FTC Open Commission Meeting

May 18th 2023

Lina M. Khan:

Hey, good morning everybody. Thanks so much for joining us for today's open commission meeting. We're meeting in open session today to consider two items before the commission, both related to American's privacy. But as always, we'll get started by hearing from members of the public. And so I will turn it over to Doug, our head of Office of Public Affairs, to get us through that portion. Over to you Doug.

Doug Farrar:

I'm the director of public affairs at the FTC. And all of us at the FTC are looking forward to hearing from the public today. Please note that we are recording this event and some or all of it may be available to the public record in accordance with the commission's rules. Now I will call on several members of the public who have joined us and each person will be given two minutes to address the commission. So without further ado, I will begin with Berin Szoka. Berin, go right ahead.

Berin Szoka:

Thank you. I'm Berin Szoka, President of TechFreedom. In 2011, President Barack Obama declared that our regulatory system must allow for public participation in an open exchange of ideas. These are two different things and the FTC isn't really doing either. In 2015, the FTC issued its first policy statement on unfair methods of competition. It recently rescinded and replaced that statement. It never sought public comment as it's on our merger guidelines, but it should have.

Former Democratic FTC chair Bob Petoskey said so in 2008, as did Republican Commissioner Maureen Ohlhausen in 2015. Open mic sessions like this one are no substitute for written comments, but comments also aren't enough. The FTC needs to hear a real back and forth. That's why the Federal Communications Commission has required reply comments in all rulemakings for 75 years. The FTC itself did so for decades. TechFreedom recently requested a rebuttal round in non-compete rulemaking, the most significant in FTC history, but the commission has ignored us.

Workshops could also facilitate an open exchange of ideas but only if the commission gives participants enough time to explore hard issues. The series of 14 workshops organized by my colleague Bilal Sayyed in 2018 and 2019 offers a good model, most were multi-day. Most critical will be how the FTC conducts the hearings required by the Magnuson-Moss Act in Consumer Protection rulemakings. The commission recently released the agenda for its first Mag-Moss hearing held in a new rulemaking in decades. 13 speakers will get just five minutes each. Claiming that there were no disputed issues in material fact, the commission authorized no cross-examination, so the hearing officer will be merely a timekeeper. That's not a hearing, it's just another open mic session.

Despite broad consensus on stopping impersonation fraud, hard questions remain on how to craft a rule that won't affect comedians, actors, or even kid's Halloween costumes. If the commission won't allow a real exchange of ideas on even such an uncontroversial rulemaking, why should anyone expect it to do so in more complex rulemaking such as commercial surveillance, the commission must do more to meet President Obama's standard for open and participatory government. Thank you.

Doug Farrar:

Thank you very much. All right, Matt Kent. Matt.

Matt Kent:

Hey, good morning. I'm Matt Kent, Competition Policy Advocate with Public Citizen. Public Citizens is a nonprofit consumer advocacy organization with over 50 years of experience in advancing the public interest in federal policy. On behalf of our half a million members, supporters nationwide, we applaud the FTCs recent actions to decrease corporate concentration in the pharmaceutical industry, protect children's safety online, and institute a national ban on the use of non-compete clauses by employers.

On the first point, Public Citizen supports the commission's move to challenge the merger between Amgen and Horizon Therapeutics. Indicators are clear that competition in the pharma markets is lagging. We support a holistic merger analysis that analyzes product pipelines to account for impacts on innovation and competition as well as a firm's prior history of anti-competitive practices. Amgen built an expansive thicket of patents to prevent Emerald from facing composition for more than 30 years and abused this monopoly by sharply increasing the price by more than 450% since introduction. Ultimately, the FTC's move is good for patients who have endured sky high drug crisis as a result of market consolidation. Generally, we encourage the FTC to center merger analysis on the incipiency standard enshrined in the Clayton Act.

The second point, Public Citizen also supports the FTC's move to adjust its 2020 privacy order with Meta. Kids should not be an engine a profit for a social media company until Congress acts on its promise to ensure online privacy for kids and adults. It is critical that the FTC move forward aggressively to enforce the law in this space.

And finally, on non-competes, Public Citizen very much supports the FTCs reason NPRM on non-competes. It is crucial that the FTC use its rulemaking authority under Section 5 of the FTC Act. I've submitted formal comment on this, but to iterate, the commission must maintain a categorical ban on non-competes income limits, other compromises will create loopholes that will avoid the entire rules effect. Secondly, the requirement that employers notify workers of a clause rescission is very important. Workers cannot get out from under if they don't know their terms of employment have changed. Thank you very much.

Doug Farrar:

Thank you very much, Matt. All right, next we have Haley Hinkle. Haley,

Haley Hinkle:

Good morning. My name is Haley Hinkle and I am Policy Counsel for Fairplay. Fairplay is the leading independent watchdog of the children's media and marketing industries and we're committed to building a world where kids can be kids, free from the false promises of big tech. I am here today to emphasize Fairplay's, strong support for the FTC's recent action against Meta. The FTCs ordered to show cause and proposed order layout allegations through the eyes of a third party auditor that Meta has repeatedly violated user privacy and the terms of its agreements with the FTC.

Meta has time and again shown itself incapable of responsibly handling user data and Fairplay believes that the FTC's proposed prohibition on the monetization of minor's data is a necessary and proportionate response to these repeated violations. Kids and teens are the population most vulnerable to Meta's failure to comply with the law and appropriately handle data, minors data in particular is

highly sensitive. Fairplay released a report earlier this month outlining META'S long history of failure to protect minors.

That report highlights among other things that Meta's platforms perpetuate child abuse of exploitation, that Meta uses its advertising apparatus to surveil teens and target them when they are vulnerable that its recommendation systems regularly push harmful content to kids. And most recently, the company decided to open its Horizon World's platform to teens despite the clear dangers the virtual world poses to young people. Meta continues to put profit over the wellbeing of its users and in particular vulnerable minors and we commend the FTC's decisive action to address this problem. Thank you.

Doug Farrar:

Thank you very much, Haley. Next we have John Davidson. John.

John Davidson:

Chair Khan, Commissioner Slaughter, Commissioner Bedoya, thank you for the opportunity to speak to you today. I'm John Davidson, Director of Litigation at the Electronic Privacy Information Center. I just want to convey my thanks to the commission for proposing significant and game-changing modifications to the consent decree governing Meta's privacy and data protection practices. As you know, EPIC has spent more than a decade calling public attention to a seeming endless string of privacy violating business practices by both Facebook and Meta.

Meta has had all of that time and two separate consent decrees to clean up its act on privacy, but it's clear that it hasn't fixed the problems. And that's of course not just the judgment of the commission, that's what the independent assessor chosen by Meta also found. Warning Facebook to follow the law in 2012 didn't work. Forcing Facebook to institute procedural safeguards in 2019 clearly hasn't been enough either. It's long past time for meaningful changes to Meta's business model that will reduce the incentive to vacuum up and commercially exploit personal data, especially the data of minors. So we at EPIC are deeply grateful to see the commission make the most of its authority to regulate Meta'S business practices.

Second, I want to make a somewhat technical point, but I think one that's very important to the proposed modification of the order. As you know, many of its provisions will benefit all users such as the restriction and pause on Meta's introduction of new products and services. One provision in particular is targeted at minors, the blanket prohibition against monetizing the data of children and teens under 18. While I think that restriction is justified as a special protection for Facebook and Instagram's most vulnerable users, I want to explain why I think there's an additional ground for that restriction to be included.

The 2019 stipulated order and the 2020 commission order did not extinguish the violations raised in the show cause order relating to Messenger kids. These violations extended past the June 19 horizon of the previous Meta order and an order did not purport to extinguish violations that the commission was unaware of in June, 2019 or any COPPA violations at all. So including this relief directed specifically at children in a modified order, I think is justified. Thank you for your time and consideration and I'll turn it back over.

Doug Farrar:

Thank you, John. Next up we have Karina Cop. Karina.

Katharina Kopp:

Thank you. I'm Katharina Kopp with the Center for Digital Democracy. CDD strongly supports the FTC's proposed changes to the agency's 2020 privacy order with Facebook now called Meta, particularly the proposal to prohibit Meta from profiting from data of children and teens under 18. This measure is justified based on Meta's alleged repeated offenses and due to the unique and alarming risk its practices posed to children and teens. The decision is a long overdue intervention into what has become a huge crisis for young people. Meta and its platforms are at the center of a powerful, commercialized social media system that has spiraled out of control, threatening the privacy, mental health and wellbeing of children and adolescents. The evidence provided suggests that Meta violated FTC consent decrees repeatedly and seriously. In addition, it violated COPPA. We do not know the full extent of its failures, but across the board failures are apparent.

This has put the privacy of all users at risk, posing a substantial risk to the public. But young people are the ones that are most vulnerable and suffer most from Meta's unconstrained practices. Meta's apparent violations are unfolding amid an alarming rise in shocking incidents of suicide, self-harm and online abuse and exploitation among the nation's youth. And yet Meta seems to be unable or unwilling to safeguard users data via procedural safeguards or by following the law. The FTC proposed action regarding minors is needed and justified. Minor's unique vulnerability must be safeguarded but prior approaches to curtail Meta have failed, a more effective approach is needed. The proposed order will minimize the amount of data that Meta can collect, use and share, and this new approach is likely to significantly reduce the privacy harms and the myriad of downstream harms to children and teens stemming from Meta's practices. Thank you very much.

Doug Farrar:

Thank you very much, Katharina. Next we have Christabel Randolph. Christabel.

Christabel Randolph:

Yes, can you hear me?

Doug Farrar:

I can. Go right ahead.

Christabel Randolph:

Thank you so much. Good morning everyone. Chairman Kahn, Commissioner Slaughter and Bedoya. My name is Christobal, I'm an LLM student with Georgetown Law and I'm a Research Assistant for the Center for AI and Digital Policy. On 8th of March, we filed a detailed 46 page complaint with the FTC regarding OpenAI and ChatGPT. We made clear many problems that the product had and we set out the prior statements of FTC concerning AI products. We also described the steps that FTC should take. We said that the FTC should open an investigation and order OpenAI to hold the release of new GPT models until necessary safeguards are established. We said that these safeguards should be based on guidance for AI products previously that the FTC has issued and established and many AI experts also express similar concerns about ChatGPT.

President Biden has also said that the company should not release or deploy AI products that are not safe. At the Senate hearing this week, even Sam Altman expressed concerns about the AI products and said that Congress should regulate the industry. Chairman Khan published an editorial this week in the [inaudible] saying that FTC will vigorously enforce the laws we are charged with administering. She also said that the FTC is well-equipped with legal jurisdiction to handle the issues brought to the fore by the rapidly developing AI sector.

I'm here today to know what is the status of the CAIDP complaint concerning OpenAI. To date, we have not even received an acknowledgement. Have you opened the investigation we requested? If you have not opened the investigation, can you tell us whether you will and if you don't, can you explain why? FTC has previously made such announcements, for example, announcing the opening of Facebook investigation after Cambridge Analytical. So we expect and we request a response from the FTC about what actions will be taken on our complaint. Thank you so much today for the opportunity to speak.

Doug Farrar:

Thank you very much, Christabel, appreciate you coming here. Andy Jung. Andy.

Andy Jung:

Good morning. I'm Andy Jung. I'm a Legal Fellow at TechFreedom Firms like Alphabet, OpenAI and Stability AI provide AI tools to the public for no charge. These AIs help users accomplish a wide variety of tasks, including writing code, conducting research, and generating images of French Bulldogs painted by Rembrandt. Lawmakers clamor for new laws governing AI. This week, several Senators proposed a new regulatory agency. But the notion that AI is unregulated is a myth. The FTC already oversees AI as Chair Khan and Commissioner Bedoya have noted.

In April, Chair Khan and officials from the DOJ, CFPB and EEOC released a joint statement asserting that their agency's enforcement authorities apply to AI, specifically the FTCs unfair and deceptive trade practice laws apply. The commission may initiate enforcement actions against AI companies for deceptive claims and unfair actions which substantially injure consumers.

Additionally, the commission may promulgate rules prohibiting specific unfair or deceptive AI practices. Either way, the commission would have to show that the practices likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. AI tools provide a variety of benefits to consumers and competitors in the marketplace. The commission must weigh these benefits as it continues to probe the depth and breadth of its authority over AI. In that vein, I encourage the commission to consider establishing a federal advisory committee to inform and advise the agency's regulatory agenda on this new and innovative technology. Thank you so much for your time.

Doug Farrar:

Thank you, Andy. Next we have R.J. Cross. R.J.

R.J. Cross:

Thank you. My name's R.J. Cross with PIRG, the Public Interest Research Group, on behalf of our 1 million American members. And I want to talk briefly about the proposed Meta decision. Regulators have long let the American people basically serve as guinea pigs of companies. Products in the marketplace are largely released before real thinking about what might happen next. And with social media, it's our young people that have born the brunt.

Leaked reports of Facebook's internal research on it's app Instagram concluded it was making body image issues worse for one in three girls. And in Britain, 13% of teen girls struggling with mental health drew a direct line between Instagram and a desire to kill themselves. I'm not telling you anything that you don't already know, but I hope you see this. What we have today is not the advertising industry of the 70s. It's with far more advanced technology, is more personal, and the threats coming down the pike are even more significant.

If the more comprehensive AI models hitting the market today are deployed in the name of advertising, even more granular data bots might be gathered, analyzed rapidly and used to deliver the content and messages that touches us even more deeply. I don't want to see what a relatively unregulated future could mean for anyone struggling with a part of themselves that tech can amplify in order to make money. And it's not just advertising that we have to consider, take for example that pivot to VR, In a single second of using VR

R.J. Cross:

... our goggles. Companies can gather 90 data points on our body language, and this is information that can be deeply revealing about our health. Consider a 16-year-old who's playing a game with his friends for 30 minutes. In that 30 minutes, an entire database of his movements may be gathered, analyzed with AI modeling, and find that he exhibits the physical traits of someone who, 60 years later, may develop dementia, may. This data is sold to a hundred of companies, including insurance agencies, and when he goes to get his own healthcare or life insurance policy for the first time, that 30 minutes may end up shaping his financial future.

Asking him to predict the implications of 30 minutes of fun is not a fair practice. The world is accelerating, profound shockwaves, a single new technology in the market can have, has never been greater, and it's imperative that regulators step up and meet the moment. It's time to look ahead on behalf of the consumers that they're charged to protect. When it comes to the proposed action against Meta, we see hope that regulators are finally confronting the threats. The stakes are much higher, and it falls on the FTC to be part of the solution. So thanks for your action and for their opportunity for concerned consumers to speak. Thank you.

Doug Farrar:

Thank you, RJ. Appreciate that. Next up is Andrea Amico. Andrea? Andrea, are you there?

Andrea Amico:

Yes, I'm here. Thank you. I appreciate the opportunity to speak, specifically about IOTs and vehicles. My name is Andrea Amico. I'm the founder of Privacy4Cars, we're the first and only privacy company that is focused on vehicle data, which increasingly, includes identifiers, geolocation, user profiles, data from their phones, and biometrics, which I know is an area that the FTC is interested in.

Our studies show that consumers are growing, have growing and legitimate concerns, but when they try to buy, or rent, finance or insure a vehicle, they're really in a thick fog. They don't know what data is being collected from them, and partly, it's because no materials are made available to those companies to fairly represent what's going on with their cars. For instance, only one in 10 dealership salespeople knows that cars can collect biometrics. Less than one in 20 correctly represented manufacturer can collect, share, and sell data, and not just for safety warranty reasons, and none of them could explain the difference between any two vehicles for sale on their route, that's just been test driven by consumers.

So, to lift this fog, we launched, two weeks ago, vehicle privacy report.com. It's a website where consumers can for the first time, for free, there's no ads, this is a completely educational tool, enter the VIN of their car, and, for the first time, they can see important and simple privacy information about their car, which includes the world's first privacy label, which we also show the recently to the Department of Commerce.

The consumer response is incredible. We really have touched on a nerve, just by word of mouth, we have thousands of consumers that come and check their car, and we are hoping, and we start to see,

actually dealers raising to the occasion, and starting to introduce fair and transparent disclosures, and try to lift this fog. The reason why it's important is because this is not just a privacy issue. The [inaudible] just did a similar study to what we've done, and there is the conclusion this is a commerce issue, because if consumers knew what data was collected by vehicles, they would act differently in the marketplace, at the time in which they're purchasing, renting financing, and insuring their vehicle.

So my hope is to do two things. One is to raise attention to IOTs, and two, hopefully the member of the commission will want to check their own car vehicle privacy report. I think you'll find it interesting, and you'll see what kind of level transparency is available to consumers today, and not in a distant future. There's no reason to wait. Consumers can have better information right now. Thank you.

Doug Farrar:

Thank you very much, Andrea. Next up we have Tiffany Cianci. Tiffany? Tiffany?

Tiffany Cianci:

Apologies.

Doug Farrar:

Oh, go ahead. I am. Can you hear me? Yes,

Doug Farrar:

We can. Thank you. Thank,

Tiffany Cianci:

Thank you very much. I represent the Happy Handstands Franchisee Association. We represent franchises across more than 30 systems, but six of those systems specialize in the service of children between the ages of birth and 16 years old.

We fully support the FTCs efforts and propose changes to the proposal to bar Meta, and if possible, other tech companies, from profiting off the data of children and teens. We witness in our programs firsthand, each and every day, the horrific toll that social media and technologies are having on children in real time, and particularly subsequent to the increased and addictive increases in reliance and interaction with technology following COVID, and the isolation children suffered. It's companies like the franchises that we serve, that have the difficult task of picking up the pieces of the damage that tech is having on our youth, to put these kids back together in real time.

We would ask that, that you need only really look to an eight-year-old's birthday party to see that 64% of children are looking at a device, instead of engaging with one another, to see the risks in real time and what they pose. We have significant concerns that the collection and profiting off of this data, while horrific now, can more likely be used to plant seeds that create a lifetime of exploitative and controlling measures, so that they can continue to profit over time, but that shouldn't be taken from data you're collecting on children now. They've been used as test subjects, and now to capture them while they're young and keep them going forward for a lifetime of profiteering is something that cannot possibly be appropriate for serving our children.

On an unrelated measure, thank you for having me. We were unable to testify during the franchise open meeting and we want to say that we thank the FTC for their efforts in looking at the possible changes to the FTC franchise role as well, and we fully support what you guys are doing there. Thank you so much.

Doug Farrar:

Thank you, Tiffany. Appreciate it. All right, next we have Santana Bolton, Santana?

Santana Bolton:

Hi, I'm Santana Bolton. I'm a legal fellow at Tech [inaudible] "The overabundance of data in the modern world," warns Swiss scientist Conrad [inaudible], "is overwhelming. It is confusing and harmful to the mind."

Tiffany Cianci:

I know.

Santana Bolton:

Of course he was talking about the printing press, not artificial intelligence. The commission has been asked to stop the release of AI tools, but applying precautionary principles to AI development would have real costs. Section five N of FTC act requires the FTC [inaudible] to consumers or to competition. Competition in AI is increasingly global. Cracking down on AI could help America's global rivals and harm our national security.

American companies are already using automatic threat assessment and developing tools to detect malware and data breaches. AI tools can help protect American weapon systems from cyber attack. Consumers also stand to benefit from AI innovation. Consider AI's medical benefits. New drug development is extremely expensive and time-consuming. If even one new treatment is discovered with problem AI tools, those benefits must be accounted for.

More generally, research suggests that AI tools could help less skilled workers the most, increasing competition and rebuilding middle class. This commission cannot afford to discount this new technologies benefits to lower [inaudible]. Like any new technology, but even more so, AI will create a wide variety of both costs and benefits. The FTC can't explore these trade-offs through two minute blocks of prepared remarks. It needs to hold workshops that allow experts from multiple fields, and with diverse perspectives, to dialogue each other, and in rule makings, the FTC will benefit from the open exchange of ideas that is only possible if the commissioner allows for replying [inaudible]. Thank you very much.

Doug Farrar:

Thank you very much, Santana. All right, Sam Heiner. Sam?

Sam Heiner:

Hello commissioners. Thank you for taking the time to hear from me. I'm a student at UNC Chapel Hill and I'm the executive director of the Young People's Alliance. I'm here today on behalf of the millions of young people across our country whose privacy has been violated, and mental health harmed, by Meta's irresponsible approach to handling our data. In addition to the patently illegal actions Meta took to warrant changes to the previous FTC order, Meta is still taking advantage of minor's data to serve content that they know will harm children with mental health.

To illustrate this, I'm going to share a story that I've heard repeated from countless people my age, especially young women. They start seeing seemingly innocuous posts about healthy eating in their Instagram feeds, and out of some interests, they look at them for just a few seconds longer than they might for other posts. The algorithm picks up on this interest and starts showing them more and more

extreme content, promoting unrealistic body standards, and telling them that eating under a thousand calories per day is the norm. Like most teens, they're on social media for hours every day, so they start to accept these unrealistic body standards as their reality. Next thing they know, this content causes constant anguish, and they can't go even an hour without worrying about how many calories they've eaten that day. This problem isn't limited to eating disorders either. I know many young people who've experienced the same pattern, but with content that promotes conspiracy theories, racism, sexism, and violence.

For hours each day. They were exposed to a barrage of posts that were targeted to play on their insecurities, and slowly drove them to become more and more extreme and hateful. I'm here before you today because it started to feel like every time I got close with someone my age, I heard another version of this story. This isn't just a small sliver of users. These are your kids, and I'm sure if you ask any young person about their generation's experience with social media, you'll hear a similar story. It's time that we hold Meta accountable for irresponsibly monetizing children's data, by keeping them online for as long as possible to sell more ads with no regard for the destruction that they've caused to my generation's mental health. Thank you.

Doug Farrar:

Thank you so much, Sam. Okay, the second to last speaker today will be Zaman Qureshi. Zaman?

Andy Jung:

Good morning, Chair Khan, Commissioner Slaughter, and Commissioner Badoia. My name is Zaman Qureshi. I'm a student at American University, and co-chair of the Youth led Design It for US coalition. We applaud the efforts by Chair Khan and the FTC to protect kids online by moving to amend the 2020 privacy order with Facebook, now Meta. We all know that Facebook has consistently failed to protect the personal data of kids and teens. This week, my co-chair made reference to the Guardian report in 2017 that Facebook told advertisers it can identify teens feeling quote, "insecure and worthless."

In 2019, the commission settled with Facebook for a record 5 billion dollars for the company's failure to protect users' data over Cambridge Analytica. In July, 2021, Facebook announced it would only allow targeted ads based on a few identifiers for users under the age of 18, but in an investigation by public interest groups, found that data collection continued for minors, even after the policy change.

More recently, experts have warned that Facebook's expansion into the Metaverse poses a risk to kids and teens. Congressional leaders in March urged a halt on the product's expansion to young people due to ongoing safety concerns. These constant failures are demonstrative of Facebook's inability to protect young people online. Consistently, the company has told regulators and the public to "trust us" and without fail, Facebook has yet to convince people of their plea. The new proposed order would prohibit Facebook from profiting from data it collects on users under 18, and actually enforce its own policies.

We welcome this change and as young people who have grown up fully online, we're grateful to share this space with Chair Khan and join our colleagues to hold Facebook accountable. Facebook's era of self-regulation is over. It's modus operandi of delay, deny, and deflect, is laid bare for all to see. This is why we need real, independent regulation of Facebook, that holds the company accountable, and for its own policies. No minor should have their data monetized and hyper-targeted at them. We welcome the commission's actions, and hope others follow. Thank you for your time.

Doug Farrar:

Thank you very much, Zaman. The last speaker today will be Bilal Sayed. Bilal?

Bilal Sayed:

Okay, thank you. In November, 2018, the Office of Policy Planning, working closely with the Bureaus of Competition, Consumer Protection, and Economics, held a two-day hearing on algorithms, artificial intelligence, and predictive analytics. Those two days of presentations and discussion remain the best public discussion of how AI and related tools will impact the commission's mission. The commission should build on that record.

In 2019, after review and discussion of the record with my then colleagues in OPP, I came to the conclusion that neither I nor the agency, in fact, had sufficient expertise in or with these tools to advise the commission with any depth of sophistication on how AI would or should impact the commission's law enforcement or policy agenda, and also how the commission's law enforcement and policy agenda would affect the development of AI and related tools. As, then, director, I was preparing an alternative, a recommendation to the commission that it establish a standing federal advisory committee to inform and advise the commission staff, the chairman and commissioners on the likely impact of AI on the commission's law enforcement and policy agenda, and the impact of the commission's agenda on the development of AI.

The commission's rules, implementing the requirements of FACA, require, among other things, that an advisory committee have brought participation, meet in public, and receive comment from the public. The advisory committee can also be charged with answering a series of questions, and to produce one or more final reports or recommendations to the commission. Now, no proposal was made to the commission, but I believe this remains a good idea, and I encourage this commission to give it serious consideration, and to solicit from the public recommendations of persons to participate in such a committee on AI. It is not an alternative to the hiring of more technologists or other experts, but a complement and supplement that would have limited impact on the commission's budget. Thank you.

Doug Farrar:

Thank you very much Bilal, and thank you to all of our speakers. We're really proud here at the commission to have these open opportunities to hear from the public on all of the different things we're working on, and thank you for participating. With that, I'll turn it over to Chair Khan.

Lina M. Khan:

Okay, thanks so much, Doug, and just to echo what you just noted, we all really appreciate when members of the public take the time to come speak with us, be it about matters that we're already working on, or on, surfacing for us issues that you think should be on our radar. So, thanks so much to everybody who joined. So we're not going to switch over to the items that we have on today's agenda, and we're actually going to begin with a staff presentation by Ben Wiseman from our Bureau of Consumer Protection, who's going to give us an overview of some of the commission's recent privacy related work, as well as preview the two matters that we're going to be considering before us. So, Ben, over to you.

Ben Wiseman:

Thank you. Good morning, I'm glad to be with you. My name's Ben Wiseman. I'm the acting Associate Director for the Division of Privacy and Identity Protection, or as we like to call it, here at the FTC, DPIP. The lawyers and staff in DPIP are the primary enforcers of privacy at the FTC. I'm particularly grateful for the work of DPIP's staff who have developed deep expertise over many years, and worked tireless to protect the American public every day, and it's their incredible work that I have the honor of sharing with you.

For nearly two decades, DPIP has been on the front lines of technological advances, from the rise of the internet to the introduction of the mobile phone to the increasing use of AI. DPIP has had to continuously adapt its tools and strategies to meet these moments. Today is another such moment. With rapid advancement in new technologies and online services. Our lives are becoming even more enmeshed in the digital world, and, as a result, companies are collecting more and more data from each and every one of us.

As recent matters from the commission have shown, we are ready to meet this challenge. Today I plan to highlight some recent actions from DPIP, as well as the two items before the commission. The notice of proposed rulemaking to amend the Health Breach Notification Rule, and a policy statement on biometric information in section five of the FTC Act. Both of these items have been informed by and fit squarely within the ongoing work in DPIP.

As hard cases have shown, we'll pursue firms, as well as individuals when appropriate, whose conduct misleads or otherwise substantially harms consumers, but our cases also point to broader concerns in the marketplace, including, most significantly, the limitations of relying entirely on notice and consent to meaningfully protect consumers' privacy. Decades of internet commerce have revealed that notice compose enormous burdens on consumers, think lengthy privacy policies, and consent is often no more than a fiction derived from checking a box.

These failures of the notice and choice model are particularly concerning as they relate to people's sensitive data, such

Ben Wiseman:

... such as data from kids, health data and biometric information. Thus, how the commission is working to establish substantive protections for consumer sensitive data will be the focus of my remarks. First, our kids' data. Perhaps no case reflects the commission's continued focus on protecting kids from online harms and privacy abuses more than the Epic Games matter that the commission resolved in December.

Epic Games is the creator of the popular video game Fortnite. The Epic Games matter demonstrates the holistic view we take in cases to ensure substantive protections for children. In addition to requiring the company to come into compliance with COPPA, we also required it to change default settings to be more privacy protective for kids and teens. Significantly, we allege that the default communication settings in Fortnite were unfair. The allegations did not center on whether the company disclosed the practices. Rather it was the substance of the practices themselves that were alleged to be unfair and thus unlawful.

We're also moving towards substantive privacy protections for kids in the Edtech context. One year ago in its policy statement on education technology, the commission made clear that COPPA isn't just about consent, but includes substantive protections for children. And COPPA isn't the commission's only tool in the EdTech space. In a case last year against a major EdTech provider, we allege that Chegg violated the FTC Act when it exposed students' sensitive information.

As a result, we obtained an order that not only requires the company to implement a comprehensive information security program, but also limits how long the company can retain users' data and allows users to instruct Chegg to delete their data. Preventing unlawful collection or sharing of children's and teens' data will remain a top priority for DPIP.

Second, health data. The commission has a long history of working to protect consumer sensitive health data. This effort stretches back over two decades to the commission's first health privacy case involving Eli Lilly, who disclosed consumer's email addresses without their authorization and in the process

identified them as users of antidepressant medication. This work laid the foundation for two recent landmark cases, GoodRx and BetterHelp.

In our complaint against GoodRx, a telehealth and prescription discount platform used by tens of millions of Americans. We alleged that the firm was disclosing sensitive, personally identifiable health information such as medications to advertising platforms like Facebook and Google, and in some cases using that information to advertise to its consumers. This was our first case under the Health Breach Notification Rule.

The complaint also included two unfairness counts as well as deception counts, including account concerning GoodRx's deceptive use of a HIPAA steal. In addition to a monetary penalty, the order we obtained included a ban prohibiting the company from sharing health information with third parties for advertising.

In our matter against BetterHelp, an online telehealth service, we alleged that the company unfairly and deceptively used and shared consumers health information with Facebook and other advertising platforms in order to target those consumers and others like them with ads. In addition to securing a similar ban on the disclosure of health information for advertising, we also obtained nearly $8 million in monetary relief for consumers, the first in a health privacy case.

A few takeaway from these cases. First, with the proliferation of telehealth companies and health related apps, more and more companies are involved in the business of collecting health data. Some of these companies may fall outside of HIPAA's reach, but it doesn't mean that consumers have no privacy protections. So the contrary, the FTC has wide jurisdiction over companies collecting health data and is committed to safeguarding consumer sensitive health information.

Second, the underlying conduct in both GoodRx and BetterHelp involve the use of tracking pixels and Software Development Kits or SDKs. Hidden pieces of code and websites and apps that can transfer user information to advertisers. These cases and recent tech guidance make clear that the FTC will scrutinize companies use of this and any technology that transmits consumer sensitive information.

Third, sensitive health information encompasses a lot of data. It's not just medical diagnosis or treatment, it's also non-medical data from which you can infer sensitive health information. For example, the fact that consumers were visiting or using a mental health treatment service is in and of itself health information. And BetterHelp disclosure of its user's Email addresses was a disclosure of their health information because it effectively identified them as seeking or receiving mental health treatment.

And finally, as we alleged in both GoodRx and BetterHelp, a company's failure to institute policies, practices, and procedures to protect health information causes substantial injury to consumers and violates section 5's prohibition on unfair practices.

This brings me to the first item I will discuss on today's agenda. The notice of proposed rulemaking to amend the Health Breach Notification Rule. The current rule was promulgated in 2009 and since then, technology has changed drastically, including the explosion of mental health apps and connected devices that collect and store consumer sensitive health information.

Further, as an outgrowth of the COVID-19 pandemic, consumer use of such health related technologies has increased significantly. The rule requires notification to consumers, to the FTC, and in some cases the media when there's an unauthorized acquisition of an individual's unsecured health information and a personal health record, whether that's a breach or security incident or voluntary sharing by the company without an individual's authorization.

Importantly, the knowledge we have gained in enforcement along with the comments we received on the rule have informed the proposal set forth in the NPRM before the commission today. It's why

recognizing the proliferation of health apps and similar technologies, we are proposing modifications that underscore consistent with the language in the current rule and the commission's 2021 policy statement that the rule applies to such technologies. And it's also why recognizing that non-health related data can reveal sensitive health information in particular contexts that we make clear the data points such as location, browsing history, and recent purchases can fall within the scope of the rule.

And finally, it's why we are recommending changes that will facilitate better notice to consumers, so that people have more information when their sensitive health information is disclosed without their authorization. The changes we are proposing to the HBNR indicate the seriousness with which we take sensitive health data, and we're likewise squarely focused on protecting consumers' biometric information.

The commission and DPIP in particular have long raised concerns about the use of biometric information, including concerns regarding privacy, data security, and civil rights. Most recently in their Everalbum matter, we alleged the company among other things misrepresented that its facial recognition technology would not apply to videos and photos that users uploaded unless users turned it on. As part of the settlement, our order required the company to delete facial recognition models or algorithms developed with users photos or videos. The policy statement before the commission today reflects our concern with the increasing risks that biometric information technologies pose to the public as well as our continued commitment to using all of our tools to protect people from these harms.

With the increasing uses of biometric information technologies, everyday activities like going to the mall or going to work can subject us to intense surveillance, frequently without our knowledge. And the risk of harm to consumers is not theoretical, it's very real. We know that certain technologies may perform differently across groups which can lead to discriminatory outcomes. Biometric data also has the potential to be used to facilitate fraud and unauthorized access to our devices and online accounts.

Just because a technology is new or innovative does not mean it gets a pass from the FTC Act. As the policy statement makes clear. That is also true for technologies that rely on biometric information. Companies should not misrepresent the accuracy of biometric information technologies or mislead consumers about whether they collect and use biometrics. But not being deceptive is not enough. Companies must take steps to ensure that these technologies are not causing substantial harms to consumers that outweigh any purported benefits.

The FTC will look closely at whether companies have taken such steps, including, for example, assessing the potential harms and risks to consumers, addressing those harms to ensure that consumers are not injured, disclosing the collection and use of biometric information and allowing consumers to opt out, and taking reasonable measures to protect consumers' sensitive biometric data.

I'll conclude by a recent action that illustrates our holistic approach to enforcement. Yesterday we announced a settlement with Premom, a mobile ovulation tracking app in connection with allegations that shared sensitive health information related to menstrual cycles, fertility and pregnancy status from users. The order we obtained includes a ban on disclosing sensitive health data including biometric information like weight and hormone levels to third parties for advertising purposes. It includes a penalty for violations of the Health Breach Notification Rule and it includes comprehensive security and privacy programs that have strong safeguards to protect consumer data.

I'll leave you with one final thought. Companies these days are collecting, using and disclosing vast amounts of consumer sensitive data. Consistent with the commission's priorities, we and DPIP are committed and prepared to use every tool available to protect the American public from privacy harms, not just through longer privacy policies and more boxes to check, but through real guardrails on the use and abuse of people's sensitive information. Thank you.

Lina M. Khan:

Thanks so much, Ben, for walking us through the terrific work that DPIP has been doing recently on protecting Americans' privacy. DPIP has long been doing this work, but I think you're absolutely right that as people's day-to-day lives increasingly depend on these technologies, this work is more important than ever.

I also want to give a big thanks to the Kochava team in DPIP, which is actively litigating one of these matters. So Brian Shull, Julia Horwitz, and Libby Scott, really an important case for us as a commission and I know we're all excited to see it move forward. Before shifting to the items on the agenda, I did just want to briefly underscore a couple of through lines across the health privacy cases that Ben mentioned in particular. So Premom, BetterHelp and GoodRx, I think all of them underscore how seriously we as an agency take protecting American's privacy, especially when it concerns people's most sensitive information.

I think each case highlights how business models that are based on monetizing people's data can lead to situations where companies that Americans are trusting with their sensitive data are then exposing that information for the sake of targeted advertising, analytics and engagement. I think each complaint also really underscores the deep technical expertise that our staff has built, which has allowed our agency to bring our law enforcement tools to bear on what can be quite technically complex business practices.

I think the other big step forward that these cases represent is a move beyond disclosure and towards substantive protections and bright-line rules. As Ben noted around a year ago, we at the commission voted on a policy statement around educational technologies and COPPA, and in that statement we noted some of the substantive protections that COPPA provides and how notice and consent is really failing to keep up with the realities of how Americans are using these digital technologies.

There are several reasons why today's business practices can render consent in these contexts of fiction. We've seen, for example, how businesses can and do use dark patterns to trick people into consent. People also often feel like they don't have any meaningful choice either because they're already locked into using these services or because the service used to critical.

And so the health privacy cases are really building on that insight and building on that policy statement and showing how we are using our tools to move past notice and consent and using our unfairness authority to secure substantive protections and relief, not just check the box processes. And so in each of the health cases discussed today, we allege that the company's conduct was not only deceptive, but also that the collection use and disclosure of health information for ad purposes was an unfair practice. And our use of the unfairness authority in each of these cases makes companies aware that regardless of what they disclosed, there are certain practices that they just cannot engage in. And so the substantive protections and the substantive bans and bright-line rules that we've achieved through these cases, I believe mark's a really important step forward and something that I'm going to be keen to figure out how we can be continuing to build on.

So thanks so much again to the DPIP team for bringing these important cases. Switching over now to the two matters we have on the agenda as Ben previewed, we have a biometrics policy statement as well as a proposed revision to the Health Breach Notification Rule. The biometrics policy statement is a really critical addition to our privacy work. We've all seen over the last decade, how there's greater and greater use of technologies that are tracking, collecting, and using biometric data such as images of people's faces or eyes or fingerprints or recordings of people's voices or gestures. And I think there's serious concern about how these technologies can really undermine American's privacy.

And so we view this policy statement as an important way to put companies on notice about the obligations that they have under the existing laws. One thing that becomes clear from the statements as

well as from the commission's recent blog posts on AI, is that the flexible nature of the FTC Act really positions us as an agency to fully protect Americans privacy regardless of changing technologies. And the statement, the biometric policy statement in particular lays out very clearly how some of these traditional consumer protection authorities would apply to the risks created by biometric information technologies.

One thing in particular that I think is especially important is the note that businesses have to assess and address risks proactively rather than allowing these tools out into the wild and then engaging in cleanup after the fact or expecting third party groups, be it civil society groups or public enforcers to be doing the cleanup.

The policy statement also notes that the FTC Act allows us to act even before consumers are harmed. So the law requires us to show a likelihood of harm and I know we're going to be keeping that in mind as we continue to take a close look at these technologies.

Thank you to the team that worked on this policy statement. I know it was a real group effort across the agency, including Tiffany George, Ryan Mam, Ronnie Solomon, and Elisa Jillson in DPIP, Maggie Cole in Delta, Beth Freeborn in BE, Josephine Liu, Richard Gold, and Francesca Schroeder in OGC and Alejandro Rosenberg in the BCP front office. I also want to give a thanks to my recent attorney advisor who recently departed, Rashida Richardson for all of her great work here too.

Now quickly just switching over to the Health Breach Notification Rule. This really, I think underscores the agency's commitment to making sure we're using all of our tools to protect American's privacy. And it's been really terrific for us to be able to reactivate the Health Breach Notification Rule to make sure we're using it to its full extent.

The HBNR really implements a statute that plainly requires companies to notify consumers when they're disclosing consumers' personal information without authorization. In September 21, the commission issued a policy statement laying out our intention to enforce this rule consistent with its plain meaning. And I'm really glad that in both GoodRx and Premom, we've been able to follow through on that commitment. The proposed changes that we're considering today would effectively make the requirements of the rule even more explicit and clarify certain provisions based on feedback that we received during the rule review. And we really look forward to hearing from the public on those proposed changes. And a big thanks to the team that worked on this rule, including Robin Wetherill, Amanda Koulousias, Tiffany

Lina M. Khan:

George and DPIP, Josephine Lou and OGC, Mike Lagauer and Divesh Rival in BE and Alejandro Rosenberg in the BCE front office. So with that I will turn it over to my colleagues for any comments and thoughts and remarks before moving things for a vote. So we'll start with Commissioner Slaughter.

Commissioner Slaughter:

Thank you so much, Madame Chair, and I want to echo your thanks to Ben and everyone on the DPIP team for that excellent presentation and more importantly for the hard work that is going on behind the scenes every day, protecting Americans' privacy. Despite DPIP's modest size and our considerable resource constraints, especially compared to sister agencies abroad, I believe we're doing some of the most innovative privacy and consumer protection work in the world. Ben's presentation showed just how adaptable and innovative our staff have been at addressing new technological challenges in this rapidly changing environment. Picking up on one thread in that presentation, I am especially proud of the work the FTC has done to advance the privacy protections of kids and teens. All three of us commissioners currently serving are parents of young children, and I think it's fair to say that we're all

above average in our tech savviness, but we all know just how exhausting and impossible it is in practice for parents to navigate the digital consents for every online service their kids use.

That's why the novel provisions in our settlements with Epic games and Chegg are so important. They move the burden away from parents and towards the companies to make their services more privacy protected by default and to minimize the data that companies collect on our kids. A key insight: the data that isn't collected cannot be misused, breached, or shared is when we've put in place across the PIPS enforcement work and Drizly GoodRx and others. I hope we continue to make it clear that protecting their user's privacy, including by shifting the burden of doing that away from the users themselves, has to be a priority for companies to traffic and consumer data. Which brings me to the two items on today's agenda. I'm very pleased to support the Commission's biometric policy statement. It appropriately highlights the risk of widespread deployment of this technology, including more commercial surveillance out in the real world. In retail stores, arenas, airports, and other venues.

The risks of collecting and using this information go beyond privacy and data security. The statement makes clear that we're also watching for the potential discriminatory and civil rights risks of this information being used to approve or deny people access to economic and other benefits or opportunities. I hope that this policy statement and the ongoing work of the commission shows industry that we are well prepared to use our Section Five authority prohibiting unfair or deceptive acts and practices against abuses of this or any other new technology. I'm also happy to support the notice of proposed rulemaking to update, clarify, and strengthen the Commission's Health Breach Notification Rule. As has been mentioned, this rule went unenforced for its first decade despite its potential to protect Americans' most sensitive data concerning their health and wellness. I even partially dissented in a matter of flow health a few years ago because I thought that it should have included account alleging a violation of this rule.

We have now brought two important cases, GoodRx and just yesterday, Premom putting this good, this important rule to work these cases built on the Commission's 2021 policy statement about the rule, which clarified that many health related apps that are not otherwise covered by HIPAA are covered by the rule. Emphasize that breaches of security can involve any unauthorized access and not only the work of nefarious hackers, and forecasted stepped up improvement. And now the notice of proposed rulemaking builds on these foundations by proposing important clarifications and updates to the rule's text. I will look forward to reviewing the comments we received to ensure that the rule can keep pace with rapid changes in society to keep Americans' most sensitive health and wellness data private.

Finally, I want to thank everyone who helped work on today's items. The chair listed all of the many staff that were involved, so I don't want to echo that, but across the agency in the BCB front office in DPIP, in OGC, in BE, in Delta, you guys are doing amazing work and we are so grateful for it and so grateful for the contributions to today's items.

So thank you very much, Madam Chair.

Lina M. Khan:

Thanks so much. Commissioner Slaughter. Commissioner Bedoya.

Commissioner Bedoya:

Thank you. Chair Khan. I want to associate myself with your comments and Commissioner Slaughter's comments on the health breach notification rule. It's extremely important and I support it. I'm looking forward to voting for it. I want to focus my remarks on the biometric statement and I'll start with a story that I think might help set... Serve as a good reminder of why this is so important. So about two years ago, a mom dropped off her teenage daughter at a skating rink in Detroit. So she goes to the front door

and security says she can't go in. They say that she has been involved in a fight there the prior March. But in reality she had never set foot in that skating rink. What had happened was that the skate rinks security system, their face recognition system had said with 97% confidence that she was a match for some other teenage girl who had apparently allegedly been involved in a fight.

Unfortunately, this isn't just happening in skating rinks. This is happening in increasingly important decisions and moments in our lives. When students log online to take a remote exam, when people literally try to walk into the front door of their apartment building. When they go shopping, increasingly automated face recognition algorithms decide for them whether they can do that. And unfortunately, if you are a woman, if you are a kid or a teen, if you are trans or non-binary or if you have a dark complexion, research suggests that biometric technology does not perform as well on you as it does other people. And that is a problem. For most of our history. Surveillance technology has tracked our technology, your car, your phone, your computer. Biometric technology tracks your body. It can track your face, your voice, the distinctive way you carry your body. And thanks to modern technology, it can do it in secret, from far away in a way that used to be completely impossible, and in a way that you cannot avoid.

People get that this is new. People get that this is different, and they responded to it in a way that quite literally, they have never responded to any other form of surveillance. Never in the history of American government and surveillance by our government has a city or state legislature effectively banned a surveillance technology. That didn't happen with wiretaps. It didn't happen with geolocation tracking. It hasn't happened with any other surveillance technology. That changed with face recognition. For the first time in our history, cities and states put near total bans or moratorium on government use of surveillance technology. So this is different, but for too long, scrutiny of biometrics has focused almost exclusively on government use, not commercial use. With today's statement, I am proud that we are setting clear guideposts for how our oldest consumer protection authority, Section Five of the FTC Act applies to biometrics.

I want to take a moment to briefly speak to the companies using this technology and highlight just three of the guidelines that we're issuing today in simple, straightforward language. First, if you're making marketing claims about how accurate your technology is or how it isn't biased, you need proof of that. And not just proof from the lab where all your cameras are high definition and all your photos are of perfect quality. If you make claims about real world validity, accuracy or performance, you need proof of how it performs in real life, in the kind of situation with the kind of technology in which it will actually be used.

Second, when you measure bias, you need to look at how it affects real people before using biometric technology to make choices about them. All of us have an age, all of us have a gender. All of us have different levels of melanin in our skin. Yet too many tests only measure bias across binaries, men versus women, black versus white, young people versus older people. Yet the leading research in the field, for example, by doctors [inaudible] and [inaudible] has shown that measuring bias in this one dimensional way can actually hide the true extent of bias. And so if you're a company using biometric technology, you need to think about how biases in that technology will affect the public. Real people. All of whom have those different characteristics. And you need to address any substantial consumer harm, as you said, Chair Khan, proactively before those harms occur.

Lastly, most importantly, there are some uses of this technology that are illegal in and of themselves. If you are tracking highly sensitive information that can be used to hurt people, if you are doing it in secret in a way that they cannot avoid it, I urge you to consider whether you should be using that technology in the first place. Like you Chair Khan and like you Commissioner Slaughter, I want to express my gratitude to the staff that worked on this and the health breach notification rule. This is absolutely terrific work

and I'm grateful to be associated with it. I'm looking forward to voting for it. Thank you, Chair Khan, back to you.

Commissioner Slaughter:

Madam Chair. Do you mind if I jump back in for one-

Lina M. Khan:

Please go ahead.

Commissioner Slaughter:

One second? Listening to Commissioner Bedoya's extremely erudite and passionate comments about the biometric policy statement, I am reminded that I totally failed to thank him and acknowledge his incredible leadership on these issues. When I started at the FTC, not long after I started the FTC some five years ago and I was trying to get my head around issues of biometric policy and especially facial recognition, and I wanted to understand it better, then Professor Bedoya was the first person I called and he generously came into my office with one of his students and sat down and explained some of the research and some of his thinking and some of the perspectives, and it was really, really illuminating for me.

So his work at the commission has been spectacular and important on this, but he has been a leader in this field and this area in particular for a really long time. And so in addition to gratitude for the staff at the agency whose work led to this statement, I think it's really important to acknowledge the work that has happened in the past and outside of the agency that has helped build our expertise. So thank you Commissioner Bedoya.

Lina M. Khan:

I had the exact same thought listening, Commissioner Bedoya just reminded of his deep expertise on this issue and we're just so, so much better off as an agency for having that expertise. And I know your input and comments in particular really strengthened the statement and made sure that we were taking a look at all sides and really being as assertive as possible. So just want to echo that. Thanks as well to you Commissioner Bedoya and I know we all share an interest in continuing to build on this policy statement as appropriate with our law enforcement work as well. So with that, I will now make the motions for each of these matters. So first I will move that the commission approve and issue the policy statement of the Federal Trade Commission on biometric information and Section Five of the FTC Act that was circulated on May 17th, 2023 under matter number P 2 2 5 4 0 2. Is there a second?

Commissioner Bedoya:

Yes, Madam Chair. Second.

Lina M. Khan:

The motion being seconded. I'll call for a vote. Commissioner Bedoya?

Commissioner Bedoya:

Yes.

Lina M. Khan:

Commissioner Slaughter?

Commissioner Slaughter:

Yes.

Lina M. Khan:

And I vote yes. The motion passes unanimously. I'll now move that the commission also approve and publish the notice of proposed rulemaking to amend the Health Breach Notification Rule circulated on May 18th, 2023 under matter number P 2 0 5 4 0 5. Is there a second?

Commissioner Slaughter:

I second Madam Chair.

Lina M. Khan:

The motion being seconded. I'll call it for a vote. Commissioner Slaughter?

Commissioner Slaughter:

Yes.

Lina M. Khan:

Commissioner Bedoya?

Commissioner Bedoya:

Yes.

Lina M. Khan:

And I vote yes, the motion passes unanimously. Again, really thank you so much again to the DPIP staff and the staff across the agency for their work on both of these. We'll be publishing the biometric policy statements and then also publishing the proposed amendments to the HB and R rules. So we'll be very, very eager to get public comments on that. And with that, we are adjourned. Thanks so much again, everybody for the time today.