible 02:23:18], so I'm not going to repeat it. I just wanted to reference Sarah Collins of Public Knowledge has some informative writing and work on this concept of consent and the limitations. So, just wanted to cite and flag that. Thanks.

Rashida:

Great. And then because we're close on time, I want to end with just an open-ended question that I hope any of you could answer, on whether there's any considerations or concerns that you think we're missing, even though we asked 95 questions. There's a lot of areas to cover in this ANPR, and Katrina, you already mentioned the great point about students being explicitly considered a type of consumer. So, I'm trying to solicit those types of responses of, are there certain consumer groups we're not thinking about? Are there certain concerns that weren't referenced in the 95 questions, or are there certain considerations from other jurisdictions or otherwise that we should consider?

Karen, I thought the anecdote you shared in your opening remarks about the young woman who tried to start the targeting that triggered her eating disorder, is one where we hear about some of the sort of negative social implications that can stem from these uses, but I thought that was a helpful example of how the even overly burdensome processes that platforms put into place, often don't work. So, now that I've highlighted things you've already said, I'll just leave the floor open to see if you have anything else to share as your closing comment.

Katrina?

Katrina Fitzgerald:

Sure, I'll list off a few. In addition to the students issue you mentioned, there's no mention of location data. I think an obvious question would've been how precise location data needs to be for particular commercial uses of it to be unfair. There are also other categories of data that are particularly sensitive and require a heightened level of protection, and I think the commission should explore enumerating categories of sensitive data. Another one would be data generated from consumer products that are voluntarily disclosed to law enforcement, like Amazon Ring, and many commercial AI products are also targeted at law enforcement, and this obviously fosters systemic discrimination in policing.

Two more. There were no specific questions about service provider relationships, and I think restrictions on what service providers can do with data disclosed to them in the context of a business relationship are critical, and the FTC should be thinking about rules for those business relationships. And then as Stacey mentioned in her opening remarks, standards for de-identification are also important. W constitutes anonymized data versus de-identified? This is something that enforcement bodies like the UK ICO have highlighted as a key concern.

Rashida:

Great. Anyone else have more to add? Oh, Spencer?

Spencer:

Sure. I know we are at time, but just wanted to add a couple of quick points here, some things that the FTC I think should think about in protecting consumers, particularly with regard to discrimination. First, civil rights challenges are evolving, and we should deepen later expertise in coordination in both tech and civil rights. So, the FTC has really led the way in building up tech expertise and should support the EEOC, HUD, CFPB, and other agencies with deep civil rights expertise, as they do the same in terms of trying to build up tech expertise. The FTC should also continue to strengthen its civil rights expertise and capacity.

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, that is good. That said, preventing discrimination should not simply be an optional business decision that some competitors embrace, and other competitors dismiss, right? Government has an important role, the law has an important role. Both cotton and the Industrial Revolution, they were incredibly profitable and they expanded our economy, but unchecked, they produced racial inequality and global warming, that are among our most significant challenges today. So today, the world's most valuable companies, they should not have the right to externalize the costs of discriminatory ad distribution onto many of the nation's most economically and politically marginalized communities. Thanks.

Rashida:

Thanks. Well, thank you all for making the time today and bringing such wonderful contributions to this panel. I hope it was very informative for audience, and helped spur more comments. With that, we're going to be closing the two panels, and now I'm going to hand it over to Commissioner Bedoya.

Commissioner Alvaro Bedoya:

Hello, everyone. Thank you, Rashida. Thank you, Professor Richardson. Thank you, Spencer. It's good to be here, and I want to start by expressing my gratitude to my colleagues, Chair Khan, and Commissioner Slaughter. We are here because of two people, Chair Khan, who is leading this process, and Commissioner Slaughter, who called for it years ago, and I am proud to call them colleagues, and as I think each of them said, each of them, I will return that sentiment. Each of them are experts in different ways, and I think that the combination is going to be a productive one.

Secondly, if there's one single thing I can stress, it is that you do not need to be an expert to comment on this process, and in fact, I would urge you that if you know there's a thought in the back of your mind, "I think this is interesting, but I'm only in high school, I'm only a college student, I'm only a law student, I'm only an engineering student," and you have something to say, please, by all means, comment and say it. You don't need to be an expert to be harmed by unfair and deceptive practices, and by that measure, you certainly do not need to be an expert to share those experiences with the commission.

Number three, I want to respond briefly to this idea that has come up at different points, it came up a little in Professor Sylvain's panel, and Professor Richardson's panel, that this ANPR is broad, because it goes beyond this conception of notice and choice, and I think that unfortunately, there's often a caricature of American privacy, as being defined by notice and choice. And what I want to stress is that from the very beginning of American commercial privacy law, privacy harms and privacy rights to protect against those harms have gone well beyond that initial point of collection. They've extended to use, purpose specification, commercialization, security, sharing, fair access, correction, et cetera.

And for me, the most salient example of that goes back to 1890, which is when Brandeis and Warren wrote their seminal article in the Harvard Law Review, and the case that people remember from this is they talked about the surreptitious photography of Boston's society weddings, and of course, this is an example of a non-consensual taking of data. This is a collection and choice question. But what a lot of people forget is that in that same article, they also talked about a separate, I think it was Boston resident, it could be wrong, who had their portrait taken. It was a woman, but she had her portrait taken by a photographer who she hired, and then a couple weeks or months later, she's walking down the street, and she sees her face on the cover of a Christmas card that the photographer had decided to market using her likeness. And again, this is from that seminal article, The Right to Privacy.

Now, I'm not here saying that that is an unfair deceptive practice one way or the other, but what I am saying is that from the very beginning, American privacy has encompassed so much more than that initial point of notice and choice. And Stacey Gray talked about this, that the fair information practices, I would add any number of statutes that the commission enforces, the Fair Credit Reporting Act, COPPA, the Kids Privacy Law, Gramm–Leach–Bliley, if you look at the sum total of these protections, they go far beyond that initial question of notice and choice. And so, the breadth of the questions that we are asking of the public reflects the breadth of that tradition and of that history, and of the fact that people can be harmed at different stages of that process, and we want to hear about that.

Lastly, I just want to underline what this is about is how commercial surveillance is impacting people. And so, if you have a story about how it's harmed you, if you have a story about how it's benefited you, please, please comment and tell us that story, so that this is not just a collection of quote, unquote, expert submissions. We very much want to hear from every interested member of the public. So, with that, I will turn it over to Peter Kaplan, who is going to moderate the public comment section of the session today.

Peter Kaplan:

Thank you, Commissioner Bedoya. Before we begin, please note that the FTC is recording this event, which may be maintained, used, and disclosed, to the extent authorized or required by applicable law, regulation, or order, and it may be made available in whole or in part in the public record, in accordance with the commission's rules. In addition, I'm going to ask for those speakers who are affiliated with a particular company or organization, we'd appreciate it if you would please disclose that affiliation before you begin your remarks. Thank you. So, now we'll hear from members of the public. Each of them will be given two minutes to address the commission, and our first speaker is Andrew Crawford. Andrew?

Andrew Crawford:

Thank you, Chair Khan and Commissioners. My name is Andrew Crawford, I'm a Senior Council on the Privacy and Data Project at the Center for Democracy and Technology. CDT commends the commission for highlighting the importance of protecting the public from harmful commercial surveillance data practices and security practices. My remarks today are going to focus on harmful uses of consumer sensitive information, data that can reveal our location, and data that can be used to make insights into our physical and mental health.

Unfortunately, there are numerous examples of inappropriate data collection sharing, and use of sensitive personal information, and the commission is well aware of these practices, and has taken action. Mobile apps, including reproductive health apps, have been found to violate their own policies when sharing sensitive health information of millions of users with third parties, including advertisers. Last month, the commission brought an action against a data broker for allegedly collecting, and then selling location data that reveals people's movements to and from sensitive locations.

The harms associated with the misuse of sensitive personal data can have lasting emotional and physical effects, and the burden of protecting sensitive data falls almost entirely on consumers. In the face of these persistent harmful data practices, it's time to place real limits on how sensitive information is collected, shared, and used. To that end, the commission should embrace the following priorities in any subsequent rulemaking regarding sensitive personal information.

First, it should limit sensitive data collection sharing and use practices to only what is necessary to provide the product, service, or specific feature the person has requested. Second, the commission should continue and expand the use of existing unfairness and deceptive practice enforcement authorities. These critical tools can prohibit inappropriate data practices, and address misleading 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.

K.J. Bagchi:

I'm getting set up here.

Apologies. Good afternoon, commissioners. My name is K.J. Bagchi, and I serve as Senior Director of Technology Policy at the Chamber of Progress, a tech industry coalition devoted to a progressive society. Our partners include large and small tech companies in a variety of industries, such as the autonomous vehicle, AI, and FinTech spaces. Our industry partners do not have a vote or veto over our policy positions.

Now, we support the commission's efforts to create baseline rules because consumers benefit when businesses have clear rules of operation, and when the tech industry is incentivized to undertake and explore stronger data protection processes. At the outset, we support many of the policy goals covered in the ANPR. For example, we share your commitment to prevent a consumer's information and data from being used against them in discriminatory ways. No one should face barriers to housing, employment, or credit, based on their personal information, and companies should be encouraged to test their products for discriminatory outcomes, and given an opportunity to cure before the problem grows. Other privacy principles such as data minimization, purpose specification, and stronger data security practices are also important for consumers to trust the products and services they use. We also believe that people can suffer from non-tangible privacy harms. For example, people can suffer from the public disclosure of private facts, such as around the non-consensual release of adult imagery.

That said, there are other areas where we encourage the FTC to tread more carefully. For example, the FTC should recognized that targeted advertising can play a critical role in supporting small businesses, consumers, creators, publishers, and competition. Further, while we recognize the limitations of a notice and choice framework, these principles should not be completely abandoned. Consumers have fundamentally different approaches towards digital engagement. Therefore, choice has to be a part of the solution. Thank for the opportunity to provides public remarks today.

Peter Kaplan:

Thanks, K.J.. Our next speaker is Heidi Saas. Heidi?

Heidi Saas:

Thank you. My name's Heidi Saas. I am a Data Privacy and Technology Attorney, I have my own practice. I want to talk to you about a couple of things today. First, don't tread lightly. Second, don't hold back. Third, these are my opinions, not legal advice. I want to talk about privacy enhancing technologies. They do not always afford the privacy level that you think they do. If we're going to require the use of PETs and other technical measures, please be sure they work. So, we're going to need to require de-anonymization attacks, just like we have penetration testing for cybersecurity.

The system of surveillance capitalism was not built overnight, it's not going to change overnight. I've had plenty of meetings with business owners that tell me, "I hear you, and that sounds like a good idea to stand up a solid privacy program, but we don't have any credible threats on the litigation or enforcement landscape." So, they are choosing not to do this, until they have a bigger stick. Please get your stick ready.

Algorithmic bias. Bias is real. It's also harder to get rid of than cellulite. So, there are residual risks that people need to know about. They must be disclosed before people are parsed, profiled, and prevented from accessing employment, housing, loans, just all the stuff they need to live. Pay attention to the new frameworks that are coming out for audits on how to conduct audits, for bias on AI and autonomous tools. I would encourage you to look at the ones coming out of the EU, as well as ones that are being 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-

Heidi Saas:

Oh, thank you.

Peter Kaplan:

Sure. Our next speaker-

Heidi Saas:

I hate data brokers. Just one more thing. I hate data brokers. That's it. Thank you.

Peter Kaplan:

Thanks again, Heidi. Our next speaker is Yadi.

Yadi:

Hi. I thank the FTC for your initiative to address commercial surveillance, which is rapidly becoming an epidemic. In my brief comment, I'll share a couple real life experiences that highlight the importance of regulating the vast amounts of consumer data that companies [inaudible 02:43:48] exploit. Before that, I would encourage the FTC to be more inclusive and seek out civil society stakeholders that better reflect diverse society needs and interests, such as foster youth and juveniles in detention. Perhaps the industry panel is too crowded to include the FPF, but it doesn't belong in the Consumer Advocacy Panel.

The FPF, a privacy compliance industry association, sprinkled with some academia, is made up of many organizations that currently use and profit from surveillance. The FPF Advisory Board is littered with organizations that have dealt with FTC privacy violation lawsuits, settlements and fines, Google in 2019, 2012, eBay in 2000, and Meta Facebook in 2019. Remember, Cambridge Analytica? Plaid in summer 2022, Twitter in 2022, Uber, the makers of God View, and I'll just pass on their best practices.

Surveillance absolutely has dire consequences. Jorge was wrongfully accused of murder due to Google geofence data, being arrested and costing him his job, his car, reputation, and severe emotional distress. That's real harm. Celeste, 18, and her moment, have been charged with a series of felonies and misdemeanors after an alleged medical abortion, using evidence from private Facebook messages, The teen is being tried as an adult. If convicted of a felony in the State of Nebraska, these two women will lose the right to vote, and be incarcerated. That's real harm. We need stronger and more meaningful actions against surveillance that puts people first, over unfettered innovation and perceived compliance burdens. Thank you.

Peter Kaplan:

Thanks, Yadi. Our next speaker is Bo Kohut. Bo?

Bo Kohut:

Can you hear me?

Peter Kaplan:

Yep.

Bo Kohut:

Good afternoon, ladies and gentlemen, and those who do not identify as either. My name is Bo Kohut, and I've been pursuing abusing what we have come to know as the internet, since I first logged on in 1991. My interest drove me to get a computer programming degree in the mid-90s, which many mocked then. Since then, I have founded architect, and managed and exited multiple technology startups, all within the highly regulated financial payments industry space. I've also been privy to assist technology matters to the multiple states of our union, as well as having written software for the United States government.

Given my direct vast experience in this arena and throughout the full spectrum, I fully support this FTC pursuit. The data exchange issue has become one of profit, over everything else, including but not limited to personal security and risk to life, as directly seen very recently with the internet [inaudible 02:46:26] of Kiwi Farms, after a US Senator's experience. However, this is a double-edged sword that will likely have exceptions, and thus loopholes, which are certain to be excluded, as some present here to know with the given recent disclosure of Fog Reveal, which was secretly in use by the very government attempting to pursue these goals. Another very recent event from that, you may not be aware, is the transcription service as an app, called Otter.ai, which has been discovered to be listening and transcribing, even after deselecting its ability to do so.

Clearly, snooping and spying has extreme value. Just ask Apple, as their great intervention called the AirTag. The world is becoming familiar with one country's response known as GDPR, however, here we are abusing our own citizens' privacy through technology, of which very few understand how any of it works, as even Meta's engineers, formerly Facebook, recently admitted under oath from a recently unsealed court hearing involving the Cambridge Analytica scandal. Our allies over the pond have also created legislation about how hardware devices must be built with security in mind. However, all hardware is software, if you didn't know this, and imposing on how something is done correctly, writing software. Heidi mentioned that earlier too, by the way.

No matter what comes with such legal pursuits, let alone enforcement of something directly related to the confidential intellectual property of the business, this is in no way we'll be fixing everyone's existing data issues that are alive today. I have read through several of the regulation's public comments, and many want it fixed, but I regret to inform everyone alive today that your data is out there, and it cannot be taken back or removed. The cat is out of the bag.

Peter Kaplan:

Thank you, Bo. Thanks, Bo.

Bo Kohut:

Thank you.

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-chairing the ACM Computers, Freedom, and Privacy Conference. Last year, I was a member of the Washington State Automated Decision Systems Workgroup, and my comments today focus on discrimination and automated systems.

Technologies reflect the biases of the makers and the implicit rules of society. Today's algorithmic systems are error prone. The data sets their [inaudible 02:51:26] have significant biases, and as we heard, it's asymmetric. The harms are usually much greater on historically marginalized communities. Who gets wrongfully arrested as a result of facial recognition errors? Nijeer Parks, and other Black people. Regulation is clearly needing, and it needs to designed to protect the people who are most at risk. The Algorithmic Justice League's four principles are a good starting point: affirmative consent, meaningful transparency, continuous oversight and accountability, and shifting industry practices.

As I discussed on the Nexus of Privacy, several of the experts whose were panelists mentioned today, are key members of AJL. Their policy recommendations for AI auditing highlight specific areas where FTC rulemaking could have a major impact, and the details matter. Too often, well-intended regulation has weaknesses, easily exploited by commercial surveillance companies with their hundreds of lawyers. For example, the proposed American Data Privacy and Protection Act Consumer Privacy Bill, doesn't require independent auditing, instead allowing companies like Facebook to do their own algorithmic assessments.

So, I implore you, as you continue the rulemaking process, please make sure that these historically underserved communities most harmed by commercial surveillance are at the table, and being listened to. Thank you for the opportunity to comment today. I go into more details in these points on a post on the Nexus of Privacy.

Peter Kaplan:

Thank you, Jonathan. Our next speaker is Serge Egelman. Serge?

Serge Egelman:

Thank you for doing this, and offering me the opportunity to speak. My name is Serge Egelman, and I direct the Usable Security and Privacy Group at the International Computer Science Institute, a research institute affiliated with UC Berkeley. I'm also a co-founder and CTO of AppCensus, which performs privacy analysis of mobile apps. I've been performing peer-reviewed research on online privacy for nearly 20 years now, which includes studies of consumers' privacy preferences, and decision making processes, as well as measurement studies to examine how industry practices comport with consumers expectations.

I've come to the conclusion that rulemaking in this area is urgently needed. Consumer privacy preferences have been studied for more than 50 years now, and from these studies, we know unambiguously, that consumers have strong privacy preferences and care about their personal privacy. That they frequently engage with online services that contradict those preferences is not evidence that they do not really care about privacy, but instead, points to massive information asymmetries. Most consumers simply have very little awareness of the ubiquitous third-party data collection that occurs today. How could they? That they do not opt out, is not evidence of consent, but instead evidence that any possible consent couldn't be meaningful, informed, or explicit.

I completely agree with many of the panelists today, rulemaking should focus on secondary data collection, and to create rules to ensure that it occurs with meaningful consent. Many data brokers currently make fraudulent or misleading claims about collecting data with consent, or that personal data is somehow anonymous. The FTC should use its authority to ensure that those claims comport with reality.

Finally, recent published research performed by one of my PhD students, Nora Alamar, shows that most app developers are simply unaware of their service's privacy compliance issues. Many of the problems are caused by third-party components, [inaudible 02:54:33] services such as ad SDKs, which in many cases, are not properly documented, or are misconfigured. Thus, I suspect that the FTC could drastically improve compliance rates, simply by better exercising its CID authority, to simply make software developers aware of the issues and their seriousness. The FTC could also offer better guidance directed specifically at software developers, as well as find ways to incentivize platforms and third-party data recipients to do the same. Thanks again-

Peter Kaplan:

Thanks, Serge. Oh, okay. You're wrapping up.

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:

Hi, this is Lydia Brown. I'm policy... privacy and data at the Center for Democracy and Technology. My work focuses on algorithmic discrimination and bias that harms disabled people. Many of whom belong to other marginalized communities, such as the LGBTQ community. We are disproportionately impacted by algorithm-driven decision making systems in every aspect of life. Students are increasingly subjected to unproven unreliable surveillance tech, like aggression detection microphones, automated student monitoring, and automated test proctoring that rely on algorithms to assess whether students are engaging in violence conduct, making threats or cheating on tests. Students with disabilities ranging from ADD and bipolar to autism, blindness and absent limbs already experience increased profiling, discipline and exponentially higher likelihood of being flagged by programs that evaluate how much they can form to an arbitrarily defined norm.

Automated software can screen out disabled and LGBTQ job seekers whose resumes reflect the impact of past discrimination and denial of access to equal opportunity in school and at work. Gamified assessments, personality tests, sentiment analysis software, and other AI hiring tools may likewise fail to accurately or fairly interpret or assessed disabled and gender nonconforming people. Disabled people are currently at extraordinary risk of compounded discriminatory effects of rapidly expanding surveillance tech. Two, disabled and LGBTQ people are more likely to be arrested and incarcerated with the Department of Justice recording up to 85% of incarcerated youth as disabled. Use of tenant screening software, employment background checks, and predictive policing tools that inappropriately and sometimes illegally use arrest or conviction records, thus has an outsized impact on disabled and LGBTQ people, creating further inequities down the line. I would urge the commission to consider explicitly addressing discriminatory and disproportionate risks of harm for disabled and LGBTQ people in developing any proposed rules on data practices and algorithmic systems. Thank you.

Peter Kaplan:

Thank you, Lydia. Our next speaker is R.J. Cross. R.J.?

R.J. Cross:

My name is R.J. Cross with U.S. PIRG, the Public Interest Research Group. Thanks to the FTC for putting together this forum and for larger investigation into the monetization of personal data by corporate actors and the real and potential harms that come with it, because there are real harms and there are harms that we need to address. For one, corporate data collection has enabled scammers to unprecedented reach to find their victim. In 2021, the Department of Justice took action against free data brokers that we're knowingly generating less potential victims for predatory operations. The scams went like this, send a mailer saying the victim had 1,000 of dollars and if they could stake, it could be claimed by paying a fee. The mailers were sent to people identified by these data brokers most likely to fall for it, and their list were largely made up of the elder are cognitively impaired, including individuals with Alzheimer's. If someone responded to a scam once, they were likely to respond to scam again. And so, these brokers contracting with new scamming companies spending new scheme use the same victim over and over again.

These brokers also use the data and who sell for it to create new models to find additional ideal victims. All of these companies fled guilty and had to pay fines, which is great. They should be held to account for the gross exploitation of swindling dementia patients, but the oversight of these companies' future activities are incredibly limited. The business model remains intact. It's going to take something larger to stop these practices. It's going to take new rules and real rules, and now is the time to act, because the case of scammers is one of the most blatant examples of how data falling to hand, seeking to make a buck off of what they can learn about it causes real harm, but there are other harms.

The commercial surveillance business model is only in its infancy. New technologies are soon going to be widely adopted by the public, like AR, VR goggles that in a single second of use generate 90 data points in our body language. It'll soon be databases on our behavior far beyond what any psychologist or business ever seen, and it will be information that can be used to identify our weaknesses, our fears, our personal gullibilities and how to exploit them. So, we asked the FTC to act. Thank you.

Peter Kaplan:

Thank you, R.J. Our next speaker is Maya Morales. Maya?

Maya Morales:

Hi, my name is Maya Morales. I'm an organizer, educator and artist and founder of Washington People's Privacy, which is an organization focused on people's advocacy. I reside in Washington state on the unseated ancestral lands and waterways of the Coast Salish peoples who lived in harmony with this ecosystem for centuries before the arrival of settlers. I'm here to help communicate the deep concerns of Washington residents about these issues and urge you to consider both current and future harms, many of which the earlier speakers have cogently outlined already.

People's privacy is a prerequisite for free, equitable and democratic societies. In this sense, our privacy is worth so much more than corporate growth and our governing bodies must protect that value. Increased surveillance via mass data collection isn't preventing crime or creating safety. People are weary of the fear mongering, xenophobic messaging and policies repeatedly employed to justify increased surveillance, increasingly invasive commercial surveillance in our daily lives rather than simply meeting basic needs that do prevent harm, creating better safety, fostering healthy people and communities. Our wellness rights and liberties are paramount to profit.

Data collection should be minimized to what is strictly necessary. Entities should be prohibited from using coercive and sneaky methods of collecting and sharing our data. Similar to ALPRs tracking cars everywhere we drive, tracking devices across platforms leads to kinds of harms. Where a commercial surveillance, automated decision systems, AI, and very soon AR and the metaverse intersect with overreaches of law enforcement and intelligent agencies, existing systemic harms and violence are amplified and yet also completely obscured as to who is responsible for the harm or violence. This is sure to produce a steady slipping away of people's rights in relation to accessing food, housing, income, jobs, and even travel, leisure and joy. With more time, I'd love to provide more substantive feedback on specific questions in writing, but I hope this brief comment will help in some way, so many thanks to all of you for your time on this.

Peter Kaplan:

Thank you, Maya. Our next speaker is Cheri Kiesecker. Cheri?

Cheri Kiesecker:

Hi, thank you. I'm Cheri Kiesecker and I'm concerned about student privacy. Many schools require parents and students to sign an agreement each year stating they have no expectation of privacy, yet schools are increasingly relying on tech and AI to collect more student data with no ability to opt out. These school apps actually put students at risk because many of them have been found to improperly share student data with advertises and third parties with no penalty. Most schools also require one-to-one devices. Think about their location tracking, websites for free, video cameras, student voice, facial 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 unproven and hidden predictive analytics. One ed tech company, eduCLIMBER, flag students as the risk using a risk ratio based on the student's ethnicity, gender and disability. Schools are requiring students to use biometric apps that monitor their heart rate for a grade in PE class. Apps can check every word the student types, even monitor when kids go to the bathroom. Schools are also using surveillance cameras linked directly to police departments or armed with AI that can detect the student's facial expression as violent, and then flag them as a future risk.

Many apps claim to measure student emotions. NWEA's MAP assessment tool gives each student a separate and hidden engagement score, regardless of whether the student answers the test question correctly. They claim their algorithm can predict deep-rooted problems in other areas of a student's life. Microsoft also uses algorithms and AI to measure student engagement. Google Classroom uses AI, including its controversial Lambda language platform to know the student and finish their sentences. In conclusion, students are unfairly forced to surrender their personal data. There's no requirement for accuracy of algorithms, no transparency on how data are used or shared with third parties, no accountability, and so far, no penalty. Companies hide behind overly broad interpretation of educational interests, school official or processing. Thank you so much FTC for your leadership, and I hope you use all your powers to protect children, including students. Thank you.

Peter Kaplan:

Thank you, Cheri. Our next speaker is Bilal Sayyed. Bilal?

Bilal Sayyed:

Thank you, Peter. I am senior competition council of TechFreedom. Timely and stable guidance with respect to privacy in the collection use and security of data is necessary, but the scope of the ANPRM and the three-two vote on its release indicate that the commission has embarked on a path with little likelihood of providing this guidance in a timely manner or in a manner that withstands changes in commission makeup and leadership. The commission should rethink its approach. It would be far better for the commission to provide a policy statement on privacy and data, or alternatively, a statement that identifies with specificity, how the principles and the deception and unfairness statements will be applied in such manners. A policy statement will provide substantial guidance to attorneys' privacy officers, with many firms likely to conform their behavior to the principal's underlying statement and to the Congress. Consumers benefit when commission guidance is grounded in core principles of consumer protection, support for vigorous competition, cost-benefit considerations, materiality of harm and robust economic analysis.

This a statement should reflect the principles of consumer welfare, reasonableness, countervailing benefits and economic analysis that are reflected in the deception and unfairness statements in the FTC Act. A statement is a legally sound approach and unlikely to lead to the litigation delays associated with an administrative rulemaking. A statement also provides more flexibility in addressing new issues and incorporating new information and academic and empirical research into decision-making. The commission should work to make such a statement unanimous to better provide certainty to firms and consumers, and so the statement has a reasonable chance of withstanding changes in commission leadership and members. Each commissioner and the agency has significant experience with privacy and data issues. Accordingly, the commission should act quickly to identify its framework and support for that framework for deciding matters within the scope of its legal authority in this area. Thank you.

Peter Kaplan:

Thank you, Bilal. Our next speaker is Kaliya Young. Kaliya?

Kaliya Young:

Thank you. My name is Kaliya Young and my online handle is Identity Woman. I've been working for 20 years on the challenge of how people can control and represent their digital selves online with dignity and be empowered. I co-founded the Internet Identity Workshop in 2005 and continue to convene it every six months. A lot of the questions put forward relate to regulating how bad things are happening by companies to people. I also encourage the FTC to take a forward-looking approach by considering the work of values-based technical communities working in alternative mechanics for data sharing between companies and consumers.

Two projects I advise, Dazzle Dow and Jlinks, are seeking to end surveillance capitalism via open standards and open source tools to give people the ability to collect all the data they generate in the digital world, tools to organize and get value from their own data from a variety of sources, along with ways for them to share data with companies they trust with new mechanisms to technically resolve, withdraw consent and companies having information. Rulemaking should make sure to support these positive, constructive efforts of ethical technologists.

I also want to make another point. The risks of technology are often not seen until it's too late. I want to bring to the commissioner's attention a key issue that they could help with under rulemaking related to data security and specifically as it relates to the emerging technology of digital wallets needed for the exchange and sharing of data between consumers and companies with protocols like verifiable credentials. There is a very real risk that because two companies control the mobile handset operating systems, Apple and Google. They will work with to limit access to the APIs within the phone, preventing any wallets created by any other companies from working well. This does not have to happen. The risk of it happening will be reduced if the FTC gets involved to ensure a level playing for wallet makers, ensuring consumers will have a choice of who they trust with a very sensitive data they will be sharing as they use this tool to transact across the digital world. Thank you.

Peter Kaplan:

Thank you, Kaliya. Our next speaker is Chris Weiland. Chris?

Chris Weiland:

Hi. Apologies, I don't actually own a webcam, so just enjoy the blank screen for a bit. My name is Chris Weiland. For my day job, I'm a freelance penetration tester and consultant, and I am also the chair of Restore The Fourth Minnesota, a grassroots advocacy group that fights against mass surveillance. A lot of great comments have been raised about the importance of privacy and the importance of implementing some rules and guardrails around public check corporate surveillance, but I would like to point this commission's attention to the existence of address confidentiality programs in, I think, more than half of the states, where victims of domestic violence, sexual assault, stalking, or other types of crime, they can apply to these programs to receive mail at a confidential address while keeping their actual address undisclosed.

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 gap in existing law, where young consumers who are using FinTech payment apps or debit cards can have their purchase history sold to data brokers unless their parents have proactively opted their child out in the selling of their data. This gap is especially harmful as we move toward a cashless society and trend accelerated by the pandemic. Children today frequently engaged in financial transactions with digital wallets and debit cards, both online and in stores. Unfortunately, some operators of FinTech apps targeting children may be exploiting this gap to user sell the data of their kids they are currently courting for their services. Nowhere in the ANPR is there a question about the impact of FinTech on children's privacy. That is why I was pleased to see the Senate version of COPPA 2.0, including an amendment by Senator Blackburn, authorizing a GAO study on minors' privacy who are using FinTech products.

This first of its kind study will identify the type of FinTech products minors are using, identify potential risks to minors, privacy from using such FinTech products and determine whether existing laws are sufficient to address such risk. It is possible to go beyond what's currently legally required. For example, REGO Payment Architectures has incorporated child privacy by design into its Missoula FinTech app and pay button and collects no information on the child. As the FTC focuses on children's privacy, it should include the FinTech child protection gap and the harm that can be caused by the collection and misuse of a minor's financial purchasing habits, especially when a child's financial history can be so easily combine a young person's social networking and browsing history. Thank you.

Peter Kaplan:

Thank you, Rick. Thanks a lot. Our next speaker is Jacob Dockter. Jacob?

Jacob Dockter:

Hi, can everybody hear me?

Peter Kaplan:

Yes, we can hear you.

Jacob Dockter:

Perfect. Thank you so much and thank you to the FTC for hosting this panel. I start by admitting from the top that while I work in tech, I am not an expert in commercial surveillance or data security. I defer to the profound and impactful work of many of the other organizations here and ask all of you to reach out and listen to and seek advice from groups like Acre, the Athena Coalition, Lucy Parsons Labs, Carceral Tech Resistance Network, MacArthur Justice, and many others. Where I do speak is as a concerned citizen, sharing from the heart about the use of these technologies that are sold to police for the surveillance and collection of data against communities. As a Portlander and carceral abolitionist, I speak from my context where our city has lived through count use years of brutality, both direct from the brutal baton of our own police officers and indirect harm from the countless invasions of homes and rights by law enforcement and the myriad companies enabling further harms.

In 2012, the U.S. DOJ filed suit against the Portland Police Bureau due to a pattern and practice of brutality against those in mental health crisis. Now, 10 years later, the DOJ has stated that Portland Police Bureau is moving further away from compliance and our police have shown to be found to rely on racial profiling, have known members of extremist groups. One member is currently known to be a supporter of the insurrectionist Oath Keepers and has maintained their job. Now, before repair of these harms, companies like ShotSpotter and many other surveillance and data security companies are seeking contracts, giving more tools to attack our communities.

In 2020, federal police came in unmarked uniforms gassed Portlanders, flew drones, piloted surveillance planes over our homes and left thousands harmed while the Federal Protective Services, ICE and DHS avoided accountability. Our community asks for substantive change. Before we expand the tools and access that give law enforcement more ability to harm, to track and to invade our data. We see the expansion of tools to attack our neighborhoods, but we do not see accountability, reparations, or truth-telling.

I hope to end with a quote from the great Ella Baker that we can leave here, where she said, "Those of us who are not yet ready for the burning will go to our city halls, go to our mayors and to our governors and even to our federal government," that's you, "and question why so much artillery," I will add mass surveillance technology, if you forgive me, Ella Baker, "is being brought and stacked and stopped to deal 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 subject to a rule. If case-by-case enforcement has already effectively deterred harmful practices, they won't be widespread enough to justify a rule. To ensure that its rules survive judicial scrutiny, the commission must do what it's done in every past magmas rulemaking, focus on discrete, egregious practices that clearly harm or deceive consumers. Of course, it should continue to police hard privacy questions case by case, but it should lead major questions around privacy to the elected representatives of the American people. Thank you.

Peter Kaplan:

Thank you, Berin. Our next speaker is Dr. Roxana Mirachi. Roxana?

Dr. Roxana Mirachi:

Thank you, commissioners. My name is Dr. Roxana Mirachi. I'm a professor of education data privacy researcher at San Jose State University, speaking today as a private citizen, not on behalf of my university. An area of emerging technologies in need of urgent regulation involves blockchain-based 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.

Let me be clear, how we protect kids here in the U.S. has implications for kids around the globe. More than 80% of the world's ed tech products that we reviewed send children's data to at least one American ad tech company. And so, the one thing I'll stop review with is that behavioral advertising to children should be banned. Commercial interest and surveillance should never override a children's best interest or their fundamental rights because children are priceless, not products. Thank you.

Peter Kaplan:

Thank you, Hye. Appreciate it. Our next speaker is Jolina Cuaresma. Jolina?

Jolina Cuaresma:

I'm Jo Cuaresma, senior council for privacy and tech policy at Common Sense Media, America's leading independent nonprofit organization dedicated to helping kids and families thrive in an increasingly digital world. At Common Sense, we're deeply concerned about the actual cost of so-called free online platforms. By merely engaging on a platform, users produce millions of data points about themselves, yet they have little say over what happens to this personal info that's automatically being generated. Tech firms collect these millions of data points, and with machine learning algorithms, they draw inferences about each user, their likes, their dislikes, their insecurities, their beliefs to create individual profiles. Depending on the profile, platforms curate what content a user will see next. Why the individualized experience? Well, it's to keep users engaged on the platform longer and all the while users have no ability to stop generating personal information that they have no control over.

Online platforms aren't free. In exchange for users' time and attention, advertisers pay platforms millions of dollars each year, while our children pay with a much higher price, their mental health and wellbeing. We know from countless studies that online platforms can lead kids into a downward spiral. Take for instance teenager Lauren Hemming, who during the pandemic downloaded TikTok for fun. First, she saw videos of families dancing and comedy skits. Then she saw a video by a fitness influencer who tracks her food intake. Lauren followed her and shortly thereafter, the platform's algorithm began recommending similar fitness and calorie counting videos. Unsurprisingly, Lauren began obsessively counting calories herself. She now hated her body, crying nightly. Within four short months, she was diagnosed with an eating disorder. This is simply unacceptable. I am grateful to the FTC for its efforts to learn more about the effects of commercial surveillance on our kids and teens, and how we can better protect our children. Thank you.

Peter Kaplan:

Thanks. Our next speaker is Tim McGuinness. Tim?

Tim McGuinness:

Thank you. Good afternoon. I'm Dr. Tim McGuinness, chairman of the Society of Citizens Against Relationship Scams, a nonprofit supporting and representing over 50 million online abuse and crime victims. We encourage the commission to use the lessons of HIPAA and GLBA for how to control privacy and limit data sharing and impose security for their rulemaking framework and even the umbrella under those statutes. Do not forget that almost all platforms and apps are also products and may also be regulated by consumer product safety statutes. Specifically, we recommend unlimited

Tim McGuinness:

Unlimited collection of user data has led to criminal activity that has harmed almost all consumers worldwide. Current internet data security has failed. We recommend a complete ban on the collection 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:

Our next speaker is Evan Colvin. Evan?

Evan Colvin:

Hey, good afternoon. My name's Evan Colvin. I'm a contractor with Shaw Communications, but please note that I don't represent or speak for them. I've worked in the analytics space for about five years now as a data scientist and a data engineer in the machine learning and big data space. I've never worked for a data broker, but I know people in that space and always been a little uncomfortable with what they'll just tell me in casual conversations. A lot of people are talking about tech companies here, but I also want to mention the credit rating agencies. Equifax, a few years ago had a horrific data breach and I don't really think they faced the consequences they should have for exposing a couple of hundred million social security numbers. From what I can tell, California and Colorado's privacy legislation seems to exempt credit rating agencies. This could allow them to do anything they want with non-financial data that should be protected and is intended to be protected, and undermine ongoing and future privacy endeavors.

I've also noticed smaller companies popping up that offer services like reporting rent and utility payments to credit agencies, and they say it's to help boost consumers credit scores for paying their rent on time. Of the companies I've looked at, they just seem like run of the mill data brokers to me. I think some of these companies want to get into the financial information space so they can say they're actually credit rating agencies and then get around current and future privacy rules saying they don't apply to them. This is probably not what we want. I hope you'll keep this in mind as you consider solutions to privacy problems. Thank you for hosting the meeting and taking public comment.

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 making inferences based on that analyzation of that data and selling those inferences completely without any visibility on the part of the consumer. And it's not just a matter of visibility, even when consumers try to gain an understanding of who has their data and how it is being used, they're faced with an implacable wall preventing them from gaining that access on the most basic of requests.

If the commission is looking to actions to take, increasing the visibility to consumers of the aggregation, transfer and retention of their data is an important first step toward the average consumer gaining and understanding of the commercial surveillance they are under. While everyone here today understands the scope of this problem, the average consumer does not. Changing the visibility of commercial surveillance to increase data transparency to the consumer will help empower them to make better decisions on how not only to use their own data, but also to improve understanding of how data is being misused for those who need the most protection. Thank you.

Peter Kaplan:

Thank you, Fred. Our next speaker is Brandon Pugh. Brandon?

Brandon Pugh:

Hi. Thank you Peter and commissioners. Good afternoon. My name is Brandon Pugh. I'm a senior fellow and policy council at the R Street Institute and the cyber team where I lead our data privacy and security efforts. Our team has devoted significant time to data proxy, especially in the nexus between national security and cyber security. We also released a multi part report on reaching consensus to traditional roadblocks to data privacy and security legislation this year, and we had a section outlining ideas for the FDCs role over privacy rule making and enforcement. So we are submitting written comments to the ANPR, but I'll highlight a few brief points. Overall, we share the FDCs view that clarity and additional protections when it comes to data privacy and security are helpful, but we have some concerns. First, we believe the ANPR is premature in some areas given that Congress is actively considering data privacy legislation, especially considering the ANPR seeks to answer select major policy questions that would significantly impact industry and security.

We believe Congress should articulate defined areas appropriate for rulemaking and that there is value in a federal comprehensive privacy and security legislation, in contrast to a patchwork of state and agency rules. Second, we believe the ANPR is too expansive. It focuses on nearly all aspects of privacy and security without clear focus and arguably in areas there's not clear authority to do so. However, we do believe there are steps that can be taken. For instance, data security is an area that the FTC should focus on and consider further action. This is an expanding concern and there's uncertainty on what is reasonable. The ANPR devotes minimal attention to data security and cyber, the R Street Institute remains willing to be a resource as you consider further action. Thank you.

Peter Kaplan:

Thank you, Brandon. Our next speaker is Edward Hasbrouk. Edward?

Edward Hasbrouck:

Thank you. My testimony will focus, and my written comments respond to two of your questions. First, what are the harms that consumers may not readily discern? My answer is that consumers are generally unable to discern the threats posed by data, the data collection when they're not able to see all of the data that is being collected. Subject access rights are sometimes wrongly perceived as secondary to other aspects of privacy and security, but in practice, subject access rights are a prerequisite to informed consent, meaningful choice, threat assessment, or damage mitigation. Time after time, what I've seen as a technical expert, as an investigative journalist and as a consumer advocate is that consumers cannot 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.

Second, what areas have not been addressed sufficiently by the commission? To date, the FTC, the Department of Transportation and the FCC have failed as a result of jurisdictional gaps or uncertainties to adequately address privacy and security violations committed by transportation and communications carriers and their service providers. The jurisdictional problems and potential gaps between the FTC and the FCC with respect to communications carriers were noted in a report by your staff last year. The jurisdictional problems between the FTC and the DOT over transportation carriers are equally longstanding and even more severe. These issues were pointed out in submissions to the FTC in 2009 and to the DOT in 2013 by consumer, civil liberties and privacy advocates, but there has been no progress. Airlines and the computerized reservation systems that host sensitive personal data on their behalf continue to exemplify a worst case scenario of insecure practices. I urge the FTC to prioritize one, enforceable subject access rights and two, closing the jurisdictional gaps and uncertainties related to transportation and communications carriers and their service providers including computerized reservation systems. Thank you.

Peter Kaplan:

Thank you, Edward. Our next speaker is Gene Radin. Gene?

Gene Radin:

Thank you. My name is Gene, and I'm the head of product for a startup that collects and processes sensitive data. I've spent the last 15 years or so working in product management roles where I've been responsible for the design and delivery of digital products that depend on or generate sensitive data. It is not, in my view an overstatement to suggest that the future of humanity will be impacted directly by the decisions that this committee will be making. What's at stake is the difference between common prosperity and increasing exploitation of people for profit. Fundamentally, a free and fair society cannot exist without privacy. The background that you see on my video along with other signals that can be collected from this video feed and my network connection can be used to judge me and put me into various categories, including on the basis of age, sex, and wealth.

There are companies now who are selling people on the idea that they can reach far more invasive deductions based on this data, putting people at risk of having their health and mental state judged along with a litany of other factors. In fact, this feed is enough for someone to produce audio and video of my likeness doing anything they want, and the repercussions for doing such things are somewhere between unclear, ineffective and simply nonexistent. There are too many privacy risks to list to tie privacy concerns and our collective exposure to data collections and analysis, but I will mention that the proliferation of financial fraud, revenge porn, digital addictions, physical targeting of individuals and human trafficking can all be mitigated with the rules that the FTC can develop and enforce. I will close with a few examples of concepts that I hope that the FTC will consider in its rule making process.

Any company collecting data must have baseline secure systems that are tested for vulnerabilities regularly. Establish simple rules around retention of all data from and about people. This information cannot be collected without a policy to enforce its deletion at an appropriate time. Ban emotional manipulation and require that any related data collection is done with informed but not forced consent, with an option to opt out at any time. Require companies that maintain consumer accounts to let people easily delete them, and all associated data that's not legally required to be retained. Set up a process to measure the impact of these policies with regular reviews to improve them. Finally, I would suggest to focus on incentivizing the people and companies who do right and want to do right by others.

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 the American economy that enhances the quality of life and functions in manner that does not threaten the privacy of individual citizens. The FTC should also include exemption language for surveying, mapping and geospatial data collection related services in the rulemaking, and by doing so, the FTC would effectively be codifying the rendering provided by Chairwoman Ramirez in 2014 and consistent with current exemptions found in the American Data Privacy and Protection Act.

Legislative and regulatory efforts to protect consumers and citizens in the name of privacy have cast two wide a net, creating unintended consequences for surveying map and geospatial firms. Geospatial data is derived from images and data collected from a variety of airborne and spaceborne platforms, as well as other mobile and terrestrial based acquisition systems. This imagery data is regularly and historically collected, utilized and applied in geographic information systems, GIS by companies engaged in free market commerce and by government authorities operating within the safeguards, rights and framework established by the fourth and 14th amendments to the constitution of the US. Thank you very much for this opportunity to provide our views.

Peter Kaplan:

Thank you, John. Our next speaker is Edwards Reed. Edwards?

Edwards Reed:

Hi, I'm Ed Reed with Aesec Corporation and Gemini computers maker of the GemSeal Security Kernel and trustworthy computer systems that use it. I'd like to thank the commission for this opportunity to comment on the specific topic of lax data security. My information technology industry experience spans more than 47 years working at large corporations and vendors like Xerox and Nobel. For the past 22 years, I've worked to make effective use of Gemsys, a secure operating system to support systems that substantially mitigate the risk of subversion, what you would call malware in critical systems. Science has made one thing abundantly clear, security for computer systems built without a trustworthy operating system is simply impossible. It is in this context, security means the ability to control access to the system and its data. Access control is at the heart of data security and lax data security is the failure to prevent unauthorized access to data.

We know how to control access to data in secure computer systems. Multiple complex systems have successfully demonstrated the required science and engineering in deployed systems, but industry has chosen to prioritize other things instead. Industry pretends that we're doing the best we can, but that's not true and it is dishonest to tell consumers and regulators that the best practices relying on penetrate and patch products can prevent unauthorized access to consumer personal data. The commission should make rules that encourage data stewards to do two things. First, protect private data using secure operating systems that verifiably enforce mandatory access controls and second, hold data stewards accountable by requiring inspectable audit records of each transfer of private data from one security domain such as storage to another like partners and analytics. Such incentives can substantially mitigate lax data security risks, allowing the commission to address other priorities such as the misuse of consumer data. I thank you for your time.

Peter Kaplan:

Thank you, Ed. Our next speaker is Dan Frechtling. Dan?

Dan Frechtling:

Thank you, Peter. Chair con, commissioners and staff. I'm Dan Frechtling, CEO of Boltive, a software company that helps other companies fix consent errors and data leakage online. Consent errors happen when consumers opt out, but the signal is lost in handoffs to third party vendors. This happens 100 times a day to the average US consumer. Also known as dark signals, these cause opt outs to vanish, vendors collect personal information contrary to consumers request for privacy. When we unpack consent errors, it's a combination of two things, consent technology and the network of partners that websites integrate with. Consent technology like consent management platforms have errors at average around 20% and the network error rate is around 24%. Together, it's a combined average error rate of 37%, and this leads to some examples of harm. For example, we helped a hospitality company discover that they had unknown parties including a malware distributor skimming user data.

We did a review with a wireless company and in tracing their parties led to Segmento owned by Russia's Sberbank, which was on a list of sanctioned entities after the invasion of Ukraine, but was still receiving personal information through online advertising. How can the FTC address commercial surveillance that occurs through unauthorized sharing of personal data? One, ensure rule making prohibits consumer opt outs from being lost in transmission between vendors. Two, require testing and auditing of business' own consent systems and their third party vendors to make sure the data isn't improperly shared, and three, avoid safe harbor clauses that could cause neglecting of testing for third parties. With FTC guidance and rule making, businesses can ensure consumer opt outs and data sharing are compliant and proper. Thank you.

Peter Kaplan:

Thank you, Dan. Our next speaker is Doug McCluer. Doug?

Doug McLuer:

Hi, my name is Doug McCluer. I'm a software engineer. My comments today are my own and don't represent the views of any company. I thank you for your attention to this important subject and I apologize for rushing. Two minutes is not a lot of time. I encourage you to record this and replay it on half speed. Consent is not the answer. Some of these companies are monopolies and opting out is effectively impossible, even if it weren't. Most of us can't understand what we're consenting to. In order to even be able to attribute harm and address the questions the FTC is asking today, we need more focus on enabling accountability through enforcing transparency. A major enabler of harmful surveillance is developer's reliance on third party SDKs where even the developer of the app has no idea what the third party is collecting. In certain cases, this is by design and a good thing, but in other cases, the developer becomes an unwitting Trojan horse.

In all cases, the subject of the data collection needs to be able to see what's being collected and by whom, and I think we can facilitate that by enforcing three rules, not necessarily with this language. Rule number one, any software product must disclose all third party SDKs, libraries, scripts or services that go into it. Specifically and by unique name and version number and must provide these disclosures before transferring any data from the end user system or modifying its files. Rule number two, any software, and that includes SDKs, libraries, et cetera that collects data must provide the subject of the data collection the ability to view that data in its unencrypted, unobfuscated form and to securely log it before it is collected. Rule number three, the exact same means used by the software to encrypt or obfuscate data prior to transport must be made available for the user to encrypt arbitrary data supplied by the user.

For example, if the software uses asymmetric encryption, the public key used must be provided along with the plain text from rule number two. This is to support the ability of the user to re-encrypt the plain text produced by rule number two, compare that to what's in their network logs and verify that it matches and there's no additional hidden data collection taking place. What this gets at in plain English 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 after another recent software update by one of the largest device manufacturers in the world. I've found myself yet again going through the new features and turning off the collection of data including on device learning by its AI assistant for the benefit of my purported preferences. After more than 40 hours of systematically documenting this process, my high level findings include pervasive surveillance controls are turned on by default and return to on by default after security updates, which often include new features and feature bundling, presumably a justification for resetting of privacy preferences without notice to the consumer. Surveillance controls are ubiquitous. For example, one would expect that if they turned off the AI assistant, then it would indeed be turned off, but that is not the case.

If the consumer uses any one of the many obscured features of the AI assistant, which one must dig to discover in a maze of hundreds of privacy policy pages, such as using the flashlight or the browser search bar, this directly contradicts the manufacturer's marketing messages wherein it repeatedly telegraphs it does not intercept such sensitive and private data. Big tech uses algorithmic memorization to get around regulatory requirements relating to data collection, processing, storage and transfer. Other data collected includes digital exhaust, pattern of life and the treasure trove of telemetry data, a process known as digitizing in real life. This data is not only a proxy for identifying the consumer, but it forms a digital twin for the consumer that owns the device. And the current state is beyond and reasonable to socialize risk to consumers, and I'd also argue citizens in the context of platforming, local government and the model of shared responsibility. Thank you.

Peter Kaplan:

Thank you, Jody. Our next speaker is Ridhi Shetty. Ridhi?

Ridhi Shetty:

Thank you for the opportunity to comment today. My name is Ridhi Shetty and I'm a policy council on the Privacy and Data Project at the Center for Democracy and Technology. CDT welcomes the commission's efforts to protect consumers from data harms that constitute unfair or deceptive practices. We urge the commission to ensure its rule making addresses enforcement gaps that affect marginalized and multiply marginalized consumers. For example, targeted ads are delivered to subset of consumers based on consumer activity on advertising platforms and third party sharing of data that consumers provide for purposes unrelated to advertising. Targeted ads for dangerous products have a 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, calling on the commission to address, for example, mobile device tracking, behavioral and programmatic advertising, the role of apps gathering geolocation, harvesting of health data, the ways racial and ethnic data are leveraged. We urge them to oppose the big data buying sprees by Google, Meta, Amazon, Oracle and others.

Today, Americans are exposed to significant risks regarding their health information, financial security, wellbeing of their children, and are at the mercy of a platform and data partnership combine that is manipulative and discriminatory. The structure of our political advertising, news and information systems, in addition to eCommerce and other consumer services, have been warped by the influence of the surveillance marketing apparatus. This rule making of the [inaudible 04:03:23] shows those days should be over. However, the online data marketing industry has worked to ensure continued methods of surveillance regardless of what laws or rules are enacted, which this rulemaking must address. Practices such as the embedded use of opt in first party data, cross device identity profiles built from streaming video and retail media network data, using machine learning to generate predictive 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 addressed by the forthcoming rule. We expect this FTC to stand up for privacy, consumer protection, and digital and civil rights. Thank you.

Peter Kaplan:

Thank you, Jeff. Our next speaker is Mona Kanna. Mona? Mona, are you on? Okay. If Mona is not available, we'll move on, and our next speaker is David LeDuc. David?

David LeDuc:

Hi, My name is David LeDuc and I'm the Vice President for Public Policy at the Network Advertising Initiative. We appreciate the opportunity to participate today. The NAI is the leading self-regulatory association for advertising technology companies in the United States. For over 20 years we've developed and evolved the

David LeDuc:

The highest voluntary industry standards for the collection and use of consumer data which, in many cases, extends beyond current legal requirements. Our industry leading code of conduct has strengthened industry practices and has become a requirement of partnerships for many publishers and advertisers across the industry. Industry self-regulation, however, has limitations. As a result, we are leading proponents of a comprehensive consumer privacy law that provides strong, consistent protections for all Americans, while preserving digital advertising and other beneficial uses of consumer data and empowering self-regulation to help enforcement.

Tailored advertising powers the market for free and low cost content that consumers rely on for news, games, email, and more. Small and medium businesses, particularly, rely on digital advertising to compete with larger entrenched competitors. A new regulatory approach that seeks to ban data driven advertising, either completely across all digital media or the processing of data by third party partners, would limit consumer access to free and no cost digital content. And this would harm competition, ultimately reducing choices for consumers, and consumers would lose.

Instead, the FTC's regulatory efforts should be focused on preventing measurable and systemic harms and providing greater clarity to businesses about the application of the commission's enforcement authority over deceptive and unfair practices, balanced against the robust examination of the benefits of data-driven advertising for consumers of small businesses. Again, we appreciate the opportunity to participate today and look forward to engaging and submitting detailed written comments. Thank you.

Peter Kaplan:

Thanks, David. Our next speaker is Zach Davis. Zach?

Zach Davis:

Hello everyone. My name is Zach Davis and I'm a 20 year old tech entrepreneur and the CEO of Brime, a live streaming platform. I'd like to thank the FTC for organizing this for all of us to share our input and concerns as everyday American citizens, and of what we've experienced in this ever evolving technology driven world. I, like many other Americans, have concerns for the data that we entrust with platforms. More specifically, I would like to voice the concern of foreign applications that may be violating the privacy and security of tons of millions of Americans. Just recently, Buzzfeed released a report of audio from AD internal meetings at TikTok, which is owned and operated by its parent company, ByteDance, headquartered in Beijing, China. Repeatedly accessed the information of American user data, and I quote, "Everything is seen in China," said a member of TikTok's trust and safety team in one of those meetings.

I believe this is a particularly concerning issue because TikTok testified to Congress that American user data would stay in America and gave false assurances that it would not be accessed remotely. With the release of this article by Buzzfeed, FCC commissioner, Brendan Carr, asked Google and Apple to remove TikTok from the app stores due to its blatant violation of American citizens privacy. This is bipartisan as well. Democratic Senator Mark Warner, and Republican Senator Marco Rubio, sent out a letter to the FTC raising their own concerns about TikTok's security.

I ask that the FTC look into making rules that regulate and enforce foreign applications and technologies that pose serious security risks to Americans. I also ask the FTC to look into how embedded in-app browsers track users. On August 19th, the New York Times published an article about how TikTok's in-app browser tracks the keystrokes of users, as found by a privacy researcher, Felix Krause. I thank you again for your time today and I hope that the FTC shares these similar concerns. Thank you.

Peter Kaplan:

Thanks, Zach. Our next speaker is Rich Jones. Rich?

Rich Jones:

Hello. My name is Rich Jones. I am a software developer and startup founder who has worked on pro-privacy nonprofit projects and anti-privacy for-profit projects. I'm here to demand that all commercial surveillance be thoroughly and immediately criminalized to the fullest degree. This is not only my opinion, it was also the conclusion of [inaudible 04:09:22] audit, the Norwegian equivalent of the FTC, which called for a full ban on commercial surveillance for the purposes of advertising.

They recently released two English language reports, which I encourage you to read. One titled, Out Of control, another titled, Time To Ban Surveillance Advertising, the findings of which were that commercial surveillance is a tremendous harm to society and provides a net negative benefit to the economy.

Three of the many harmful findings which the report found, I'd like to highlight. Manipulation. The fundamental purpose of commercial surveillance is to manipulate behavior, a violation of our right to live freely and without interference. This manipulation affects all of us, but the harm multiplies with vulnerability. As one of countless examples, online casinos were found to routinely target those with prior gambling addictions.

Second, discrimination. Segmentation of people by race, class and other protected status, either directly or by proxy, is a key capability offered by ad targeting vendors and is routinely used for discriminatory targeting of consumers. As an example, Facebook recently paid a fine of only $100,000 for facilitating race based housing discrimination, which amounts to less than one minute of their revenue.

Three, erosion of social trust. At the end of the day, everybody knows this is creepy and doesn't like it. We all feel spied upon and we all feel tricked. This undermines fundamental trust in government, in business, and in society at large. There are no tangible benefits to the public and only benefits to parasitic corporations, many of which are benefiting from large scale fraud.

Society would be freer and happier if commercial surveillance was criminalized. If the practices that these companies routinely engage in were done by ordinary people, they would meet the criteria for criminal stalking and harassment. I know from having worked in this industry for nearly two decades that whenever people's data can be exploited for profit, it will be. And then that exploitation will be lied about by industry representatives who use weasel words like, 'pro-ecosystem,' 'diversity of choice,' and, 'enhance the end user experience.' The industry has shown no ability to regulate itself as shown by the fact that many of the other speakers here today have been working for nearly 20 years. The cost of funds is-

Peter Kaplan:

Thanks, Rich. Thanks. Sorry, you're over time. Thanks, though. Our next speaker is Sheila Colclasure. Sheila?

Sheila Coldasure:

Hi. Thank you so much. I am Sheila Colclasure with Interpublic Group, where I concentrate on Kinesso, our responsible advertising service engine built on the ethical use of data. We have long supported passage of responsible and balanced federal data privacy law and regulations, so long as those rules simultaneously protect individuals and support a robust competitive connected marketplace. That marketplace simply cannot exist without marketing and advertising that relies on the use of personal data.

A fair marketplace also depends on accountable and ethical marketing and advertising solution providers. Rules are needed to avoid consumer manipulation and stay on the side of persuasive selling. Those rules must be nuanced enough to encourage responsible behavior and penalize bad behavior. The rules that result from this process will not only impact individuals and their data, but also competition and our American economy. Any privacy regulation is also inherently a competition regulation.

This process has been framed around commercial surveillance, which connotes monitoring illicit activity of a targeted individual. Responsible marketing and advertising solution companies do not survey people, they use technology that observes to serve. There is no question that observed data is extremely useful to linking the consumer with the seller to serve the interests of both.

For more than 25 years, we at Interpublic Group, have been designing and implementing ethical data systems for marketing and advertising to assure we properly balance this equation. Not everyone recognizes the need for this balance, so rules are needed, preferably a federal law, but rules should both protect individuals and the marketplace and advertising benefits. We need a law that is better for America and better for Americans. Thank you for your time.

Peter Kaplan:

Thank you, Sheila. Our next speaker is Leonie Haimson. Leone?

Leonie Haimson:

Yes. Hello. Thank you so much for holding these hearings today. My name is Leonie Haimson. I'm the co-chair of the Parent Coalition for Student Privacy. Since Congress passed COP in 1998, the use of ed tech apps has flooded schools, among them, controversial behavioral and biometric tracking and surveillance programs. Insufficient oversight by the FTC and other agencies have allowed children's personal information to be breached, commercialized, and otherwise abused. The lack security provisions in COP and the absence of any FERPA, has led to an explosion of breaches with the personal information of millions of students subject to ransomware, malware and other cyber attacks.

Federal laws are especially weak when it comes to the use and disclosure of personal student data as there are gaps in both FERPA and COP and the intersection between them is often unclear. But even so, 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.

Peter Kaplan:

Thank you, Elif. Our next speaker is Jordan Crenshaw. Jordan?

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 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 would've done so like it did under KAPA and GLBA. Congress is currently working on complicated issues regarding tradeoffs under the proposed American Data Privacy and Protection Act, a bill that the FTC said it would consider changing its approach for. It passed. Why change course if Congress has already clearly spoken to give the commission authority to make broad rules.

The business community takes issue with the commission unfairly referring to its potential rules as those concerning commercial surveillance. This is clearly a privacy, security, data and algorithmic rule making. The term commercial surveillance connotes that the use of consumer data is negative. If a rule making was lawfully held, the FTC with objectively and independently be required to look at both harms and countervailing benefits.

For example, data is being used to secure networks, promote financial inclusion and improve healthcare outcomes. It is also helping small businesses survive and drive through things like tailored advertising, a practice 77% of Americans prefer. We urge the FTC to wait on Congress, as constitutionally required, to pass a true, clear and workable national privacy law that protects all Americans equally. And to follow the FTC acts requirements by remembering the tremendous benefits consumers derive from our data economy in any unfairness enforcement proceeding. Thank you.

Peter Kaplan:

Thank you, Jordan. Our next speaker is Benjamin Gaines. Benjamin?

Ben Gaines:

Hi, good afternoon. My name is Ben Gaines and I'm the CTO for a lower middle market private equity firm. And as such, my opinions are my own, but I hope to represent a few points from private industry that maybe is not already present in this panel. First, I want to thank the FTC, and I really mean that. I view the entire FTC as just patriots in preserving the fundamental American right to privacy and freedom.

As the FTC pursues potentially making policies and standing rules, I would encourage, please don't abandon the case by case penalties that are being used right now. They are effective and I'll give you just an anecdote from my viewpoint and how we operate, on why. Presently, we go to the FTC's website every week and we look to see who's been penalized for what. And it's often ambiguous, at least in the writeup, and it causes us to ask meaningful questions about how we operate. And not questions about policy and how can we avoid it and maintain a checkbox, but how are we actually operating and is this 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, Davis and my lab conducts research to investigate consumer privacy issues. I want provide my input to the commission from the perspective of the academic research community. One, the commission asked about biometric information collected and used by companies and whether consumers are typically aware of that collection and use. I want bring attention to recent academic research that has uncovered serious privacy issues with voice information collected by voice assistance and smart speakers. The convenience of voice input has contributed to the rising popularity of smart speakers, but it has also introduced several unique biometric privacy threats. Recent academic research has shown that smart speakers use voice data, directly or indirectly, to infer user interests and use it to serve behaviorally targeted ads. This is despite them making deceptive public promises that they do not use this information to target ads. The commission should strongly consider biometric information collected, processed and shared by smart speakers and voice assistants, in its rule making efforts.

Second, the commission also asked which practices do companies use to [inaudible 04:27:18] consumers? I want to very briefly mention that as third party cookies and mobile device identifiers are being phased out, academic research has shown that companies are resorting to new techniques for cross site and cross device tracking; such as first party cookies, which are now being used on more than 90% of top 10,000 websites, and browser fingerprinting, which is now deployed on more than a quarter of top 10,000 websites on the web. In summary, academic research is showing that many companies are actively attempting thwart privacy protections against cross site and cross device tracking. This has led to a technical arms rates, and I believe the commission should pay special attention to such circumvention attempts in its rule making efforts, because they seriously undermine consumer privacy efforts in the short term and the long term. Thank you.

Peter Kaplan:

Thank you, Zubair. Our next speaker is Paul Lekas. Paul?

Paul Lekas:

Chair Khan and members of the commission, thank you for allowing me to speak today. My name is Paul Lekas. I head public policy at the Software and Information Industry Association. We are the principle trade association for those in the business of information, representing over 450 large and small companies including publishers, platforms, analytics firms, education technology companies and others. We appreciate the commission's attention to consumer privacy and the security of consumer information and we recognize the risks associated with this collection and usage. We've long advocated for a national data privacy standard as essential for US businesses and consumers, and for the United States as a global leader in digital democracy. We also support measures to protect student and children's privacy and appreciate the commission's focus on this population.

As this rule making process unfolds, we urged members to reconsider the framing of this issue around commercial surveillance. As defined in the ANPR, this includes all collection, aggregation, analysis, retention, transfer or monetization of consumer data, and the direct derivatives of that information. This definition covers virtually all consumer activity, as well as a large swath of commercial publishing in the United States today. And without tailoring, it is too broad and ambiguous to provide meaningful guidance to consumers or businesses or to comport with First Amendment.

The term mistakenly presumes that all such activities are inherently bad. Businesses use consumer data for many purposes that enhance consumer welfare and respond to consumer demands. This includes using data to improve the quality of services, protect against harmful content and security risks, and deliver personalized services that directly benefit consumers. The commission must balance privacy rights, consumer needs and safety, including the need to safeguard the public, at large, from fraud. We commend the commission on its recent actions to enforce rules against deceptive and unfair business practices, while respecting undue burden on legitimate business activity. We look forward to engaging further with the commission. Thank you very much.

Peter Kaplan:

Thank you, Paul. Our next speaker is Leela Krishna. Leela? Leela, are you there?

Leela Krishna:

Can you hear me, sir?

Peter Kaplan:

Yes.

Leela Krishna:

It is morning here in India. Basically I'm pursuing my PhD in cyber information security and I started doing research on the data production rate aspects, and I'm doing research on the FTC and a combat analysis on GDP as well. So the main issue, which is mainly concerned with the privacy regulation legislation, is that it must go beyond the notice and choice perspective, protect the rights of the individuals. So in the [inaudible 04:31:17], in the preamble, I have seen in there, the fundamental values is to protect the rights and the dignity of the individual.

But the recent legislation, which is that bill which is drafted by the federal, I couldn't see any form of preamble which could state that it can move beyond consent. So the main problem which arrives here is that, to stop and to curtail the disapproved practices, say, the tracking devices, and to protect the minors and children from the tracking. And to please, one has to protect the individuals first, but not the data. To protect the individual, we can automatically protect their interest standards. Thank you very much. I'm looking to the recommendations and to provide my comments to the latest bill. Thank you very much, sir.

Peter Kaplan:

Thank you Leela. Our next speaker is Sal D'Agostino. Sal?

Sal D'Agostino:

Thank you and good afternoon. My video should be on, I guess, I don't know why it's showing open exchange. But, good afternoon. Thanks to the FTC for this opportunity and thanks to the other participants for their contributions. My name is Sal D'Agostino from Brookline, Massachusetts. I'm the founder of IDmachines and the co-founder of Zero Public Networks and a security and privacy professional and entrepreneur. I want to talk about transparency, two factor notice and co-governance, and how these can address the questions on how to regulate consumer consent, and what requirements are needed for companies, notices and disclosures to companies.

Notices today are not, but need to be, interoperable, technically legal and socially, for security and [inaudible 04:33:17] of scale. To address this, the FTC can and should leverage the existing body of international privacy standards and regulations, which the FTC itself helped to initiate. United States is not China, Russia or North Korea, where the digital world is firewalled off for consumers. Here, we 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 extreme measures to try to keep my data safe. I don't bank or conduct any financial transactions on my phone. I barely use social media and never post anything sensitive like political or religious opinions, medical status, or even any indication of my age. But I should be able to safely enjoy these digital platforms and services because our privacy is truly a public good, just like the air we breathe.

Privacy law in the United States is based on the concept of human dignity and the right to control our own information. My data is part of my human dignity, and control over personal information means having control over our lives. We can't have that if decisions about us are made in secret without our awareness or participation. The FTC's authority to investigate deceptive and unfair practices is woefully inadequate to address the mass commodification of consumer's personal behavior. But some members of the FTC who oppose this ANPR, would argue that platform regulation and data security measures are 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.

Cali Schroeder:

Thank you, and thank you to the FTC for this rule making and the opportunity to contribute. My name's Cali Schroeder. I'm the Global Privacy Council at the Electronic Privacy Information Center, and I am also the US chair of the digital group at the Transatlantic Consumer Dialogue, on whose behalf I am speaking today.

Many of the experts you spoke to earlier highlighted key elements that should be considered in this rule making, including many of the specific harms that can result from commercial surveillance and insufficient data security practices. I wanted to build on that a little bit by emphasizing the importance of including meaningful and clear enforcement measures in this rule making, including fines and algorithmic disgorgement. Rules without enforcement are easily ignored, and clarity around what enforcement actions can be anticipated and what recourse wronged consumers may have would provide a level of stability for consumers regarding their privacy rights and provide clear expectations for businesses.

The EU has been very active lately in pursuing enforcement penalties over privacy violations tied to commercial surveillance, and this is both against US based companies that are operating in the EU and against EU based companies. Some recent examples include investigations of Meta regarding how personal data collected through commercial surveillance is transferred across borders, and a recent ruling against IAB Europe for their realtime bidding structure's personal data processing.

These actions demonstrate to consumers in the EU that their statutory rights will be vigorously defended, and by providing clear requirements through this rule making and taking enforcement actions within the US, the FTC will be able to demonstrate the same to US consumers. We urge the commission to protect consumers through enumerating and pursuing specific enforcement measures that will accompany this rule making, and look forward to contributing as we can there. Thank you.

Peter Kaplan:

Thanks, Cali. Our next speaker is Jennifer McTiernan. Jennifer.

Jennifer McTiernan:

Hi, my name is Jennifer McTiernan. I'm here as a trained lawyer who has worked for tech companies for most of my career, data privacy certified professional, a parent, and an individual who conducts many aspects of my home and work life digitally. These opinions are my own as a private citizen, and do not constitute legal advice.

Data protection is urgently needed, and I emphatically encourage the FTC to use its deception and fairness standards to implement rules to better protect the data privacy of Americans, and especially the data privacy of vulnerable groups, and most especially, children under the age of 18. I offer the GDPR as an excellent starting point in terms of offering a comprehensive privacy framework that has been enforced since 2018, and that a significant number of American tech companies have already had to comply with.

I would like to point out that if you are an EU citizen in the US, you can avail yourself to the GDPR in order to assert control over your personal data held by an American company. These rights include the right to restrict processing, the right to object, and the right to not be subject to automated decision making. As a US citizen, these same rights are not available to you, even though many, if not most American tech companies have built the infrastructure to allow EU citizens the ability to exercise these important individual data protection rights.

I'd like to press on that point. The GDPR has shown us since 2018 that it is possible for companies all over the world, including the biggest tech companies in the US, to comply with robust data protection regime. At this very moment, American companies that are GDPR compliant offer certain rights to EU citizens that Americans do not have. I also want to mention too that children especially are vulnerable, and are only increasing the amount of time they spend online due to the pandemic.

The comments made in this form about edutech I was not aware of as a parent with children who have devices from their schools, and I find them quite alarming. It's my view that data privacy will in no small degree determine the future of humanity, and I thank Chair Khan and the FTC commissioners for convening this critically important hearing.

Peter Kaplan:

Thank you, Jennifer. Our next speaker is Evangelos Razis. Evangelos.

Evangelos Razis:

Thank you. My name is Evangelos, and I lead privacy and AI policy engagement at Workday. Workday is a leading provider of enterprise cloud applications for finance and human resource groups. Workday applications have been adopted by thousands of organizations around the world and across industries from medium size business to more than 50 percent of the Fortune 500.

As the FTC considers rule making, I would like to make three points. First, privacy is a fundamental right and Workday is a strong supporter of a comprehensive federal privacy law. We have all the sponsors of the Bipartisan American Data Privacy and Protection Act, which passed out of a House Energy and Commerce Committee at a historic 53 to two vote. While the proposal would benefit from additional refinement, the ADPPA is a high watermark for efforts to pass federal privacy reform. We therefore ask that if the commission proceeds with rule making, it does so in a manner that compliments and aligns with congressional efforts to enact much needed privacy legislation.

Second, the tech industry is not a monolith. Enterprise cloud software providers such as Workday operate in a B2B market and provide services that include privacy and security protections. Importantly, most enterprise cloud software providers process data at the direction of their customers, determine 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 working with you on these crucial issues.

Peter Kaplan:

Thank you, Evangelos. Our next speaker is Carl Holshouser. Carl.

Carl Holshouser:

Appreciate the opportunity to speak at today's forum on behalf of TechNet, the non-partisan voice of the innovation economy, celebrating our 25th year this year. I'm Carl Holshouser, senior vice president and corporate secretary. I've got about 20 years of experience in tech policy.

TechNet represents over 5 million employees at over 100 businesses and countless customers in a variety of industries. For America's innovation economy to continue growing, creating jobs and developing cutting edge services that businesses and consumers depend on, we need US rules and regulations to keep up with the demands of a rapidly changing world.

For nearly a decade, TechNet has been a leader in calling for comprehensive federal privacy legislation, but this isn't just a tech sector issue. It impacts every sector, every business across our entire economy. Like we've heard a lot today, right now the current landscape of state privacy laws has created a conflicting and very confusing 50 state patchwork of privacy rules that hurts our country's small and medium sized business the worst.

According to a recent study by ITIF, if Congress doesn't pass a federal privacy law this year, it could cost our economy over one trillion dollars over 10 years, with small businesses footing more than $200 billion of that bill. Instead of sleepwalking into a job killing, innovation crushing 50 state privacy patchwork that will make it harder for entrepreneurs and small businesses to succeed, we're advocating for a federal privacy law that will protect consumers no matter where they live and give businesses certainty about their responsibilities. In other words, we need to make it possible for small businesses to invest in innovation and job creation, not litigation.

Recently, as has been mentioned today, Congress has demonstrated a willingness to address this challenge and is making real progress in crafting bipartisan federal privacy legislation. We are hopeful this momentum continues, because at the end of the day, this will be much more effective when it's signed into federal law than written in regulation that could be more easily undone down the line by whatever party's in charge.

We're also heartened by the statements of several of the commissioners during the announcement of this ANPR, that the intent is not to derail Congress' ongoing effort to craft federal privacy legislation. We at TechNet look forward to working together to protect consumer privacy, strengthen small businesses, 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, data brokers, and other private entities. Many of these companies engage in a widespread pattern of unfair and deceptive practices embedded throughout society, especially harmful to historically disadvantaged communities.

In the healthcare realm, researchers from the University of California have found an algorithm widely used in US hospitals to allocate healthcare to patients systematically discriminated against Black people who were less likely than equally sick white counterparts to be referred to hospitals. In the housing realm, Meta recently settled a lawsuit with the Department of Justice regarding its housing advertising scheme, admitting that it engaged in discriminatory practices that meant Black users saw fewer or no ads for affected housing on Facebook.

In the voting context, researchers from the University of Texas and Austin found that Black, Native American, and Latino users were subject to sophisticated micro targeting efforts ahead of the 2020 election, targeted with deceptive content on social media platforms about the voting process.

How data is collected, processed, retained, and sold has a direct impact on civil rights and economic opportunities. These issues fall squarely within the FTCs authority, bolstered by its history of advising on complex privacy issues. Free Press has worked closely with dozens of consumer and civil rights groups over the last year to sound the alarm on digital harms affecting a range of communities: communities of color, children, non-English speaking individuals, and other members of the general public.

Those groups overwhelmingly support this rule making. We are eager to help build the record of harms in this proceeding to advance FTC rules that protect consumers. Thank you.

Peter Kaplan:

Thank you, Nora. Our next speaker is Clark Rector. Clark.

Clark Rector:

Thank you. My name's Clark Rector. I'm the executive vice president for government affairs at the American Advertising Federation, which is the umbrella association for the advertising industry. We represent all parts of the industry, from major corporations to thousands of individuals practitioners.

AAF is supportive of national privacy and data security law, and believes Congress is the body to pass such a law. We have and continue to encourage them to do so. As Congress is deliberating, we believe it's premature for the commission to initiate rulemaking. The AAF does believe, though, that when the National Privacy Law is passed, the FTC is the appropriate enforcement agency. We have long supported your actions to combat false and deceptive advertising, and know that your work against bad actors benefits not just consumers, but the vast majority of honest businesses, as well.

As to the content of the ANPR, we're disappointed that there's little to no discussion of the benefits that come with responsible use of data and data driven advertising. In short, data driven advertising supports a competitive online marketplace and contributes to strong economic and job growth. It allows small, local and niche businesses to grow and plant potential customers, nation and even worldwide.

Responsible data driven advertising helps fund the internet and free content for consumers. Loss of advertising revenue means that much of the content would go to a subscription based model, which the commission has acknowledged many consumers would likely be unable to afford. Studies have shown that consumers are comfortable with data-driven advertising, and more than half desire relevant ads.

We urge you to be mindful of these benefits and not take any actions that will harm a beneficial, safe and successful online marketplace supported by the responsible use of data and data-driven advertising, and we thank you for the consideration of our problems.

Peter Kaplan:

Thank you, Clark. Our next speaker is Mark Smith.

Mark Smith:

Thank you. Can you hear me?

Peter Kaplan:

Yep.

Mark Smith:

Okay. Good evening. My name is Mark Smith, representing the Center for Information Policy Leadership, known as CIPL, which is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth. I thank the commission for the opportunity to speak tonight.

While CIPL has been and continues to be a staunch advocate for federal privacy legislation, in the absence of a legislative solution, CIPL looks forward to engaging with the FTC as the US considers an appropriate framework to encourage and enable good data practices based on organizational accountability.

For more than a decade, CIPL has pioneered organizational accountability as a key building block of effective data privacy regulation and its corresponding implementation within organizations. Indeed, CIPL's accountability framework is a recognized standard for the development of best in class data privacy practices and organizational compliance programs.

We, therefore, encourage the FTC to review our papers, especially those addressing the ways in which policy makers and data protection authorities can effectively promote and incentivize the uptake of organizational accountability, which in turn would enable broader uses of data for the benefit of consumers and society.

Indeed, both consumers and businesses depend on the ability to share and use information broadly and effectively. The commission should ensure that legitimate uses are not undermined, and innovative uses are not suppressed. We look forward to providing more detailed input in our writing, and I thank you for your time and attention.

Peter Kaplan:

Thank you, Mark. Our next speaker is Andy Jung. Andy.

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?"

I commend the commission for addressing innovation, which is a key factor in the FTC's analysis required by Section 5N of the FTC Act. Broad and sweeping trade regulation rules on privacy and data security could impede innovation in three primary ways. First, new regulations can create higher compliance costs and raise barriers to entry for companies developing online tools and services. This may disincentivize firms, especially small ones and startups, from building or investing in online tools and services.

Second, new privacy and data security regulations could make online tools and services less effective and less accessible. For example, rules limiting how firms collect and use consumer data would restrict the ability of firms to offer targeted personalized services based on behavioral and browsing data.

Third, privacy and data security rules may force firms to start charging consumers for online tools and services that are currently ad supported. New privacy and data security rules would limit firms' ability to monetize free online services, forcing them to switch to paid models which may charge consumers upfront.

Section 5N requires the FTC to weigh such costs to innovation against the benefits of any new rules. How to assess such trade offs will be among the most important disputes of material fact in this rule making, and critical to whether any rules the commission issues can survive judicial review down the road. Thank you for your time.

Peter Kaplan:

Thank you, Andy. Our next speaker is Joshua McGrath. Joshua.

Joshua McGrath:

Thanks Peter. My name is Joshua McGrath, and I'm the co-founder of mAdSpace.io. This has been an extremely informative forum, and I hope it'll set the stage for further action.

I'd like to start by saying third party data collection and data sale is inherently deceptive, as Mr. Martineau mentioned in our first panel, but first party data sale is increasingly common and equally opaque. Mr. Kent mentioned that this first party data sale and management is anti-competitive, as it creates walls to entry for smaller companies and doesn't benefit smaller publishers and businesses as we typically hear from these larger platforms.

The fact is, advertising budgets will be spent regardless of whether consumer privacy is put at risk, but the danger first party data sales posed to consumers is equally large, if not larger, without the radical transparency proposed by today's panels. We at mAdSpace are focused on being transparent custodians of consumer data, giving them tools to manage their data however they see fit, but that's impossible for any party without clear transparency and regulation around data access.

Without this transparency and active regulation, there's no recourse for consumers who want their data truly protected, particularly once it leaves the silos of these first party data brands and platforms. Along those lines, we argue that the data a consumer creates and leaves behind is an extension of themselves, and needs to be protected as strictly and as a direct interaction with merchants. While the direct interaction takes place when a consumer gives their data to receive a service, they're not at all benefited 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. Great. Go ahead, Jean.

Jean Ross:

Thank you, Peter and commissioners, for spending this time listening to public [inaudible 05:03:15] My name is Jean Ross. I am a nurse and a co-founder of a tech startup called Primary Record, currently developing a health consumer app.

I was moved today to speak because as you may know, the office of the National Coordinator for Health Information Technology has been working with stakeholders to promote patients' right to medical records in consumer apps of their choice on their smartphones. As a nurse, I applaud the work and efforts of ONC, as I've seen the harm done and the time families must spend to coordinate their care when health data is so siloed as it is today.

I wanted to share my experience as a nurse entrepreneur, as you think about the balance of innovation and regulation. As a co-founder, there is a challenge in understanding my legal and financial risk taking on health data for consumers, so not knowing the direction Congress and the FTC is taking, so I appreciate this conversation getting moved forward.

Out in the community, consumers, and even those in the health industry, are confused by the role of FTC, especially when it comes to health data. There is an applied assumption HIPAA follows a health data no matter where it is. In the competitive space of health record data aggregators like myself, there 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 impacted communities are not able to contest the decisions that are made about them, demand changes to abusive systems, and seek redress for the harms that have been named today. It is critically important that transparency mechanisms be treated as a foothold for accountability to the public, rather than simply flagging how a technological system will treat citizens and consumers.

The FTC should look to successful public documentation models, such as environmental impact assessments, for examples of how the public can have a voice in product development that shapes the public sphere. The FTC must provide the public with opportunities and infrastructures to shape how these companies collect and categorize our data, make decisions about us, and potentially trap us in abusive and unfair sociotechnical systems. Thank you for the opportunity to speak today and for the work of this commission.

Peter Kaplan:

Thank you, Janet. And our last speaker is Stephen Dnes. Stephen.

Stephen Dnes:

Hello. Thank you for the opportunity to speak today. My name is Stephen Dnes, and I'm speaking on behalf of the Movement for an Open Web, which represents a range of open web users who have interest in data handling and in the balance between competition and privacy law.

Privacy is important, but like any subject, it depends on its context. When people interact with online systems, there are many interests involved, some them not necessarily obvious, and some of them quite 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 HIPAA, CRPA, [inaudible 05:08:29] GDPR all provide guidance on the reduction of risk.This includes privacy by design measures, such as [inaudible 05:08:36] the right to be forgotten, resetting identifiers. It's important to remember how powerful some of these safeguards can be and how they can result in good consumer outcomes with minimal or low risk of bad outcomes.

A common misconception is that names are specifically tracked, but in reality, interoperable identifiers with appropriate measures to safeguard identity and keep it distinct from data can be powerful in recognizing consumer benefits. Where these safeguards are in place, there may be less reason to restrict data handling.

One point that's often missed in this debate is that some of the largest networks can use some of the most invasive practices and not employ these safeguards. This is very visible at standards bodies, notably the W3P, and the argument that's often made is that one large system is the safest, but recent legislation, particularly EEA development such as the DMA and the Digital Services Act, identify that larger platforms can pose larger risk.

Smaller players may have an important role to play in helping consumers gain benefits such as those referred to earlier, free content, avoiding pay walls, and it would be important for any new rules to consider how smaller companies could use innocuous data and perhaps to look more at data use restrictions rather than the restriction of data handling, per se.

Peter Kaplan:

Can you wrap up? Yep. I'm sorry. You're over time. I want to thank everyone. That concludes our public comments for today, and that concludes our event, and so I want to thank everyone for their participation, including all our public speakers. You can submit further comments through the FTC's website, and I wish you all a good evening. Thank you.