FTC Open Commission Meeting | October 21, 2021

Chair Khan:

Good afternoon. This meeting will come to order. We are meeting in open session today to hear a presentation by FTC staff on the privacy practices of internet service providers. Please note that this will not be a deliberative meeting. As with our other open meetings, once we have concluded commission business, we will open up the meeting to hear from members of the public on the work of the commission generally, and any relevant matters that they wish to bring to the commission's attention. The main item on the agenda today is a presentation by FTC staff on the privacy practices of internet service providers, or ISPs. In 2019, the commission issued orders under its 6(b) investigative authority to AT&T and its advertising affiliate, Verizon wireless and its advertising affiliate, Comcast, Google Fiber, and T-Mobile.

Chair Khan:

These orders sought information about each ISP's data privacy practices, including the types of information that is collected, used, and shared, the method and manner that such information is collected, and from which sources the information is received. After reviewing the data shared by these ISPs, along with relevant public information, staff prepared a report that summarized their findings. Staff's in depth study of the data practices of these six major ISPs reveal the staggering breadth and granularity of the information collected by these companies, prompting key questions for us at the commission, as well as for lawmakers and our peer enforcers. The commission voted unanimously to publish this report, which will be made available today.

Chair Khan:

I'd like to thank the staff of the office of policy planning, who under the direction of Sarah Mackey, spent long hours reviewing the data and compiling this report. In particular, I'd like to thank Andrea Arias, Bob Schoshinski, Alex Iglesias, June Chang, Elizabeth Tucci, Richard Gold, and Jared Ho for all their work crafting this study and the report. I'd also like to thank former FTC chair Joe Simons for initiating this effort, Acting Chairwoman Slaughter for stewarding it, and my fellow commissioners for their engagement. After staff's presentation, I will share some comments and then invite my co-commissioners to share any thoughts or reactions in response to the study. I will now turn it over to Andrea Arias to begin the presentation.

Andrea Arias:

Thank you, chair comm. I appreciate the opportunity to present on this very important staff report. Next slide please. In August, 2019, the Federal Trade Commission issued special orders under section 6(b) of the FTC Act to the country's six largest ISPs, AT&T, Verizon Wireless, Charter, Comcast doing business as Xfinity, T-Mobile, and Google Fiber, which comprise approximately 98.8% of the mobile internet market. We also issued special orders to three advertising entities affiliated with these ISPs. AT&T's app Nexus, rebranded as Xandr, Verizon Online, and Oath Americas, rebranded as Verizon Media.

Andrea Arias:

The orders require these entities to provide information about their data collection and use practices, as well as any tools provided to consumers to control these practices. Staff in the FTC's Division of Privacy and Identity Protection collected and analyze the material presented in this report. Next slide, please.

Court Reporter:

This is the court reporter. I'm not hearing anything.

Alex:

It seems Andrea's connection has frozen.

Court Reporter:

Okay.

Alex:

Andrea. This is Alex from Open Exchange. Can you hear me okay?

Andrea Arias:

I can.

Alex:

Okay. You may continue. If you can turn your video on please. Wonderful. Sorry, I think we lost you right at the beginning of this slide.

Andrea Arias:

Great. Can you hear me now?

Court Reporter:

That's correct.

Andrea Arias:

Yep. Great. As an overview for today's purposes, I'd like to discuss a few of the top level findings discussed in the report. Due to sections 6(f) and 21(d)(1)(B) of the FTC Act, which prohibit the commission from disclosing trade secrets or commercial or financial information that is privileged or confidential. The data discussed today and in the report is provided on an aggregated and anonymized basis. The report provides a snapshot in time, comprised of information provided between July 2019 and July 2020. The data pertains to information regarding first, the types of products and services offered by ISPs. Second, the type of data collected combined and used by ISPs. Third, the ways ISPs use data in connection with advertising. And finally, the privacy practices of the ISPs and related entities.

Andrea Arias:

Next slide, please. Many of the ISPs in our study collect and use information to provide one, core ISP services to consumers, such as internet, voice, and video. Two, other services to consumers. For example, internet of things devices, such as home automation and security, connected cars, and wearable devices, and content, such as TV, video, and website content. Three, advertising, including both the service of ads and analytics. And four, other services to businesses, such as mobile money and search services.

Andrea Arias:

Next slide, please. The report discusses at length the variety of ways that many ISPs in our study, and their related entities, collect and use consumers. Data in the interest of time, let me highlight some key findings. First, some ISPs in our study combine data across product lines. Indeed, three of the ISPs in our study reveal that they combine information they receive from consumers across their core services, and at least some of their other services, such as TV and video streaming services, home automation and security products, and connected wearables.

Andrea Arias:

Second, it is not unusual for some ISPs in our study to collect data that is unnecessary for the provision of internet services. In our study, we learned that some ISPs in our study collect data from their customers beyond what is necessary to provide ISP services, and use that additional data to enhance their ability to advertise to consumers. For example, several ISPs in our study collect information about consumers' app usage history to use in connection with advertising.

Andrea Arias:

Third, a few of the ISPs in our study use web browsing data to target ads. In fact, two of the ISPs in our study stated that they use web browsing information to target ads to consumers, and another reserves the right to use such information for advertising purposes. Notably, while consumers can block tracking by additional tracking ad networks through browser or mobile device settings, they cannot use these tools to stop tracking by these ISPs which use or have used super cookie technology to defeat those tools and persistently track users.

Andrea Arias:

Four, many of the ISPs in our study group consumers using sensitive characteristics to target ads. Many of the ISPs in our study serve targeted ads across the internet on behalf of third parties. In doing so, they place consumers into segments that often reveal sensitive information about consumers, allowing advertisers to target consumers by their race, ethnicity, sexual orientation, economic status, political affiliations, or religious beliefs. Examples of such segments include viewership gay, pro-choice, African-American, Jewish, Asian achievers, Gospels and Grits, Hispanic Harmony, and political views, Democrat and Republican. Fifth, some ISPs in our study combine personal app usage and web browsing data. In fact, at least three ISPs report combining consumers' personal information, app usage information, and/or browsing information for advertising purposes. This gives ISPs the ability to target consumers on a granular basis, because unlike many other entities, ISPs have access to each of the websites a consumer visits, and they can target based on subscriber information.

Andrea Arias:

Finally, a significant number of the ISPs in our study share real time location data with third parties. There is a trend in the ISP industry to offer real-time location data about specific subscribers to their third-party customers. In addition to using this information for emergency roadside and medical assistance, there've been reports that car salesman, property managers, bail bondsmen, bounty hunters, and others have used such information. Next slide, please.

Andrea Arias:

In addition to discussing how many of the ISPs in the study collect and use data, the report also examines their practices relating to notice and disclosure, consent and choice, and access correction and

deletion. We have concerns in four key areas. The first is opacity. While several ISPs in our study tell consumers they will not sell their data, these ISPs obscure the myriad of ways that their data can be used, transferred, or monetized short of selling it, often burying such disclosures in the fine print of their privacy policies. In addition, three of the ISPs in our study reserve the right to share their subscribers' personal information with their parent companies and affiliates.

Andrea Arias:

The second area of concern is illusory choices. There's a trend in the ISP industry to purport to offer consumers some choices with respect to the use of their data. However, problematic interfaces can result in consumer confusion as to how to exercise these choices contributing to low opt-out rates, typically less than 2% of total subscribers.

Andrea Arias:

The third area of concern is a lack of meaningful access. Although several of the ISPs in our study purported to offer consumers access to their information, the information they provided was often indecipherable or nonsensical without context, contributing to low access requests. For example, an individual's information might be labeled by an ISP in a code with a symbol attached, such as religion code as 54, race code as W, heritage code as 23, [inaudible] plus four, US consumer segment as N. This coded information, without explanation, would be meaningless to a consumer.

Andrea Arias:

The final area of concern is data retention and deletion. While several of the ISPs in our study provided timeframes for deleting information, many asserted that they keep the information as long as it is needed for a business reason. However, business reason is a vague term that many of the ISPs in our study can define as broadly as they wish, or leave undefined, giving them virtually unfettered discretion. In addition, some of the ISPs in our study give all us consumers the right to delete their data. Others restrict the right to California residents. Next slide, please.

Andrea Arias:

Finally, the report makes several observations about the ISP industry. Our first observation is that many ISPs in our study amass large pools of sensitive consumer data. Several ISPs in our study and their affiliates collect significant amounts of consumer information from the range of products and services that they offer. The vertical integration of ISP services with other services, like home security and automation, video streaming, content creation, advertising, email, search, wearables, and connected cars. From it's not only the collection of large volumes of data, but also the ability to pool and cross reference highly detailed data about individual subscribers, resulting in extremely granular insights and inferences to not just ISB subscribers, but also their families and households.

Andrea Arias:

Our second observation is that several ISPs in our study gather and use data in ways consumers do not expect and could cause them harm. While consumers certainly expect that ISPs to collect certain information about their websites they visit in order to efficiently provide internet services, they would likely be surprised at the extent of data that is collected and combined for purposes unrelated to providing the service they request. In particular, browsing data, television viewing history, contents of email and search, data from connected devices, location information, and race and ethnicity data. More

concerning, this data could be used in ways that are harmful to consumers, including by property managers, bail bondsmen, bounty hunters, or those who would use it for discriminatory purposes.

Andrea Arias:

Our third observation is that although many ISPs in our study purport to offer consumers choices, these choices are often illusory. Although many of the ISPs in our study purported to offer consumers choices, some of these choices were not offered clearly and indeed nudged consumers toward greater sharing of personal data through a variety of dark patterns. Indeed, we found interfaces where the option to share more data was highlighted and the option to share less was grayed out. We found interfaces that did not allow consumers to reject information collection or that continually prompted consumers if they selected a disfavored setting. We found interfaces that buried or hid certain choices from consumers, and we even found unclear toggle settings that led to the selection of unintended privacy settings.

Andrea Arias:

Finally, our last observation is that many ISP in our study can be at least as privacy intrusive as large advertising platforms. Despite ISPs' relatively smaller size in the advertising market dominating by Google, Facebook, and Amazon, the privacy challenges that permeate the advertising ecosystem may be amplified by ISPs. Because first, many ISPs have access to 100% of consumers' unencrypted internet traffic. Second, many ISPs are able to verify and know the identity of their subscribers. Third, several ISPs can track consumers persistently across websites and geographic locations. And fourth, a significant number of ISPs have the capability to combine the browsing and viewing history that they obtained from their subscribers with the large amounts of information they obtained from the broad range of vertically integrated products, services, and features that they offer. Next slide, please.

Andrea Arias:

We encourage you to read the entire report, which provides additional and more detailed information about these findings. Thank you very much.

Chair Khan:

Thank you so much, Andrea, for the terrific presentation, and again for all your hard work on the report. So as the internet has become increasingly essential for navigating modern life, scrutinizing the practices of the firms that provide these key services is critical. The staff study does a terrific job of documenting the data privacy practices of internet service providers, including their extensive collection, consolidation, and use of customer data. The findings are striking, and the staff report is worth reading in full. In short, Internet Service Providers are surveilling users across a broad swath of activities, enabling hyper granular targeting in the servicing of ads and other services.

Chair Khan:

In my view, the staff report should focus our attention on a few key issues. First, I believe these findings underscore deficiencies of the notice and consent framework for privacy, especially in markets where users face highly limited choices among service providers. The report found that even in instances where internet service providers purported to offer customers some choice with respect to how their data was collected or used in practice, users were often thwarted by design decisions that made it complicated, difficult, or near impossible to actually escape persistent tracking.

Chair Khan:

The fact that several ISPs made general privacy commitments that were [inaudible] by text buried in their fine print is emblematic of the broader ways in which users are often deprived of the conditions that would actually enable them to exercise meaningful choice and the ways in which the current configuration of commercial data practices often fail to reflex actual user preferences. A new paradigm that moves beyond procedural requirements and instead considers substantive limits increasingly seems worth considering. Second, the expansion of ISPs into vertically integrated entities that not only provide internet, voice and cable services, but also produce the content transmitted across these pipes and sell behavioral advertising has enabled these firms to consolidate and aggregate a staggering array of data. ISPs today have access to not only what websites you visit and your location at any given moment, but also the content of the emails you write, the videos you stream and the devices you wear. The ways in which expansion across markets enables firms to combine highly sensitive and often highly valuable commercial data underscores the need for us to consider in our merger review, how certain deals may enable degradation of user privacy. Third, the individualized and hyper granular dossiers that ISPs are collating can enable troubling and potentially unlawful forms of discrimination. As the report notes, the collection and use by ISPs of data on race and ethnicity raises the risk of digital redlining and other practices that undermine civil rights.

Chair Khan:

Although enforcers must scrutinize these practices, there are serious questions around whether the type of persistent commercial tracking that we see employed by internet service providers and other market participants across the economy creates inherent risks. Moreover, the information asymmetries that enforcers face when seeking to fully understand how firms are actually using this data also raises questions around whether we must target our efforts upstream at the collection of particular forms of data, rather than just its use.

Chair Khan:

Lastly, as the risks of persistent tracking continue to come to light, we face more fundamental questions around what it means to condition the use of essential technologies on this type of user surveillance. It's worth noting, of course, that the Federal Communications Commission has the legal authority and expertise to fully oversee internet service providers. I fully support efforts to reassort that authority and once again, put in place the non-discrimination rules, privacy protections, and other basic requirements needed to create a healthier market.

Chair Khan:

We intend this report to be the continuation of an ongoing discussion about commercial data practices and user privacy and I look forward to continuing to consider how we can incorporate these insights into our work. Thank you again to agency staff for their hard work in producing this report and highlighting these important issues. I'd like to now open it up to my fellow commissioners to share any thoughts starting with Commissioner Phyllis.

Commissioner Phillips:

Thank you, Madam Chair. And thank you, Andy, for that great presentation. I also want to commend you Sarah and the rest of the team for their excellent work on this project, which as the audience have heard the commission initiated in 2019. Congress gave the commission investigatory power in Section 6 of the FTC Act, a critical tool for advising Congress and the public of facts to inform the policy making process.

By way of background, in 2016, the FCC, the Federal Communications Commission issued a privacy rule concerning internet service providers. Invoking the Congressional Review Act, however, Congress undid that rule. That put the FTC back as the cop on the beat for ISP privacy, which we proceeded to study using our 6(b) subpoena authority. This snap report is the culmination of that effort, a gun under a Republican led FTC and ending under a democratic led one. This is a good example of the bipartisan way in which the FTC functions, when the policy process is allowed to work. The report sheds light on the privacy practices of ISPs revealing the types of information they collect from customers of their various business lines, information they obtain from other sources outside the business and the ways in which they may combine and make use of that data.

Commissioner Phillips:

ISPs can amass vast amounts of personal data on consumers and the report highlights the need for greater transparency. It also presents useful information about the privacy choices that ISPs currently make available to consumers and suggests ways that consumer interfaces could be made more user friendly. I don't agree with everything in this report and I'm concerned that too often, it goes outside of the bounds of what we study. The report also particularly focused on ISP's use of data for advertising.

Commissioner Phillips:

I have some concern with language suggesting that combining data obtained from consumers with other sources for advertising is necessarily bad and suggestions that targeted advertising is per se, harmful to consumers. I'm also concerned that the report rehearses the arguments that privacy problems are both the result and cause of market power, theoretically plausible, but counterintuitive claims that I have addressed elsewhere. The report cuts against these arguments to some extent stating that the ISPs in question, which it describes as "small players" in the digital advertising industry "can be at least as privacy intrusive as large advertising platforms" like Google, Facebook and Amazon. But my disagreements with this or that aspect should not stand in the way of staff releasing a report, reflecting good work over a long time and that I hope will contribute to the ongoing conversation about consumer privacy. So thanks to all of you.

Chair Khan:

Thanks so much, Commissioner Phillips. Commissioner Slaughter.

Commissioner Slaughter:

Thank you Madam Chair, and thank you to Andrea and everyone for the presentation and for all of your hard work on this report. It is a really important document that shows just how essential our investigative authority can be to uncovering prevalent industry practices. This report sheds light on the truly staggering amount of data collection and surveillance broadband internet service providers conduct on their customers. It points to the need for urgent action across agencies and in Congress to protect users of these ubiquitous and critical services. I think the report speaks well for itself and I really also want to associate myself with all of the comments that the chair made at the beginning with which I agree entirely, but I'll just highlight three quick takeaways that were the most important from my perspective. First, the data uncovered in this report underscores what in my view is the era of the last administration's rescission the open internet order, more commonly called net neutrality.

Commissioner Slaughter:

The FCC is our country's expert telecommunications regulator. It should be able to investigate and regulate the practices of internet service providers, a critical part of telecommunications infrastructure. This report shows how absent the FCC's oversight, many ISPs participated in a race to the bottom to partake in the lucrative market of monetizing their customer's personal information. I hope the FCC is able to return ISPs to their proper classification as telecom services under Title II, and to provide appropriate protections for these essential services.

Commissioner Slaughter:

Second, this report is a call to action for the FTC too. The study uncovered massive over collection and surveillance of Americans by their ISPs, practices that are common across the internet and ecosystem. As we just heard, ISPs collect far more information on their customers than is necessary to provide them the service for which they pay. They collect information like browsing history, contents of email, search history, location data, and monetize it to make even more money off their customers in ways I doubt most of their subscribers understand or ever aware of. The report also has like the ways in which as the chair so eloquently articulated a notice and choice regime to control data collection and abuse is merely illusory, rendering it functionally ineffective.

Commissioner Slaughter:

Finally, the report illustrates some of the ways in which the harms and abuses that stem from the over collection that fuels digital surveillance go beyond traditional privacy concerns. In fact, civil rights abuses, digital redlining and further marginalization of black and brown communities, the LGBTQ+ community can all stem from the compilation of this information and its sharing with unrelated businesses. Addressing these equity issues head on is a critical part of the FTC's mission to make sure we have an economy that is fair and works for everyone.

Commissioner Slaughter:

This report demonstrates problems of unavoidable and unfair behavior across the internet economy. While it certainly supports better oversights of ISPs, oversight of ISPs by the FCC through revive net neutrality regime, I think it also shows the value of clear rules on data abuses, including limits on collection and use to protect people's rights. I look forward to working with all of my fellow commissioners to seeing that through. Thank you.

Chair Khan:

Thanks so much, Commissioner Slaughter. Commissioner Wilson.

Commissioner Wilson:

Thank you, Madam Chair for setting aside time for the staff to present these important findings. I would like to thank Andrea and all the rest of this staff who worked on this report for their excellent work in conducting this study, preparing the report and delivering this summary of findings. I would be remiss if I didn't take a moment today to thank Maneesha Mithal, the Associate Director of the Division of Privacy and Identity Protection also known as DPIP and Daniel Kaufman, Former Acting Bureau of Consumer Protection Director for their supervision of our privacy program.

Commissioner Wilson:

Daniel left the agency a week ago and Maneesha is leaving shortly. Maneesha and Daniel's exemplary combined decades of service to the agency were of great benefit to consumers and their loss will be felt for many years to come. The FTC's ability to conduct industry studies using our 6(b) authority is one of the agency's unique strengths, a support using this authority to continue our learning in this area.

Commissioner Wilson:

This study is one important step in our journey. We have another study underway, analyzing data collect action and use by social media and video streaming services. I look forward to reviewing the findings of that study as well. These studies constitute some of the most important work the commission is doing. So I commend the staff for their tireless efforts in this area. Given these studies in our extensive portfolio of and data security cases, I believe authority in this area should remain at the FTC. I am disappointed that some of my colleagues fail to appreciate the value that we add in this area and wish to give away our jurisdiction.

Commissioner Wilson:

But I guess I shouldn't be surprised given the disdain that current leadership has expressed both for our staff and for the important work of the agency. Moreover, I am disappointed by my colleague's choice to politicize the important findings of this study and thereby detract from the information that we can otherwise add to the important dialogue on the need for additional transparency in this area for consumers who absolutely need to understand more clearly the kinds of information that are collected from them and the uses to which the collected data is put.

Commissioner Wilson:

In closing, I'd like to thank, again, Chair Khan for setting aside time to make known these important findings and also DPIP and the Office of Policy and Planning for their important work in this area.

Chair Khan:

Great. Well, I'd like to thank the commissioners for their remarks. Certainly much to continue discussing and thinking about as we continue our important work in this area. This concludes the official agency business of the commission that we are disposing of today under the Sunshine Act. I am adjourning the meeting and we will now turn to hearing from members of the public. 16 individuals have signed up to address the commission today. Based on feedback from some of my colleagues, we have increased from one minute to two minutes, the time that we've reserved for each person to speak. Based on additional feedback, we will also consider for the next meeting taking public comments at the beginning of the meeting rather there then at the end, and assessing how that format works. So I'll now turn it over to Lindsay Kryzak to open it up to the public.

Lindsay Kryzak:

Thank you, Chair Khan, before we begin, please note that the FTC is recording this event, which may be maintained, used, and disclosed to the extent off authorized or acquired 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. Today, each member of the public will be given two minutes to address the commission. Our first speaker is Jim [inaudible].

Lindsay Kryzak:

Jim. Okay, we'll come back to Jim a little bit later. I know he was on earlier. Our next speaker is Tad Mollnhauer.

Tad Mollnhauer:

Can you hear me?

Lindsay Kryzak:

We can. Yes.

Tad Mollnhauer:

Okay. My name is Tad Mollnhauer and I'm the executive director of the National TUPSSO Franchise Owners Association, and a 14 year UPS Store franchisee. I'm deeply concerned about the imbalance of power that exists within my brand. The latest franchise agreement mandates a remodel that can cost more than the current fair market value of my store. This mandate will certainly have a negative impact on my equity as I will be forced to walk away from my six figure investment, sell for a loss, or essentially buy my store for a second time at the end of my current franchise agreement.

Tad Mollnhauer:

In addition, the latest franchise agreement introduces a new three strikes in your [inaudible] policy. If a franchisee receives three or more customer complaints or negative reviews within a six month period, then at its sole discretion of The UPS Store, Inc., the franchise agreement can be terminated without opportunity to cure or appeal such a decision.

Tad Mollnhauer:

What qualifies as a negative complaint or review has not been specified despite the fact that the vast majority of the complaints reported are not related to the franchisee's operational obligations. So theoretically, a six figure investment can gloss simply because somebody had a bad day and complained about a UPS service failure, something which is beyond the control of a franchisee on Facebook, Instagram, and Yelp. For these reasons and many, many more I fully support the petition submitted September 22nd, asking the FTC to investigate the business practices of the franchise industry. Thank you for your time and thank you for your attention to this matter.

Lindsay Kryzak:

Thank you, Tad. Our next speaker is Aurelien Portuese.

Aurelien Portuese:

Hello. Can you hear me?

Lindsay Kryzak:

We can. Yes.

Aurelien Portuese:

Right. My name is Aurelien Portuese and I'm the director of The Schumpeter Project on Competition Policy at the Information Technology and Innovation Foundation. I would like to make two points about consumer privacy that the FTC should consider in order to promote not stifle innovation. First, the popular claim that consumers pay with their data is plain wrong. Of course, many companies monetize data, but there's no monetary transactions from consumers to the company. Quite the contrary, consumers often have discounts and free services, thanks to the data that they generate. Consequently, there's no consumer harm under [inaudible] laws when companies monetize consumer's data, the consumer benefits, thanks to this monetization by the provision of free product and services. Second, establishing the sector focused privacy laws for is ISPs is neither needed nor beneficial. An ITIF analysis

Aurelien Portuese:

Showed that the major ISPs have strong privacy policies that allow consumers to opt out. Rather than craft an ISP specific privacy regulation, Congress should pass a national privacy law that preempts states and set baseline standouts for the whole economy. Consequently, the FTC should advocate for a national and privacy law that applies to all US companies instead of being willing to unilaterally enforce sector specific privacy standards that will distort competition across industries. Thank you for considering those remarks and thank you for having given me the opportunity to speak today.

Lindsay Kryzak:

Thank you Arlan. Our next speaker is John Wickiser, John.

John Wickiser:

Yes. Can you hear me?

Lindsay Kryzak:

We can, yes.

John Wickiser:

John, again, an average person with an idea, continuing the conversation from where we left off on September 15th. Large technology groups that monopolize current and newly discovered social inventions can be stopped from that monopolization in our free and open market environment. If we simply utilize the existing framework and laws as have been established, and individuals meet their ethical and moral obligation in performing their job. Motivated consumer identifies a problem, large technology inventions trying to be social inventions. These technology inventions disregard the primary means of separation from a social invention. They want to maintain secrecy instead of privacy, they want to have the overriding control instead of provide security. In other words, they may provide options, but the lack of transparency shows ultimately they choose for us. A real social invention provides us the consumer privacy security and our own ability to choose what we share. Knowing that there are times when the social invention has to be that: social and selfless, not selfish.

John Wickiser:

And so collectively we agree by majority how that should be handled. Will you identify existing patented intellectual property that exists with a purpose and process in the social invention realm, listen to and support inventors and entrepreneurs that are unable to defend against attacks from these massive

technology inventions, knowing that a real social invention must belong to society. How do we create something like that? Protect it, allow every person equal ownership in it. I have ideas as that is my question to the FTC commission.

John Wickiser:

In my attempts to do so, it has been created, validated, the utility process secured by US Patent 10885096, multi-user integrated communication platform. And now I ask you to help in protecting it and establishing a way for all of us to have fair and equal ownership in it. By doing so you will see the property and utility process provide superseding solutions to the technology inventions being manipulated today, solving many problems as we consumers are currently experiencing. Many of these large entities have been notified of their illegal activities, infringement, their fraud and deception placed upon the consumer. Enforcement entities have been notified as to the criminal side.

Lindsay Kryzak:

Thank you John. Sorry to interrupt. Thank you. Our next speaker is Tyson Slocum. Tyson.

Tyson Slocum:

Hi, Madam Chair. Thanks so much for the opportunity to be here today. I'm Tyson Slocum, I direct the energy program with Public Citizen, where I focus on the regulation of electric power, natural gas and petroleum markets. And the problem I wanted to raise today is that weak affiliation and competition rules in Federal Energy Regulatory Commission jurisdictional power markets are exposing consumers to anti-competitive harm, and we're asking for the FTCs help. FERCs default rules conclude that any owning less than 10% of a power seller has a rebuttable presumption that they can't control that power seller and therefore such entities are excluded from competitive market screens. In 2009, the FTC provided fantastic criticisms and a formal docket of these weak FERC standards, with the FTC noting that FERC relies too much on the role of the 10% control in the competitive analysis with no consideration of the incentive effects associated with partial acquisitions or the possible increased risk of coordinated interaction from such investments, especially by hedge funds and private equity firms.

Tyson Slocum:

US power markets have recently been defined by a significant influx of hedge fund, private equity and wall street bank investments that appear to undermine competition. And so far FERC has failed to take effective action. I have raised numerous formal challenges at FERC regarding hedge funds that appear to significantly influence the operations of power sellers, and so far FERC has failed to adequately address this.

Tyson Slocum:

For example, I submitted formal protests at FERC noting that the hedge fund Elliot Management has acquired significant financial stakes in at least four competing power sellers, negotiated non-public agreements with those power sellers that grant Elliot Management, sweeping access to material non-public business information, and conspired with additional hedge funds, such as Bluescape Energy Partners to install preferred board members, and significantly direct management of these power sellers. FERC so far has failed to take action.

Tyson Slocum:

Separately when Carl Icon acquired less than a 10% stake in First Energy, but installed two of his top executives on the board, we raised a protest at FERC and again, FERC declined to take action. Finally, we provided evidence to FERC that a management services agreement between the energy focus private equity fund IIF and the Wall Street bank, JP Morgan Chase.

Lindsay Kryzak:

Thank you Tyson.

Tyson Slocum:

Thank you.

Lindsay Kryzak:

Our next speaker is Jim Halpert. Jim.

Jim Halpert:

Thank you very much. Apologies for not being present when you first called my name, I'm at the International Association of Privacy Professionals conference and was at a reception for people who've been at the bar for a very long time. I've been practicing for 25 years in this space. I do have just a few comments, particularly with regard to transparency. It's important. I've followed all the state privacy and security laws. It's important to understand that there is a big movement in the states toward very, very long notices that are required. The California Initiative, the CPRA will require extensive privacy notices with regards to very specific categories of data that will make transparent, clear notice to consumers, which is very important in this area, more difficult. And having one set of rules, one set of requirements for transparency and for other rules with regards to data, I think will be easier for consumers to understand.

Jim Halpert:

And also requiring that notices be provided in a clear way that's easily comprehensible, but limiting the amount of information that needs to be in the pop up prominent notice to consumers will be a much better way to allow consumers to understand and make decisions with regard to use of their personal data.

Jim Halpert:

I also wanted to point out to you that states are adopting conflicting requirements with regard to sensitive categories of personal information, which I specifically noted as being of concern to the commission and its findings in this report. In some states, there's an opt out rule with regard to this data. In others there's an opt in rule and having one set of clear rules that gives consumers the ability to exercise choices and make decisions on a national basis, no matter where they're located in a particular moment would be preferable I think to the existing fragmentation. I'd also make the point that having different rules for different businesses often doesn't make sense. And so...

Lindsay Kryzak:

Thank you Jim.

Jim Halpert:

Thank you very much.

Lindsay Kryzak:

Our next speaker is Arthur Stamoulis. Arthur.

Arthur Stamoulis:

Good afternoon. Again, my name is Arthur Stamoulis, I'm speaking on behalf of the Trade Justice Education Fund, which is a nonprofit focused on how emerging issues in trade policy affect workers, consumers, and civil rights. And I'm here today to flag our concerns about how so-called digital trade proposals could limit government's ability to protect consumer privacy and to combat anti-competitive business practices. Certain terms of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, the Digital Economic Partnership Agreement and the WTO's joint statement initiative on eCommerce are problematic in both of these areas.

Arthur Stamoulis:

First, these proposals contain binding language that would undermine consumer privacy and data security by prohibiting limits on cross border data flows, as well as rules on the location of data storage facilities. And second, they contain provisions that forbid countries from establishing or maintaining policies that limit the size or range of services offered by online companies that limit the legal structures under which companies may be required to operate, and that otherwise restrict the regulation or breakup of tech monopolies.

Arthur Stamoulis:

And so we urge the FTC to please investigate the various digital trade agreements that the United States is being encouraged to join, and to ensure that such pacts did not end up restricting the regulatory space needed for consumer protections and for pro competition measures. The digital economy is obviously an area where there's still not widespread agreement on the regulatory environment needed to best protect consumer privacy, civil rights, gig economy workers, and small businesses. Our view is that cementing in any particular system by a trade pact at this point is likely to privilege the interest of the largest players in this sector, over the interest of the majority and to needlessly tie regulators' hands. We thank you for your consideration.

Lindsay Kryzak:

Thank you, Arthur. Our next speaker is Matthew Dinger. Matthew.

Matthew Dinger:

Thank you to the commission. My name is Matthew Dinger. I live in Salt Lake City. I am a member of the board of trustees of T1 International and a patient with type one diabetes. Nearly 100% of the US insulin market is dominated by three corporations, Eli Lilly, Novartis and Sanofi. These companies have a well established record of anti-competitive behavior, frequently raising prices within days or even hours of each other in search of higher and higher profits, no matter the impact on patients. One quarter of patients with diabetes in the United States ration their insulin. I am one of them because the same insulin that used to cost $15 a vial now costs nearly $300. At the end of last year, I changed jobs and as a result was uninsured for a month. I had time to prepare for this, so I made sure I filled a three month

supply of insulin, researched the rules for COBRA to make sure that I could retroactively apply for it if something catastrophic happened.

Matthew Dinger:

And even when I did receive insurance, I avoided getting insulin until January because I had a new deductible to meet. So my out of pocket insulin costs would've been about a thousand dollars a month. I rationed my insulin. These are the things that I had to do in order to stay alive and secure my family's financial future as an insulin dependent diabetic. I'm a job loss away from financial ruin because the concentration of economic power, when it comes to the price of insulin, lies almost entirely in the hands of three companies. I am completely beholden to them, and that terrifies me. I'm asking the FTC to make insulin pricing a priority issue on the competition council to help thousands of patients like myself. Thank you.

Lindsay Kryzak:

Thank you, Matthew. Our next speaker is Anna Squires, Anna.

Chair Khan:

Hi. So my name is Anna Squires and I have been a type one diabetic for almost 11 years. I am joining T1 International and asking the Federal Trade Commission to make the cost of insulin a priority issue on the competition council. In the time since my diagnosis, I've used $132,300 in insulin pens and vials. That number does not include all of the supplies that I also need to survive, and all of the hours spent traveling to and from doctor's appointments. The approximate cost to produce the same amount of insulin that I have used is $3087. Diabetes does not choose who it impacts. It is not a living thing. If you know nothing about diabetes, learn this today: I need insulin to survive. Without insulin, a diabetic will die. It is graphic, but it is true, and I need the commission to understand the urgency behind this issue.

Chair Khan:

There is no other treatment for type one diabetes, and there is no cure. I have to make multiple medical decisions that could end my life every time I want to eat, exercise, or go out with my friends. In the world, three companies, Eli Lilly, Novartis, and Sanofi produce and provide 90% of insulin. These pharmaceutical companies leech every cent they can off of people who are already dealing with a debilitating, chronic illness. Many diabetics live below the poverty line and are unable to afford basic necessities, let alone $900 a month in medications. Life giving prescriptions should not be a for-profit business venture for people who already own three homes. The patent for insulin was originally sold for $1 so that all those who need it could access it. 100 years later, it is treated as a luxury rather than an absolute necessity. The longer these companies are allowed to price locking their insulin, which is a clear sign of a monopoly, the more people will unnecessarily suffer and die. Thank you.

Lindsay Kryzak:

Thank you, Anna. Our next speaker is Shane Toos. Shane.

Shane Toos:

Thank you, Lindsey. And thank you commissioners for the opportunity to speak to the commission about the importance of consumer data collection and privacy regulation. I'm Shane Toos. I'm a non-resident Senior Visiting Fellow at the American Enterprise Institute. The most important part of the FTC conducting these studies is the reminder of the importance of moving forward with a federal privacy law

that should cover all US citizens and move us away from the current patchwork process that creates a lot of consumer confusion.

Shane Toos:

We need to take a holistic approach to privacy protections, and apply the same safeguards to all the entities throughout the internet ecosystem that are collecting and using data. Consumers should all expect that every company that engages online will be affording the consumers the same protections. Subjecting different companies to different requirements is confusing to consumers and reduces their confidence in the privacy of their online information. We need to build a transparent and accountable way to regulate consumer data to ensure the understanding that the information that is collected, stored, and deleted is done so in a secure fashion. A privacy framework would avoid the current fragmentation of guidance and encourage more secure digital innovation. Again, thank you for the time to speak today.

Lindsay Kryzak:

Thank you Shane. Our next speaker is Nancy Liven. Nancy. Nancy Liven? Okay. We'll try to come back to Nancy. Our next speaker is Adam Tobin. Adam.

Adam Tobin:

Thank you. Yes. Can you hear me okay?

Lindsay Kryzak:

We can. Yes.

Adam Tobin:

Great. Thank you for the privilege to speak. My name is Adam Tobin, adjunct professor at Brandis University, advisor at Canon collective with 25 years experience across privacy identity media and targeting techniques. With this report's focus, some context from my research can explain why ISPs do not play a unique role in the collection and use of consumer data.

Adam Tobin:

First ISPs do not pose unique threats and are not able to collect online consumer data in any unique way that increases privacy risks for consumers. And in fact, face significant restrictions with encrypted traffic and VPN usage, significantly limiting ISP data access to domain information, or even less in the case of VPN. Also, consumers are expanding the use of mobile devices to access the internet, fracturing ISP visibility between for example, home and coffee shop internet experiences.

Adam Tobin:

Second ISPs are not relatively big ad tech players. Non ISP platforms derive most, sometimes virtually all, of their revenue from advertising sources. ISPs by contrast collect most revenue from subscriptions and thus have less need to use consumer data for advertising purposes.

Adam Tobin:

Third and finally digital platforms pose far greater risks to consumer privacy, and here's why: encryption does not prevent these platforms from collecting vast consumer data since they decrypt internet traffic to carry

Adam Tobin:

Out the consumer's desired function. Second also, these digital platforms, track consumer activity across multiple devices and websites with unparalleled reach, non ASP digital platforms on nine of the top 10 mobile apps and all finally digital platforms use expensive consumer data and mature machine learning capabilities to develop powerful predictive models of consumer behavior. I should know, I've spent over 15 years of my career advising on the construction and inherent privacy limits of these ad models. These models achieve what researchers affectionately call data intimacy, which is an approach to gather and infer and materially greater levels of effectiveness. The most predictive consumer behavior to drive an advertising revenue. These inferences aligned with the platforms, advertiser driven incentives, pose a privacy risk.

Lindsay Kryzak:

Thank you, Adam.

Adam Tobin:

That we should all keep in context. Thank you very much.

Lindsay Kryzak:

For our next speaker, we're going to go back to Nancy Libin. Nancy?

Nancy Libin:

Thank you very much. And sorry about that, I was having technical difficulties. I'm currently a lawyer in private practice and was the chief privacy officer at the justice department under the Obama administration. And I want to discuss briefly the very good work that the FTC did on consumer privacy during that administration and in particular it's 2012 privacy report. And [inaudible] building on that, going forward, that report articulated a flexible technology neutral framework that among other things distinguishes between nonsensitive and sensitive data, giving the latter heightened protection and provides the companies shouldn't have to give consumers choice for data use and disclosure. That's consistent with the context of the transaction or with the company's relationship with the consumer. This framework was praised by privacy advocates and industry alike as achieving the right balance in ensuring strong protection per consumers while allowing businesses to innovate and operate without unnecessary friction in the marketplace.

Nancy Libin:

For instance, under this framework, companies generally don't need to provide consumers with choice about the use of their data for first party marketing, because such use is consistent with the context of the relationship and consumer consent can be inferred. However, the framework directs companies to give consumers an opt-out mechanism when context doesn't allow consent to be inferred in an opt-in mechanism. When companies deliberately collect and market using sensitive data, the Obama white house took a similar approach in its 2012 consumer privacy bill of rights, which also recognized that

companies should infer consumer consent, for first party marketing explaining that consumers expect such use and have an easily identifiable party to contact or end a relationship with if they are dissatisfied. To conclude the FTC report and the Obama privacy bill of rights are a great foundation for a national conversation about the FTCs approach going forward. Thanks for the chance to speak today.

Lindsay Kryzak:

Thank you, Nancy. Our next speaker is Van McGuire. Van?

Van McGuire:

Hi, good afternoon everyone. Thank you for allowing the public to get involved. My name is Van McGuire. I'm a student at University of Massachusetts studying cybersecurity and digital forensics, at this moment. The two points I would like to point out to the FTC, which requires further investigation is two issues. One is healthcare privacy for the use of third party apps by healthcare providers like commissioner Slaughter pointed out this, actually crosses lines and causes civil violations as well for people because these apps are requiring people to go ahead and sign up having a privacy policy posted on a website is not enough. There has to be action afterwards, that comply with their own privacy policies. For example, there's an app called DocResponse. You cannot register as a patient unless you agree to the sharing of third party information with non-medical providers.

Van McGuire:

ProVia healthcare uses this app and a patient cannot register or be seen by the doctor, and this is just not a consent to treat, but it's sending information to third party such as CRISPR. There is no opt doubt. So there's a number of these healthcare apps that are coming and the doctor's offices are using them. And I think it violates our privacy. Also, another issue is with core logic, which is first American and sharing of private information that is not personally identifying information. And it's not just real estate information that our information is being shared with. It's just our personal information, including loans and loan amounts and financial information. Currently core logic has no privacy opt-out policies. And I just wanted to bring this to the FTCs attention. Those are two points, which I'm very concerned about.

Lindsay Kryzak:

Thank you, Van. Our next speaker is Nicole Smith Holt. Nicole?

Nicole Smith:

Thank you. So my name is Nicole Smith Holt and I am from Richfield, Minnesota. I am the ambassador for T1 International and a number of the Minnesota [inaudible] chapter. I'm here today because of the price fixing and collusion of the three insulin manufacturers, Eli Lilly, Novo Nordisk and Sanofi. I'm asking you to oppose the price fixing practice by these three companies. This practice by them has direct resulted in the death of my 26 year olds on Alex Smith and many others. I've been fighting since Alex's death in 2017 to make insulin more affordable, organizing other families who have also lost loved ones to rationing, participating in vigils and demonstrations outside of Eli Lilly and Sanofi, as well as testifying at the state and federal level for legislation that will end this pricing crisis.

Nicole Smith:

We're fighting for the lives of those who require insulin to stay alive, and we need your help. Every day, diabetics are risking life and limb because they're experiencing difficulties purchasing their life sustaining medication, a product that has been in existence for more than a hundred years and a product that has

increased in price by more than 1200% over the past 20 years, I asked that you make insulin a priority issue on the competition console. Thank you.

Lindsay Kryzak:

Thank you, Nicole. Our next speaker is John Verde. John?

John Verde:

Thank you so much. My name is John Verde and I am with the future of privacy forum, a think tank here in Washington, D.C. Thank you for the opportunity to speak at this open meeting. I am here today to comment on one very specific topic, which is comprehensive baseline, federal privacy legislation. I appreciate the commission's use of its six B authority to do fact finding that's an incredibly important process. And the commission has a track record of pursuing the underlying factual basis regarding business practices and technology practices and the use of technology by entities and individuals that impact data and privacy. I also understand that some at the commission have talked about employing existing rulemaking authority to pursue some of the commission's goals. And I know that some outside the commission have urged the commission to do so, fact finding and rule making are no doubt, important endeavors.

John Verde:

However, there is emerging and I think growing consensus that what is needed to provide strong consumer protections and clarity for industry in the United States is a comprehensive baseline federal privacy law. Privacy is a bipartisan issue on Capitol hill. It's a bipartisan issue at the federal trade commission, and it is a bipartisan issue in state legislatures across the country. And I urge the commission to work with your colleagues on Capitol hill to craft a wise and impactful federal privacy law that gives the commission new powers and new authority to investigate and enforce strong protections for consumers. Thank you.

Lindsay Kryzak:

Thank you, John. Our next speaker is Allison Hart, Allison?

Allison Hart:

Excuse me. Thank you, madam chair and members of the commission. My name is Alison Hart. I'm based in Portland, Oregon, and I'm an advocacy manager with T1 international. I appreciate the conversation around data and privacy here today. I am here to raise concern about another issue that will hopefully lead to future action by the FTC. My partner has had type one diabetes for 36 years in the last 10 years. He has gone to extreme lengths to afford his insulin, even with insurance and full-time employment.

Allison Hart:

Since the 1990s, the cost of insulin has increased over 1200%, despite the cost of production for a vial of most analog insulin remaining between three and $6. As you've heard today, the big three insulin manufacturers, Eli Lilly, Novo Nordisk and Sanofi dominate more than 99% of the world insulin market by value and have participated in anti-competitive practices by raising the price of insulin and lockstep, in January 2021 grassly widen reports, states insulin manufacturers lit the fuse on skyrocketing prices by matching each other's prices in price increases step for step rather than competing to lower them because of the high list price of insulin.

Allison Hart:

My partner has been in multiple situations where he cannot afford his life saving insulin, that he needs to survive from his pharmacy. Instead, he has sourced it from other countries, relied on generous donations from friends and family, and even purchased it from a stranger in a gas station parking lot. Because of the current list price of insulin. One in four patients in the United States is rationing their insulin. I'm asking the FTC to make insulin a priority issue on the competition council so that the big three manufacturers can no longer put profits over patients. Thank you.

Lindsay Kryzak:

Thank you, Allison. Our next speaker is Jennifer Janny, Jennifer?

Jennifer Janny:

Hi, thank you. My name's Jennifer Janny. I'm a type one diabetic. My son is also a type one diabetic. I was diagnosed at age 40, type one can onset at any age. I'm a volunteer advocate with T1 international and Utah insulin for all. I'm the outreach lead, people contact me a lot because they cannot access or afford their insulin. And this is due to the price fixing from Sanofi, Novo Nordisk and Eli Lilly. I'm asking you to make insulin a priority because it's essential, because it's a humane issue. And because we're in a major crisis. So please do something. Thank you.

Lindsay Kryzak:

Thank you, Jennifer. Our final speaker is Mo Tachick. Mo? You are still on mute. I don't know if you can hear us?

Mo Tachick:

Can you hear me now?

Lindsay Kryzak:

We can. Yes.

Mo Tachick:

Excellent. Let me just read my, I am Mo Tachick. I am a senior fellow at the American economic liberties project, and I wanted to make a statement about, I'm an antitrust researcher who spends my days pouring over the plumbing of a lot of different industries. I'm also a former waitress. Who's married to a chef of a restaurant that tried and failed to do business with the delivery app cartel. I run a group of restaurant owners that was recently featured in the New York [inaudible] called protect our restaurants. And we existed kind of try and get regulators to pay more attention to the various deceptive and anti competitive practices of those apps. There's been a wave of news interest in platform pay for play recently, on the back of new revelations that Amazon not only minds its data for popular products to copy, but rigs its algorithms to preference its own products while suppressing those of third party sellers, the delivery apps do the same thing to restaurants.

Mo Tachick:

Only a lot more blatantly it's a little bit over much to call what DoorDash and Uber have algorithms. It's more the direct pay for play operation. It seems like my husband signed up with DoorDash after the city passed its temporary lock capping commissions at 15%. And I don't think he got a single DoorDash order

in six months. He got maybe three from Uber Eats. And that was weird because when DoorDash was in customer wooing mode, he would often have DoorDash drivers show up at a hotel when his restaurant wasn't even open because they had tried to uploaded the menus of all these restaurants that weren't actually their partners to try and win more customers. But now that he was open for business, they suppressed his existence. And I thought maybe it was personal, but when a customer went on DoorDash or Uber eats and entered their location as his hotel or across the street from the hotel, you couldn't find his restaurant no matter how far you scrolled.

Mo Tachick:

Was it personal? Uber has a track record of going after watch dogs and whistleblowers, or it could have just been the 15% commission caps and DoorDash and Uber were trying to make a statement to say that they weren't going to do any favors for you until they got their full 30, 35%. Visiting the two platforms to try and prefer to determine who was getting promoted. I found a lot of gene restaurants and restaurant I'd never heard of before Bun More Time. Vegan Craving, FN good pizza. They were not real restaurants. Their brands owned by companies like future foods, which is owned by the founder of Uber or next by which just saves 120 million in funding from SoftBank or even Gopuff, which has raised about a billion dollars from SoftBank and 3.5 billion altogether, recently a Gopuff warehouse manager, confessed to business insider that in the midst of a supply chain meltdown that has caused ramping shortages to play against the summer camps, to hospitals, to our own restaurants.

Lindsay Kryzak:

Thank you, Mo. Appreciate it.

Mo Tachick:

That's all.

Chair Khan:

Thanks so much, Mo and thanks to all of, everybody who took the time to come share comments with us. I find this portion of our meeting extremely helpful and informative. So, this concludes the open forum in today's event. Thanks so much to my fellow commissioners for joining and to all of you. And we really look forward to seeing you at future meetings. Thanks so much.