FEDERAL TRADE COMMISSION

COMPETITION AND CONSUMER PROTECTION
IN THE 21ST CENTURY

THE FTC'S APPROACH TO CONSUMER PRIVACY

Wednesday, April 10, 2019
9:00 a.m.

FTC Headquarters
600 Pennsylvania Avenue, NW
Washington, DC

FEDERAL TRADE COMMISSION

I N D E X

WELCOME AND INTRODUCTORY REMARKS

MS. JILLSON: Good morning, and welcome back to Day 2 of the FTC's privacy hearing. My name is Elisa Jillson. I'm an attorney in the Division of Privacy and Identity Protection, and I have the distinguished role this morning of getting to provide you with administrative announcements.

So please silence all cell phones and other devices. Please be aware that if you leave the Constitution Center Building for any reason, you will have to go back through the security screening. Most of you have received a lanyard with a plastic FTC event security badge. We reuse them, so please return them on your way out.

If an emergency occurs that requires you to leave the conference center but remain in the building, please follow the instructions provided over the building's PA system. If an emergency requires evacuation, an alarm will sound. Everyone should leave the building in an orderly manner through the main 7th Street exit. After leaving the building, you'll turn down 7th street, cross E street to the FTC emergency assembly area. You will remain in that area until instructed to return to the building.

If you notice any suspicious activity,

please alert building security. Please take your seats rather than standing. Actions that interfere or attempt to interfere with this event are not permitted. Anyone engaging in such behavior will be asked to leave and anyone who refuses to leave voluntarily will be escorted from the building.

Question cards are available from staff or from the information table in the hallway. Staff will be available to collect your cards. Please raise your hand to alert them.

FTC Commissioners and staff cannot accept documents during the event. Any documents provided are not part of the official record and will not be considered as such by the Commission. This event is to be photographed, webcast and recorded. By participating, you agree that your image and anything that you say or submit may be posted indefinitely at FTC.gov, on Regulations.gov or one of the Commission's publicly available social media sites. The webcast recordings and transcripts of the hearing will be available on the FTC's website shortly after the hearing concludes.

And, finally, restrooms are located in the hallway just outside the auditorium.

We have today, I think, a very exciting

agenda. This morning, we will be talking about the role of notice and choice, and then another panel on the role of access, correction and deletion. This afternoon, we'll hearing remarks from Commissioner Rebecca Kelly Slaughter. Then panelists will discuss accountability and a two-part panel will tackle the big topic of whether the FTC's current toolkit is adequate.

With that, it's my pleasure to turn it over to Peder Magee and Ryan Mehm, who will be moderating our first panel of the day on the role of notice and choice. Thank you.

PANEL: ROLE OF NOTICE AND CHOICE

MR. MEHM: Well, good morning. My name is Ryan Mehm, and I'm joined by my co-moderator, Peder Magee. We work in the FTC's Division of Privacy and Identity Protection. This panel, as Elisa just mentioned, is focused on the privacy principles commonly referred to as notice and choice.

We're delighted to have with us this morning six panelists and experts who've spent a lot of time thinking about this issue. To our left is Jordan Crenshaw, Policy Counsel at the U.S. Chamber of Commerce; Pam Dixon, Founder and Executive Director of the World Privacy Forum; Florencia Marotta-Wurgler, Professor of Law at New York University School of Law. Neil Richards, Professor of Law at Washington University in St. Louis School of Law; Katherine Tassi, Deputy General Counsel, Privacy and Product at Snap; and Rachel Welch, Senior Vice President, Policy and External Affairs at Charter Communications.

I want to thank our panelists for participating today especially so early in the morning. I also want to thank all of you here in the room and those following online. And for those here in the room, again, as Elisa mentioned, if you have a question, please raise your hand, FTC staff will bring

around a question card for you to write your question on and someone will bring that up to us to take a look at.

So, with that, I'm going to start with some questions that are intended to lay the groundwork for our discussion this morning. The Fair Information Practice Principles, or FIPPs, have been around for decades. While all of their principles have their place, in some respects, notice and choice are often the starting point when we talk about consumer privacy.

So I want to start with a baseline question this morning. When we refer to notice and choice in the privacy context, what do we mean? Do I have a taker?

MR. CRENSHAW: I'll start off. I mean, I think, in terms of notice and choice, I think two things come to mind. The first is certainty, in that consumers and businesses have certainty about how data is used and how data is shared and how data is collected, so that there's no ambiguity in terms of what companies or what holders of data are doing.

And the second is control, putting the consumer in the driver seat with regard to how data is shared, how data is -- whether it's retained by a

company as well, too. So when you have those together, you create a balance in which companies and consumers are, in fact, able to have certainty and able to know the rules of the road as they go forward.

MR. MEHM: Great. Thanks, Jordan.

Let me ask if any other panelist wants to add something to what Jordan just said.

(No response.)

MR. MEHM: Okay. Well, let me go, then -- these two concepts, notice and choice, are often linked together, but are they different? And, Pam, do you want to take that one?

MS. DIXON: Yes, and thank you. Thank you to the FTC for inviting me here today. I really appreciate the opportunity to talk about these important issues.

You know, notice and choice has a lot of different meanings, depending on who you ask and what jurisdiction they live in. So it's a very difficult question to answer. So a lot of it depends on your jurisdiction. But speaking broadly about the US jurisdiction, notice, when I think of notice, I really think of the Privacy Act and those laws, and I really like to think of notice as something that's meaningful and robust.

In regards to choice, I don't view it as individual control, and the reason I don't view it as individual control is because, okay, so, in a paper world, when some of these terms were conceived of, in a paper world, I do think that you could apply certain mechanisms and have more control of your data. There was this lovely term "privacy by obscurity." You know, if you're dealing with a room full of paper, certainly you can have privacy by obscurity. It's really difficult to get to all that paper all the time. But when you're dealing in a digital ecosystem of some complexity, we cannot fool ourselves that we have individual control of our information.

So, for me, when I think of notice and choice, I think of a paradigm that no longer fits the reality on the ground, and I do think that that is one of the reasons that a lot of the privacy tensions have arisen today. So one of the things about notice and choice is that that system tends to push decision towards the end of the process, not toward the beginning of the process, and that's a problem.

So, for me, personally, I would rather have notice, I love notice, but I also want a seat at the table when the notices are being decided upon and written, and I really don't want to have a choice that

is a checkbox at the end of a process. And I think that's the real downside of what is often referred to as notice and choice. I do think there are alternatives that are very powerful, and we'll get to those later, I hope.

MR. MEHM: Yes, we will.

Let me ask if anyone else has an additional thought on this topic. Go ahead, Katherine.

MS. TASSI: Just one final thought for me. I think we'll probably find, as we go further in this panel, that notice and choice don't always go together. You could have notice without choice and choice without notice, and, so, just to add a little bit of nuance to the concept of choice that it doesn't always mean one thing. Choice can be control, it can mean opt-in, it can mean opt-out. You can choose between one thing and another thing, and any of these might be the right kind of choice, depending on what the context is, depending on what type of data we're talking about or what type of processing is happening.

And so the notion of choice as a flexible principle, I think, is really important and, also, that every type of choice has an actual impact on the organization that is offering the choice. Choices have engineering impact, they have operational impact,

and so allowing flexibility in what the choice is that an organization offers, depending on the type of data and the type of processing, I think, is important when thinking about memorializing the principle of choice in, for example, legislation.

MR. MEHM: Great. Thank you.

Neil?

MR. RICHARDS: So I think before we get too deep into the technicalities of notice and choice and opt-in, it's worth looking at the big picture here. I think Ryan very helpfully started us off by talking about the Fair Information Practice Principles, right, and those were designed, as Pam mentions, for a paper world or maybe a world of paper and tape.

So those computers with the big reel-to-reel spools that we see in the old photographs, that is a world, a world in which there was not very much data collection, a world in which the people who came up with the notice -- the idea of the FIPPs -- you know, I'm thinking about like Alan Westin and Privacy and Freedom in the late '60s, or Willis Ware, who chaired the report of the Department of Health, Education and Welfare in 1973, which gave birth to the FIPPs. We're trying to manage a real fear of a world in which everything people do is tracked and collected and

monitored and in which people have really very little knowledge of what is going on and very little ability to affect the way information about them is collected, used, disclosed, stored, breached, and otherwise processed.

Notice and choice have been a distillation, a boiling down, I would say a weakening of those principles. So we have the situation that we have today. If you asked Willis Ware, if you asked young Alan Westin, what the FIPPs would have done, I think the FIPPs, for the purpose of forestalling that world the people of the late '60s and '70s feared desperately, the FIPPs have been a spectacular failure and notice and choice have been a spectacular failure, which is not to say that notice and choice have no place in a consumer protection regime for the 21st century.

But I think it is important to look at the evolution of these principles and to look at what they were trying to do and how they failed to do that if we want to look broadly and critically and intellectually honestly at the series of really complicated and nuanced and difficult issues of competition and consumer protection we face today.

MR. MEHM: Florencia?

MS. MAROTTA-WURGLER: A quick followup to Neil's point. In addition to that, there is the added complexity of the information going through several layers and several parties, through a particular chain. So when we think about notice and choice, we also need to think about, to the extent that we might think that the model is somewhat feasible in some respects, and we can talk about that later, and the need, as Katherine said, for some type of flexibility, which might be necessary in some cases.

So notice and choice might be only operable within a particular domain, when you have a consumer or a user facing a particular firm. The issue that arises is that even when we talk about the internet of things, when we talk about subsequent transfers of data, is that it becomes increasingly complex and almost impossible to extend the model to the current ecosystem in which information transfers and it's used about us. That doesn't mean that we don't need or that the market doesn't need the type of flexibility that notice and choice affords.

So it's a complex question. It would be a lot easier to say, well, you know what, clearly it's not working, let's scrap it, but it has some important benefit. So the question is how do we distill those

benefits? Well, taking into account the particular problems that arise from, first of all, the structure in which tons of information about us gets gathered and in ways that are impossible to track and notify consumers, but also if we think about consumer's limitations and really we think in a more wholesale manner the relative effectiveness of disclosure regimes in every single context that you want to think of in the area of consumer protection.

MR. MEHM: All right, thanks.

Pam, I know you wanted to add a thought.

MS. DIXON: Yes, I so appreciate both of your comments. There has been -- you know, FIPPs, Willis Ware, for anyone who has not read the HEW report, Willis Ware could see around corners, he had just an extraordinary mind, and it's worth reading that original report. But one of the authors of the report, who is deeply involved in it, is still alive, and her opinion is that people deeply misinterpreted the FIPPs. And the authors of the HEW report intentionally threw individual control under the bus.

FIPPs was never meant to be a regime of, for example, notice and control. That's not what it was about. So I do think, to Neil's point, there's been some rather profound misinterpretation of FIPPs, and

we have to understand that it's not a regime that you're supposed to be using for controlling data. They understood, even back then, that controlling data at an individual level was a fool's errand and would not be feasible going forward into the future.

MR. MEHM: Rachel?

MR. WELCH: Well, we maybe come at this with a slightly different approach coming from a company's perspective, and we actually believe that notice and consent and choice are actually important parts of the process, and that they are deeply interrelated, that consumers need to have transparency about what companies are doing, about what their interactions are with the company that they are contracting with or engaging with online.

And from our perspective, we see that there's growing consensus that there's a need for a federal framework, that we've tried to do this through self-regulatory principles, we've tried to do this through kind of trial and error, and it seems as though across the ecosystem there is a growing consensus and across civil society and regulators there's a growing consensus that we need to reduce this to paper and have there be strong guidelines that people follow in terms of how they interact with their

consumers. And a little bit I feel like some of the conversation about we're maybe in a post-notice and consent world is giving up before we tried.

So Charter's put forward five principles that we think should undergird any US privacy framework and those include transparency and choice. For us, we actually think that having more stringent rules about an opt-in consent, where the consumers all start with kind of blank slate, they get to start with zero and engage with the company and decide do I trust you, do I have confidence in this process, do I want to engage with you to take this service and to trust you with my information?

And so we think an opt-in approach really gives consumers a lot of control over how they engage with the companies and it's a good starting place. There may be opportunities where you need some limited exceptions, but we think having broad and ambiguous exceptions actually undermines that confidence that we're hoping to see encouraged through a US privacy law.

And I think we've seen, with Europe, with other countries, with California engaging in this, that there's a real desire to have some kind of clear rules of the road. They may not be perfect, the world

is complex, but it doesn't mean we throw up our hands and give up before we try.

MR. MEHM: So I have a followup question. We've heard a lot already this morning about this idea of choice and very different viewpoints about whether it's working and control, you know, offering different choices to consumers. So when we talk about choice, what do we mean? So should consumers get to choose whether to allow collection of their data at all, or do we really mean that consumers should only have a choice regarding how a collector uses that data once it's collected?

And I realize, you know, things are very context-dependent, and we've heard about that different situations may merit different answers, but I'm wondering if anyone has a thought about this.

Pam?

MS. DIXON: Yes. Thank you so much.

So there are many different solutions that exist to cope with many different problems. I don't think we should have one silver bullet that we think of for, you know, looking at privacy issues. This includes, you know, one federal bill. It's not going to solve everything. It can't because of the complexity of the data ecosystems which overlap with

tremendous, tremendous complexity.

So if you really go to a basic layer of understanding how the regulatory process works, you really have three models to choose from. You can look at a centralized structure, such as command and control legislation. That's what I think a lot of people were talking about yesterday with GDPR and CCPA. Those are centralized structures.

People also talked yesterday about privatization, paying for data, and, you know, data is property. That's a different model. And then there is a third way that I really didn't hear anyone talk about yesterday, which is self-governance. So the Nobel Laureate Elinor Ostrom spent 40 years of her life doing empirical research on self-governing ecosystems that were enormously complex and figuring out what allowed them to thrive by being self-organized, and she came up with eight principles.

And those principles -- I wrote a paper -- I presented it at Harvard's Kennedy School -- on digital identity ecosystem and I laid out how the Ostrom principles work in complex ecosystems. There's a role for command and control. Should we have breach notification? Yes, thou shalt, right?

There's a role for privatization. When

extreme victims of domestic violence need a social security number change, they have the ability to do so with their data. But in enormously complex ecosystems, data brokers are one such ecosystem, identity ecosystems are one such type of ecosystem, there is often a need for something that is more granular, that allows a closer fit to these very distinct and difficult models.

So, today, we actually released a discussion draft. It's called the Consumer Privacy and Data Security Standards Act of 2019, and it discusses how to do voluntary consensus standards but with due process. And this is already actually written into law in the US, and the FDA has been using this for medical devices for at least 20 years. So we know it works for very complex issues. And I think that that's a way forward that would be very powerful and work.

MR. MEHM: Okay, let me ask if anyone has something that they want to add.

(No response.)

MR. MEHM: Okay. Let me move on to another question for our panelists. Are there some practices for which only notice is needed and no choice?

MS. DIXON: I have a comment.

MR. MEHM: Pam?

MS. DIXON: Please someone -- you've got to step in and save me.

MS. WELCH: Do you want to go first, Pam?

MS. DIXON: I have a quick comment. I think that there is room -- because of the complexity of data, I do think there are some uncontested uses of data, for example, fraud analysis. I think we can agree that that is an uncontested use. Can there be potentially an agreement made perhaps through these standards, processes, with due process, openness and transparency, can there be a general agreement amongst all the stakeholders that have an interest in the data that some uses can be routine and can be allowable without consent, such as fraud, et cetera, et cetera, decided upon by the stakeholders? And then anything -- and they decide the boundaries of what exists outside of that.

Something that is more meaningful would need, for example, meaningful consent. But I think the stakeholders who are a party to that should have a say in that, not a checkbox, but a seat at the table.

MR. MEHM: Florencia?

MS. MAROTTA-WURGLER: Yeah, just a quick

point to add to that. So here context and expectations matter a lot and understanding what consumers expect and know might be something that we need to do more research on. I mean, hopefully, whatever comes out of this will be based on a systematic analysis of the market and what consumers want and what they expect because, many times, just like when we go to a supermarket and we expect certain things, over time, we become relatively savvy or sometimes relatively not savvy.

So the extent to which there are data collection and use are consistent with the expectations and the needs of the business, there seems to be very little need to require a choice. Also, when we think about how consumers get tired of making decisions on a constant basis -- remember the one week where we all had to close the GDPR pop-ups? It just becomes meaningless.

So one thing to keep in mind is how the entire -- how whenever we think about a system, whenever it gets adopted, how it will look on a systematic way. Are we going to be bombarded in choices in a way that makes innovation difficult and decision-making difficult? So it would be important to distill those types of decisions that might need

some either additional education or information to correct misperceptions, and also those that are outside of the scope of context of which consumers expect to share information.

So when you give your credit card information to process something, you expect that this information will be shared with a third-party payment processor. You might not expect that then the information will be sold to a post-transaction market or something like that. So we need to think about context, but also how this affects not only consumer decision-making in general and the meaning -- how meaningful that is, but also how it affects the experience that we have and the ability of these highly innovative markets to continue to evolve in a way that is respectful of consumers' expectations.

MR. CRENSHAW: And I will echo that as well, too, in terms of there are some contexts in which notice and choice are not necessary. And I think when you're looking at consumer expectations, as has been said before, in the context of the transaction that you're making with the consumer as a business, for example, clearly mapping software requires the use of geolocation data, for example.

So that's an example of clearly inherently

you have to use data to provide the service that you're giving to your customer. Other examples are public policy examples as well, too. Anti-money laundering, prevention of shoplifting, for example, security, trying to use data to prevent malicious activity and comply with other legal obligations. So there is a space in which some data should not be subject to notice and choice given the fact that it's neither necessary for the transaction or there are public policy reasons behind it.

MR. RICHARDS: I think it's really important when we talk about notice and choice, though, to be specific about what we mean. The question that Ryan originally asked was whether there are situations where notice but not choice -- was it notice without choice or choice without notice or both you're interested in?

MR. MEHM: Notice only.

MR. RICHARDS: It was notice only, right, in which there is notice but no meaningful choice or no choice. You could describe the entire internet ecosystem in the United States up to this point as falling under that model, particularly surveillance-based advertising, particularly, you know, a lot of activity of data brokers. What has practically

happened is there has been notice and it's often been fictive notice or, sorry, constructive notice that is buried in either the privacy policies that are either too vague to tell consumers anything or too specific for the average consumer to be able to rationally comprehend.

And in any event, as Florencia points out, the sheer scale and scope of the numbers of such notices are more than a privacy expert or a privacy council can comprehend in the aggregate acting as a consumer, much less our average consumer for whom we want to target these laws.

So I think it's important to, rather than sort of -- we need to be critical about our use of the terms "notice" and "choice" because, very often, we talk about them as if notice is meaning and consent is real, rather than notice being constructive and consent being fictional. And the model with which we construct these rules has to take into account, as Florencia points out very eloquently, the actual context in which they're deployed and the bounded rationality of all consumers.

MS. WELCH: And I would just add that I think that there are -- maybe we come at it from a slightly different perspective that, while we agree

that there should be some limited exceptions to consent, that when people talk about context, I'm not sure I really know what it means.

So when Jordan was talking about some of the enumerated exceptions, so interacting with legal process, you know, preventing fraud, potentially improving your service, rendering the actual service that the consumer has requested, whether it's the sale of a product or the purchase of broadband service, but when you get into trying to add ambiguous concepts like context that maybe the consumer doesn't understand, the business may be substituting its judgment for the consumer's judgment, and that that can result in consumer confusion, it can reduce trust, and we worry that the exception can swallow the rule.

We might prefer an approach like the GDPR approach where they have legal bases for processing, but those are limited and bounded. And then I think that helps to educate the consumer to ensure that their notice is more than constructive and that their choice is more than fictional and that that is what companies are looking to do because, at the end of the day, we're hoping that we can sell services, that consumers will come back to us again and again and trust us, that we're going to treat their relationship

with us with respect, that their data is going to be treated with respect by us, but if we create a system where there are broad exceptions to the concept of choice, I think that that leaves them feeling limited in their ability to direct how their data is used and how they engage with businesses.

MR. RICHARDS: The problem -- and I respect about, I think, the importance of trust is really essential to this whole process, which I think we're going to talk about later and I don't want to foreshadow. I do think, though, the difficulty is that consent of that sort, sort of what we might call gold standard consent, informed consent, does not scale.

We can only make a certain -- as human beings in our minds, we can only make a certain number of rational, conscious, thoughtful choices in a given day, and the sheer number, the scale and scope and technical and legal complexity of these sorts of agreements, even with the very best intentions of lawyers and engineers and, you know, improvements of interfaces and privacy dashboards is just far too much for the average consumer to comprehend.

MS. MAROTTA-WURGLER: Just to add a --

MS. DIXON: Can I jump in? So I want to

respond to Rachel's concerns, and I think your concerns are legitimate and we have to take those concerns into account.

So, in thinking about those concerns, I think that one of the things that we have to understand -- and I agree with you, Rachel, in regards to broad exemptions -- I think it is very, very dangerous to create standards from rhetoric or from metaphor either. Either one is very dangerous. History teaches us this over and over again.

We need to have data-driven decisions. In order to get data-driven decisions, I do really support a voluntary consensus standards process that allows for granularity. So, for example, for your business model, you could hold a stakeholder process that could articulate the consumer concerns at the table so that they help articulate what they make choices about in the first place.

So it moves the decision-making into a place where not only are consumers having genuine decision-making ability, they have a seat at the table and they can assist in outlining what their concerns are at the very beginning of the process. And I think this is very powerful and very meaningful when it's done with due process, with fairness involved.

But I think that waiting until the end of the process and giving consumers a whole bunch of checkboxes is not powerful, and I think we need to get away from that model. And to the points that Florencia has been making, I think it's very important to understand that it is not possible, at this point in data complexity, to have one model that just fits absolutely everything. We need a multiplicity of solutions to attach to a variety of problems and challenges in privacy.

MR. MEHM: Okay.

MS. MAROTTA-WURGLER: Just a quick followup to Neil and Pam. So I agree that data-driven decision-making is important and I also agree that notice, that consent on this point, real, actual consent is, for the most part, a fiction. So I have some data on that.

So I have been working on whether consumers read contracts, and you know, it sort of turns out that about -- you know, when you look at consumers in real settings, it's only about 1 in 1,000 that access these very saliently-described or displayed contracts that you have to click on "I agree." Not that many actually bother to figure out what it is that they click on. Maybe there's more hope in simplified

notices. But it's also true and research also shows that consumers systematically misperceive and misunderstand certain things, not everything.

That's why more research and understanding -- and Rachel is right that, you know, context is such a malleable thing and you can have an exception swallowing the rule. But that doesn't mean we can't find out what those are. We do it in other concepts, in deceptive advertising or in trademark confusion. So why not have more of a data-driven approach here?

And, also, these privacy notices have been growing and growing and growing exponentially over the years and they require a graduate degree to understand.

MR. MEHM: Katherine, last word, and then we're going to segue to Peder who has questions about pros and cons of the existing models.

MS. TASSI: Okay. I was just going to say that I don't think notice and choice don't operate effectively. I think -- so at Snap, we use a couple of different models --

MR. RICHARDS: I'm sorry, did you say you don't think they don't or you don't think they do?

MS. TASSI: Yes. I don't think that notice and choice don't operate effectively. I think they do

in certain contexts. Sorry. Three negatives.

(Laughter.)

MS. TASSI: At Snap, we use about three different models to be able to provide effective privacy protections to our consumers, and we think that notice and choice operate effectively as privacy protections in certain circumstances that include, for example, when the product or feature that we're providing notice and choice about is not complicated, that we're able to provide just-in-time notice and choice, usually within the context of providing the product or feature to the individual right at that moment, when the product or feature isn't collecting very much data or isn't using very much data, that it's not sensitive data, when the choice can be presented simply and exercised simply right there and then in the moment, when the choice is meaningful to the individual in that moment, and when the Snapchatter isn't given so many choices that's it's confusing and rendered meaningless.

We combine notice and choice with privacy by design. We build privacy into the design of our products and features. And this is really critical to balancing with notice and choice as a privacy protection because there are many types of privacy and

data processing that you want to take out of the hands of consumers and just build the privacy protection into the design of the product, things that you shouldn't burden the consumer with having to make choices about.

So, for example, we build specific data retention periods into all the data that we collect and process. That's not a decision that we leave to our individuals, even though we give them choices to simply delete the data even sooner than when we might delete it. So we think the combination of building privacy into the design of products and features, balanced with sensible decisions about choices about products and features that the individuals are using in the moment, is the right balance.

In addition, we have found it really, really useful to do legitimate interest assessments related to other data processing in the GDPR context, and that kind of speaks to giving notice and no choice. When you do that balancing assessment, it requires you to think about the privacy interests of the individuals. And if you land on legitimate interest as your lawful basis for processing, you can really only do that if your business interest outweighs the privacy interest of the individual, and that balancing can only come

down in your favor if you've given enough privacy protections to the individual. So we found that to be kind of a third way of giving privacy protection to individuals. So the three combined, I think, can provide adequate privacy protection.

MR. MEHM: Great, thanks, Katherine.

Peder now has a question for the panel.

MR. MAGEE: Sure. I'm going to actually follow up with something with Rachel. You mentioned that Charter is supporting federal privacy legislation with an opt-in approach, and I'm just wondering why opt-in is preferable to an opt-out approach, from your perspective.

MS. WELCH: Thank you. So from our perspective, and as I said earlier, we believe that an opt-in approach really helps engage the consumer. And I understand that there is some research, but I think there's research on both sides, that consumers -- they have said in surveys that they want to engage, that they want information. At the same time, the consumer then maybe doesn't take the information.

But if every consumer is starting from the same place, that nothing is being collected from them, nothing is being processed from them, then they have the opportunity to really engage and make a decision,

and we think it should be meaningful. I don't know what the silver bullet is in terms of meaningful, but we certainly would say no pre-ticked boxes. It has to be renewed with reasonable frequency. It needs to be renewed when there's a new practice that it wasn't first provided by the company for.

So we think that they are -- you know, at the same time that technology creates complexity, it also creates new tools to engage with the consumer. So as Katherine said, you know, pop-ups in the process of engaging with the service or the product. There can be "just-in-time" notice.

But we also see with the privacy policy -- and I'm not going to be the one who sits here and defends it as the perfect answer, but it certainly forces a company to sit down, take an inventory of what we're doing, think about it. It requires us to do a gut check about does this make sense? If this were printed on the front page of the "New York Times," would we be proud of this practice?

It also enables academics to look at the privacy policy to say this makes no sense or this looks misleading and to call us to account for that. It also enables regulators to look carefully at it and make sure that we're acting in compliance with that.

And I think what we've seen with the various breaches and misuses and mishandling of data over the last year to 18 months is there's been a new ability to educate the consumer, to help them understand.

So we really believe in the consumer, that they are intelligent, that they understand what their preferences are, and that consumers really differ in their preferences. So if you have an opt-in, they have an ability to determine my preference today, because I woke up on the wrong side of the bed, is I don't want to share anything with anyone. Tomorrow, I may change my mind. Whereas with an opt-out, then the burden is on the consumer. They have to go and figure out what is Snap's process, what is Charter's process, how do I opt out, where do I go to do it, whereas an opt-in is brought to them and they get to make a choice on the front end.

MR. MAGEE: Well, just to play the devil's advocate and then I'll open it up to the rest to weigh in, but you said that in opt-out, you're putting a big burden on the consumer, but in a purely opt-in world, isn't there also a pretty heavy burden on the consumer to make choice after choice and possibly just, you know, throw their hands up in frustration and opt-in to everything just as a default?

MS. WELCH: Well, I think that's always the balance, right? It's the balance for us in creating our privacy policies, how do you make it simple and clear enough, at the same time balancing the need for comprehensive disclosures. And with regard to a consent model, it's the same thing.

We're always looking for the Goldilocks and we certainly are open to the ideas of enumerated exceptions. There may be ways to enumerate prohibited practices as well, but we think we should start from kind of a core set of -- there's a vast middle where we think the consumer should be engaging and that there's ways that we can do this so that it doesn't result in fatigue and it really helps the consumer to engage.

MR. MAGEE: Anyone want to weigh in on this?

MR. RICHARDS: Yeah, I do, Peder. So I think --

MR. MAGEE: Neil looked like you were going to say something.

MR. RICHARDS: I would absolutely agree with you, Rachel, about the virtues of long-form privacy policy. I know Mike Hintze is going to speak about this, I think, in the next panel. Long-form privacy policies do have those virtues, but they do not inform

the consumer. If our goal is to inform consumers to enhance choice, to enhance meaningful consent, long-form privacy policies have their virtues, but those are not the virtues that they have.

I am sympathetic to the idea of empowering consumers and empowering the use of technology. I think the context, though, unfortunately, does matter. So I, for example, am a customer of both Charter and Snap. If I'm using Snapchat, I think in those contexts, good privacy engineering and good cues might help me not share the image I want to share with the wrong person. I think that is good engineering and that is an empowering choice, and it helps because I'm thinking about it.

But, ultimately, I don't really want to engage with my cable company. I don't want to engage with my search engine and with my first social network or my second social network or my third social network. I don't want to engage with the equipment manufacturer of my smartphone and the service provider of my smartphone who may be different from my cable company. The problem is that kind of engagement on data processing practices just does not scale.

Woody Hartzog at Northeast University and I have an article which we're about to publish in the

Washington University Law Review called the "Pathologies of Consent." And we catalog many of the problems with consent models in American law, particularly in the digital services context. But we conclude not that consent, not that opt-in choice, not that empowered consumers are a bad thing, but that they don't scale and that they're limited.

I think three principles need to happen for that kind of consent, that kind of choice to be effective. First, choice has to be infrequent. We cannot have that kind of engagement with all of the various companies we have relationships with any more than we can memorize all of the passwords we have with all of those companies, a separate but related problem with similar implications for the limits of consumer cognition.

Second, the consequences must be clear. If I send a picture I meant to send to my wife on Snapchat to my daughter on Snapchat or they're not my friends, but to my students on Snapchat, the consequences of that choice would be clear, but the consequences of opt-in processing to target online behavioral advertising, to provide more relevant goods and services, don't you want that, just does not work for consumers. The consequences there are not clear,

the legal terms are not clear, the technologies are not clear, and the risks are not clear.

And third, choice has to be meaningful. There have to be meaningful alternatives to the data practices, and take it or leave it, you know, accept all of our terms or don't use Amazon or don't use whatever service it is simply cannot work. So choices have to be infrequent, the consequences have to be clear, and choices have to be meaningful. There have to be real alternatives.

MS. DIXON: Just to jump in. Thank you.

There's a couple of thoughts I have. The first -- I wanted to respond to Rachel or to the comments. One issue that came up in discussion here was the issue of data mapping, how privacy notices afford a company the opportunity to map their data. We've seen in Sarbanes-Oxley and even in improving compliance technically under GDPR how useful data mapping can be for a company. It's also useful for any kind of process in discussing options directly with consumers.

And for me, you know, when we put a credit card to a vendor to make a payment, there is a standard that controls how that happens. When data is deidentified under HIPAA, there's a standard that

controls how that's happened. There are certain instances -- in fact, many instances -- in privacy, in the interface between consumers and their data and companies where there are tough privacy problems that edge on all of these consent issues, which are known and well-understood issues at this point.

So why not ask the consumers in a formal, open, transparent, voluntary process that includes principles that comport with due process? Why not ask them what they think and help establish the standards with all the stakeholders at the table? And then consent is contextualized for that specific business model and/or business and/or sector, depending on what the problem is to be addressed. I think we have to be careful.

Again, I'm just going to go back to the models. We've got a centralized model, we've got a privatized model, and then we've got more of a self-governance model, and these are three different tools that we can use in overlap and in varying situations for really tough problems where there's going to be an overreliance on consent. Ask the consumers, have a multi-stakeholder process that's more formal, and figure out the answers. It will take more time, but it can be more useful than ending up with huge volumes

of decisioning at the end of the process that consumers may find either not meaningful or overly burdensome.

MR. MAGEE: Florencia?

MS. MAROTTA-WURGLER: One additional thought to build up on what's been said is that we might want to distinguish between what consumers say and surveys or when they're asked, we usually present to ourselves the best versions of ourselves, like I should do this and I should do that, and then when we act, we act quite differently, hence this privacy paradox, right? Everybody says they care, but they act as if they don't, at least in some contexts.

So to the extent that we want to understand this better and to the extent that we want to offer only infrequent, simple choices -- some choices are just not simple at all; sometimes consumers don't want to make choices or sometimes they don't want to make them wholescale -- is to also observe, given that we can add a little bit, is the extent to which there is inconsistencies between beliefs and actual practices because this is doable. This is not something that is not not feasible. And in that way, inform the particular recommendations that Rachel and Katherine were talking about.

MR. MAGEE: Great.

Jordan, I want to get you in on the conversation a little bit more.

Could you talk about how notice and choice would operate in the chamber supporting a privacy bill right now?

MR. CRENSHAW: Yeah, sure thing. Earlier last year, the US Chamber of Commerce really saw that the writing was on the wall that a state patchwork was emerging, starting with California and now with Washington State. As I talked about certainty and control earlier today, one of the things that we wanted to make sure was there was certainty with regard to regulation with regard to data.

You know, for example, you know, I think it's going to actually dilute notice if you begin to get notices from different states on your rights under that current regime under a different state approach. I mean, if I end up seeing those exceptions or those extra state notice requirements, I'm more than likely to probably ignore those with notice fatigue.

But what we did was we brought together over 200 companies from all different sectors, all different sizes to try to come up with consensus privacy legislation, and we actually came out with

text on this topic. Basically, what our bill is it is a notice and choice bill. First of all, it takes into account that there are brick-and-mortar businesses out there, it takes into account that there are online businesses out there, and context is definitely important as we created these principles that we developed and also the model legislation that we put forward.

First of all, our bill would require companies to essentially post a privacy policy that is clear and conspicuous, those that are covered by our Act. The second would be that if, you know, you don't find that necessarily to be adequate as a consumer, you can go to the company and the company is then required to inform the consumer about how the data about them is collected, how it's used and how it's shared, and the business purpose for the use of that data.

And, thirdly, our data requests that a consumer could do for a company, the company would then also have to say the type of entities that they're sharing that data with. So that way the consumer is on notice to begin exercising control rights under the Act. So the second piece is control.

The first control element we give is a right

to opt out of data sharing. Now, California, for example, actually has a right to opt out of the sale of data. The definition out there is a little bit squishy in terms of what that means. We felt that it was easier and gave more clarity and certainty to say that this was a sharing bill with regard to opt-out rights.

And then, if that's not enough, what we did is we also gave consumers control and the ability to have data about them be deleted by companies. And we wanted to make sure that, if you are concerned about the use of data, if you can direct a company to delete that data, that begins to take care of that issue as well, too.

MR. MAGEE: Great. So -- but if I'm understanding you correctly, there's no opt-out right to prevent the first party from collecting your data in the first instance. You would actually have to reach out to that company and say delete it.

MR. CRENSHAW: You would either have to say delete or you could opt out of the sharing of that data with third parties.

MR. MAGEE: The sharing, but not the collection by a first party.

MR. CRENSHAW: Not the collection itself,

no.

MR. MAGEE: Okay. I mean, again, we seem to keep coming back to different iterations of this burden on the consumer, you know. In the pure opt-in regime, the consumer is faced with choice after choice. In something like that, the consumer then has to actively find out what companies have collected information about them and seek to have that deleted.

MR. CRENSHAW: No, I agree that a lot of these different approaches are going to have to put some burden on consumers to act if they so choose to exercise privacy rights. But, at the same time, we do have to recognize that there is a balance out there with regard to the use of data and that consumers benefit greatly from the use of data as well, too.

So, you know, I think as Rachel mentioned, too, you know, we have to find that Goldilocks, that sweet spot in terms of what is the right balance in terms of opt-out and also data deletion and other uses. But at the same time, we have to remember, too, that consumers are benefitting greatly from the use of data, whether it be from potential new safety and things like autonomous vehicles to whether or not we're able to expand lines of credit to people who were marginalized before and using new data points.

So I think we do need to make sure that we also are looking at the benefits of the uses of data in light of, also, the regulations and the burden that may be on consumers to exercise their privacy right.

MR. MAGEE: Yeah, and I didn't want to downplay that there are tremendous benefits to consumers from services they receive based on data collection. I'm sorry.

Pam?

MR. DIXON: Yes. Thank you.

Well, Jordan, I agree with you. I do think there are tremendous benefits to data use, and we need to preserve data uses because -- and you mentioned autonomous vehicles. So I just finished a lengthy process with the OECD. The OECD has approved the first soft law global, truly consensus, guidelines on artificial intelligence. And something that was very apparent during the expert discussions of these guidelines is that machine learning absolutely, which is a part of AI, absolutely changes the ball game in regards to privacy.

You know, when we shop at a retail outlet of whatever sort and we use either a credit or a debit card, I think all of us in this room and perhaps watching understand that that information is

extraordinarily useful and valuable. There's a gentleman in California that does a profound number of lawsuits under the Beverly Song Act, and that is when a retailer collects zip code, which is not allowable in California because it creates so much robust data about an individual.

But something that no one has talked about yet is knowledge creation. So if you look at machine learning and all the data that goes into it, yes, maybe our credit card or retail purchase history is input into a data model, a machine-learning model, but what gets output is new information. It's created knowledge. And that is not something you get to opt out of or take back or withdraw consent for. It's new.

So that information is relevant to the consumer to whom it refers. They have a stake in that information. But so does the company that went through that machine-learning process to create it. That is a common resource. No one gets to own it. It is a common pool resource. It's shared. What on earth do you do with that? That is why we've proposed a voluntary consensus standards process to deal with some of these very, very difficult problems where there are not easy answers.

I think that sometimes you can have a simple model. But especially when AI gets involved, the models and the new knowledge, it is very difficult to articulate a single frame of reference or a philosophical basis for understanding how to do privacy at that level.

Now, in the GDPR, essentially, AI is deeply diminished, right? And that becomes a deep question about, okay, what are you going to do about the countries that don't have a diminished capacity for doing AI? What do you do with that? What kind of outcomes do we want to see? These are serious questions, and there are not easy, simplistic answers here.

MR. RICHARDS: And I would say that one of the easiest, simplistic answers, unfortunately, at the risk of disagreeing with Jordan, is the Chambers bill. I understand -- I guess we're talking about Goldilocks and bowls of porridge where they're too hot or too cold. As I understand it, clear and conspicuous privacy policies, duty to inform, disclosure of data sharing practices, opt out of data sharing, but not collection and control over deletion is a bowl of porridge that is so cold it is stale.

I think the reason we got into this mess, I

think the Chambers bill doubles down on the spectacular failure of the FIPPs, which has led to this hearing, which has led to hearings in the House, which has led to hearings at the Senate. It's led to Cambridge Analytica, it's led to data breaches. This is just insufficient and we need to have a better way than really doubling down on the existing pathologies of notice and choice.

MS. MAROTTA-WURGLERY: Just to add some hard data to that, so a systematic analysis of privacy policies that I've conducted over time, first measured from the beginning of -- from 2009, taking weekly snapshots of privacy policies until 2014, and then finally now in 2018, what you can see is that privacy policies have grown from about an average of 1,300 words to almost 3,000, and they just continue to grow. So there is more detail.

The 2012 FTC guidelines recommending layered or short notices have not been taken up. Actually, there's a really interesting recent study that also measures the extent to which the plain and simple directive of GDPR has been followed and the author has found that it hasn't at all. And, in fact, when you look at readability scores, both in US and the EU, it requires about 15 years of education and the reading

level -- basically the type of reading level that you see is a type of article that you would read, not a law review article that has a million footnotes, but an article in a scientific journal.

So that makes it -- it's great for -- it's a great way of showing commitment by a firm. It's a great way for regulators and others to hold companies accountable, I mean, assuming that damages problems can be fixed. Many cases just get thrown out. It's great for me because I study them and I've been studying them for years. But they are not the way to interact with consumers and that's why this idea of maybe short, just-in-time notices, ways of meaningful, not that many choices when it matters.

And this idea -- again, the collection of information and what we do with it and what firms do with it is extremely valuable. A lot of people and the GDPR regulators are extremely -- or EU regulators adopting GDPR are extremely concerned by what it's going to do to innovation. This is not a law without costs.

This is something that we need to keep in mind because consumers benefit greatly from this. But also they can get hurt in many different ways and in ways they cannot track. So choice, when you can't

understand, as Neil said earlier, you can't understand the consequences of that choice, it becomes very difficult.

So amping up privacy policies, which is basically the weakest point of notice and choice, seems to me a misdirection and more than anything a missed opportunity.

MR. CRENSHAW: I would just like to respond to Neil's comment --

MR. MAGEE: Sure.

MR. CRENSHAW: about the Chamber bill. You know, we're talking about porridge. I mean, I think that this is a first crack of the business community looking at this issue. I mean, we've gone from an era of self-regulation to an era of really calling for meaningful privacy protections. I mean, if you view it as cold in terms of porridge, it's better than no porridge at all not to feed anyone.

I mean, what I would say is that this is a step that we're taking and I think that we are continuing in the business community to look at other options and other ways to address consumer privacy. But at the same time, too, we have to look at the tools that the FTC has in terms of what it actually statutorily has been able to do.

When we're talking about things like Cambridge Analytica, we're working in a world we only have unfair and deceptive trade practices, in which for privacy enforcement in this country really requires that a company not live up to their privacy practices. At least our proposal does begin to get teeth in actual definite consumer rights to individuals and consumers. But, once again, we're willing to work with others to go along the way to try to look at other options as well, too, that work for businesses and consumers.

MR. RICHARDS: I think the reason we have this problem is that entities like the Chamber of Commerce have opposed meaningful privacy legislation for 20 years. And serving up a stale version of these practices now is just woefully insufficient to respond to the complexity and the importance of the problem. This is the hearing on the future, not the past, so I won't say anymore on that.

MS. DIXON: So there's a very interesting issue that I want to bring up, which is the issue of data brokers. You know, the FTC did a 6(b) study on data brokers. What that study revealed was not surprising. I've studied data brokers for 20, 25 years now. Something that's become very apparent to

me, I was looking at business models of data brokers. So when I first started looking at data brokers, there was about a dozen or so major business models. But, now, there's about 50 or so business models. You know, that's really complicated.

I think if we're going to look at a problem, if you want a really hard problem in privacy, a really actually sexy problem in privacy, it's data brokers. If we can figure out how to address what you do for consumers who do not have a relationship with a company, but the company has their personal data, if we can solve that problem then we can solve a lot of problems.

And that is why we're really looking at the voluntary consensus standards because I do think that's a way to have surgical strikes. It's not a broad brush. It's a lot of different surgical strikes. That's one of the only ways you can get at some of these enormously challenging business models. We're going to need a multiplicity of approaches to solve the multiplicity of problems, some of which are very challenging.

MR. MAGEE: Well, just to drill down on that, I realize you're suggesting a multiplicity of approaches. But just using the example of the data

broker, what are the responsibilities of the first party to inform consumers and offer choice about sharing with a third party? And then what happens after that? What's the third party's responsibility to the consumer?

MS. DIXON: So I would really like to see appropriate notification to the consumer of what's happening. And it's got to be in a way that's clear to the consumer. But even better, I would really like to see consumers have a choice about whether it happens at all. And by that, I mean, to determine best practices around what gets shared or if.

For example, can we agree that there is some data that should not be shared in that fashion? For example, you know, genetic data or perhaps other biometric data. There should be some agreements that we can come to in certain contexts. I don't see why we can't find that.

Another way of doing this is to say are there standards that can be created with all the stakeholders present, having a discussion that is open and transparent and comports with due process where we can come to some kind of agreements about acceptable data uses in that context and nonacceptable data users that require consent. I actually think it's going to

require some kind of process that has teeth. I'm not sure what will happen if we just get a written notice from the first party with no teeth. I'm just not sure that that will actually work in the long term. We've had that for about 25 years.

MR. MAGEE: Well, I think it is very interesting, this concept of perhaps just taking certain uses out of the equation. I mean, it sort of begs the question of what those uses are. I mean, we've -- to go back to the online behavior advertising context when we first issued a report in 2009, we suggested perhaps sensitive data shouldn't be collected and used for that purpose. It's very difficult to define what's sensitive. It's an incredibly subjective question.

Just to pull in some of the other folks on the panel, I thought maybe Katherine or Rachel, if you'd care to weigh in how you would make a determination of what sort of data shouldn't be collected and used, how you define what is sensitive or what would be particularly upsetting to consumers.

MS. WELCH: I'm happy to. So maybe before I take that question, if I could just make a comment about the first party/third party data broker discussion that Pam was having. We agree that this is

a very thorny issue. How do you convey to consumers what's happening kind of behind the scenes, what's happening that's invisible to them? And in some cases, it's not just third party, but it's also first parties who are invisible to them, especially if you're interacting with a website, there's usually 10, 20, 30 entities that may be interacting with you, and how do you ensure that the consumer has knowledge of that and has some opportunity to consent?

I think, for us, we have grappled with this question of how do you define "sensitive," what might be a prohibitive practice, what might be a permitted practice. And we find that it is hard. This is line drawing and it can differ depending on the sensitivity of the user. So Neil doesn't want to engage with me and I feel kind of bad with that.

MR. RICHARDS: I wouldn't say --

(Laughter.)

MS. WELCH: With my company.

MR. RICHARDS: With your entity. You're great.

MS. WELCH: But, you know, how do we draw lines for Neil that may be different from the lines that we need to draw for Katherine or for me and that's why we've kind of come back to this concept of

saying opt-in for everything. It may be difficult to scale, but I think it's something that we need to think hard about because it has been difficult.

And I'll just add one other piece to it is that, you know, the idea of having comprehensive privacy legislation I think is helpful to hopefully minimize some consumer confusion in the sense that if there are strong privacy laws at the federal level, people have a sense of this is what is permissible and this is how I can control my engagement.

And so I little bit differ with Neil about notice and consent. I haven't given up on the notice and consent and Charter hasn't given up on notice concept. I'm not sure Cambridge Analytica was caused by that. There are -- the idea of having a strong law that consumers know what the rules of the road are, that the companies know what the rules of road are, I think that could help prevent those type of things happening, misuse, mishandling, misappropriation of data.

MR. MAGEE: Katherine, do you have anything to add on that?

MS. TASSI: Yes, so --

MR. MAGEE: And the Florencia.

MS. TASSI: So I think that having

legislation that outright bans certain types of data from being collected or processed would be too drastic. There are just far too many industries and organizations that that have reasons to collect and process all sorts of data that could be for very good and beneficial purposes.

I mean, even if we started with the GDPR model of having to at least begin with having a lawful purpose, you know, to outright ban certain types of data collection would be even more drastic than having to start with -- having a lawful purpose. At Snap, we focus on having substantive privacy protections for all users, things like having built-in retention periods for all data, shorter retention periods for data that we consider more sensitive, like location data or interests or behavioral data, and as I had mentioned before different types of privacy protections depending on where data's being collected.

And in terms of, you know, federal privacy legislation, Snap believes that good federal privacy legislation would require companies to be transparent about their data practices, promote flexibility through privacy by design, as I mentioned before, and privacy risk assessments, incentivize good privacy

practices through data minimization and deidentification or pseudonymization where possible.

I want to return to the transparency, making companies be transparent about their data practices, as a kind of counterpoint to all of our discussion about notice. Because I do think that there is a difference between companies giving notice of their data practices and data processing and being transparent about it. And I want to relate this to the transparency principle and the GDPR a little bit and suggest that we could borrow something from the transparency principle in the GDPR.

The GDPR, although the transparency principle and requirement is contained specifically in a couple articles -- and it's actually -- if you read the entire GDPR, which I'm sure most of you have, it really flows throughout the entire GDPR, the transparency principle. It underlies the entire law. And transparency is really essentially fundamental to all of data protection under the GDPR. And it's embedded.

In the very word "transparency" is all of those things that we want notice to be to individuals here in the United States, which is clear and understandable and communicated well. You don't have

to say that when you say make your data practices transparent to individuals. It's right there in the word.

So at Snap, for example, what we do to make our data practices transparent is have them communicated in a multi-faceted way. The privacy policy is the floor, not the ceiling, which is why when we give notice in app in our just-in-time notices, it doesn't matter if we've said the same thing in our privacy policy or in our privacy center. What matters is whether we've actually communicated that in a transparent way to individuals, and the transparent way of communicating certain things is in the moment to the Snapchat or when they're going to use the product or feature, not did they read it in the privacy policy when they first registered for the app. We're quite realistic and know that most individuals don't read the privacy policy when they register.

And so in order to fulfill the transparency requirement, we actually want to put the just-in-time notice up there and give the choice then. So that's where I think notice really can borrow from the transparency principle in the GDPR.

MR. MEHM: Thanks, Katherine. That was very

insightful. There is a tremendous amount to unpack in what you just said, but, unfortunately, we only have a few minutes left and we want to be mindful of the other panels today.

So what I want to conclude with is asking each panelist in one minute or less what you would like the audience to take away from today's discussion about notice and choice. And let me start with Jordan and each of you have one minute. Thank you.

MR. CRENSHAW: Sure, thank you.

I think the most important takeaway today is that, as I said earlier, is certainty and control for consumers and also having that cycle lead to trust with the consumers and also with business. I think there is a definite place for notice and choice in the equation with regard to how data privacy is regulated. I also think there is a role for collaboration as well. And that was actually the Chamber model bill. We actually have safe harbor provisions that enables some self-regulatory guidelines with FTC approval.

I think there's a role for collaboration and there's also a role for really meaningful privacy protections in federal legislation that would create certainty through removal of a patchwork emerging in the states.

MR. MEHM: Okay, thanks.

Pam?

MS. DIXON: Thank you.

We didn't get a chance to talk about trust on this panel, but we are living in what Bo Rothstein describes as a social trap, which is where parties that would be benefit from collaborating with each other don't trust each other, so they don't and they get -- but they both get stuck. So basically we're all cutting off our noses to spite our face by not working together. I do think it's extremely important to work together to find solutions in a way that encourages mutual trust.

So I want to talk quickly about uses. We didn't really focus on data uses because of the structure of the panel, but I just want to bring up the Fair Credit Reporting Act and the Equal Credit Opportunity Act. It's important to understand that instead of restricting data collection sometimes it's a lot more useful to look at the end uses as a way to try to work on things.

But I want to end with following up on what Jordan said. Self-regulation is not going to be able to provide a safe harbor from the FTC. OMB Circular 119 provides that any regulatory process that the FTC

or any US agency would join in has to have due process. Has to be made with due process. So that would be a voluntary consensus standard. I do support that as a way forward.

One of the ways forward I also support, broad-based legislation and other tools and things that will assist. We need a lot of different tools.

MR. MEHM: Thanks, Pam.

Florencia?

MS. MAROTTA-WURLGER: So the takeaway point from the discussion, I think, is that notice and choice is complex. It has many benefits and that it affords firms a lot of flexibility and consumers some seeming choice. But choice can be daunting and consumers just do not get -- are not informed. So just to add a little bit of data to the discussion and analysis of the event, the extent to which there's been compliance with the FTC guidelines by firms, shows that it's been very weak, extremely modest at best, at most with 50 percent of the recommendations.

That being said, I've noticed very intense difference across markets in ways that are intuitive. So places where information protection matters a lot, there's been a lot of protection and where it matters less, there's been less. That doesn't necessarily

mean that the markets are working or that there are any market failures. But what it does show is that there is a need and a desire by firms and across markets to have some flexibility in the approach. So this kind of strict top-down regulation prohibiting everything could create a lot of damage. Now that being said, focusing on more notice is, in my view, barking up the wrong tree.

And then this interesting difference, there's been some very strong spillover effects from GDPR. In May 2018, all of the US privacy notices mostly changed, and the compliance with GDPR has been so -- has shown some interesting changes, particularly when it has to do with contract third-party contracts, data retention limitations, anything that's in the privacy by design approach where a firm has to comply globally. All of that has changed tremendously.

MR. MEHM: Thank you. We're going to keep people to a minute or less, if possible.

So Neil?

MR. RICHARDS: Four points, one minute. First, notice and choice are not evil. They have virtues that Katherine and Rachel have pointed out in appropriate context, but they are insufficient to

protect privacy and to protect consumers, which is what we are talking about. In practice, most notices are constructive and most choice is a fiction. Notice and choice, the way it has evolved in the United States, has been better at harvesting data than at protecting privacy and protecting consumers.

Second, notice and choice don't scale for the reasons I talked about earlier. Third, what we need are not the procedural protections of weak notice and weak choice, but substantive practices and we need to develop those. It's interesting that in both the Fourth Amendment context and in the consumer protection context with the FTC Section 5 standards have been more effective than rules.

Finally, fourth, those substantive protections can include trusts. That's something that Woody Hartzog and I have written a lot about. We think trust has four elements itself. Companies who are trustworthy, whether based on business incentive or coerced by law, are honest to their consumers. They are discreet. They don't show data unless it is necessary. They protect those consumers from breaches and bad choices that are avoidable. And, fourth, they are loyal to their customers. In the duty of loyalty and the idea of an information fiduciary is something

that is being discussed, but I'm out of time. So I'll stop.

MR. MEHM: Thanks.

Katherine and then Rachel, and we have less than a minute.

MS. TASSI: Two seconds. At Snap, we think that notice and choice can be effective in certain circumstances, especially when communicating directly to the consumer, but that it needs to be combined with other methods of protection where we use especially privacy by design.

Rachel?

MS. WELCH: Thank you. So we support a framework based on five principles, and key principles included are the idea of consumer control and transparency; from our perspective, an opt-in control that's meaningful, that's renewed with frequency is important; and for transparency, we agree that it needs to be something that is communicated to the consumer, is clear, is readily available, and at the appropriate time.

MR. MEHM: Thank you all so much, and that concludes the panel on notice and choice.

(Applause.)

MR. MAGEE: We're going to be taking a 15-

minute break, and I think the next panel starts at 10:35.

(Panel concluded.)

PANEL: ROLE OF ACCESS, DELETION, AND CORRECTION

MR. HO: Welcome back from the break, everyone. My name is Jared Ho, and I'm an attorney in the Division of Privacy and Identity Protection. To my left is my fellow co-moderator, Ruth Yodaiken, an attorney in the Office of Policy and Planning. So we're delighted to be here today to -- we have a stellar panel of experts to discuss access, correction and deletion rights.

So starting from Ruth's left and going down the line. Jonathan Avila is the Vice President and Chief Privacy Officer of Walmart; Katie Race Brin is the FTC's former Chief Privacy Officer and current Chief Privacy Officer of 2U; Chris Calabrese is the Vice President of Policy at the Center for Democracy and Technology; Jennifer Barrett Glasgow is the Executive Vice President of Policy and Compliance at First Orion; Ali Lange is a Senior Policy Analyst at Google; and Gus Rossi is the Global Policy Director at Public Knowledge. So we're delighted to have them here today and you can see their full bios online on our website.

So today, we'll kick off the panel with a moderated discussion on access, correction, and deletion. Ruth, do you want to start off with the

first question?

MS. YODAIKEN: Sure. And I'm going to ask Chris to start with the answer to this one. We heard a lot of discussion about the goals for different privacy protection measures, and so we'd like to start off by asking what do you see as the goals for giving consumers access, rights to correct, delete, and port data, especially in these days where there are complicated data ecosystems involving AI and big data?

MR. CALABRESE: Sure. Well, thank you first for having us represented on the panel.

So I think the place to begin is by recognizing that this is only part of the solution. I know we've had a lot of discussions and I won't bring in all the other parts of the solution, but I don't think anybody should lean on access, correction, and deletion as the sole answers here. But they are answers and they do play some really important roles.

I think the first is that they empower consumers. They really do allow consumers to have some certainty about where their information is going, what's happening with it, and provide some accountability for that.

So I'll give you an example. So the app, Grindr, was in the news recently because the Chinese

owners of the company are being forced to divest of it because of national security interests. Well, if I'm a US consumer, I have no way, when that transaction takes place, even before the divestiture happens, to say, well, maybe I'm not comfortable with my information being held by a Chinese company. So what should I do? How can I make sure that I have the legal right to delete that information and know that it's not going somewhere I don't want it to go? Well, that's why you need an access or correction and deletion right.

You know, I think that we also want to look at the time horizons at play here. These are going to be the rules for a very long time. I don't need to tell this audience how long many of the privacy laws in the United States have been in place. We're going to be setting rules up for years to come. So I think by setting a strong standard for these individual rights, what we're going to do is say to consumers that they can expect this. We're going to tell businesses that they can expect to build on this and build all kinds of positive powerful tools to help consumers. So I think we're going to have a lot more on this, but I'll leave it there.

MS. RACE BRIN: Thanks --

MS. YODAIKEN: Go ahead, jump in.

MS. RACE BRING: So, again, thanks so much for having me. It's so great to be back.

So in addition to what Chris was saying about empowering consumers, I think having these rights in place also keeps organizations honest. So even though there may be a very small percentage of consumers who actually exercise these rights, companies and organizations need to have procedures in place to allow for access, to allow for correction, to allow for deletion. So it forces companies to know where their data is, to minimize data because they don't want to have to provide swaths of data if they don't need to, and to provide mechanisms to answer those requests on a consumer's behalf.

MS. YODAIKEN: Go ahead. I think Jennifer and then --

MS. BARRETT GLASGOW: Yes. I would like to kind of amplify some of the things that Chris initially brought up. I would characterize providing more intelligence as a partial or improvement on transparency, not so much, as was mentioned in the earlier panel, the sole solution for transparency. I think we need to be careful of that.

It does provide, in the right circumstances

-- and, again, the earlier panel, I think, kind of highlighted some of those differences, some reasonable choices and controls. And it also, I think, should be tied to the reason for the request. This is something that we don't talk about very often.

But I think there are a number of reasons that a consumer might want to exercise their access right. It may be pure curiosity about what's going on. It may be a decision that they are trying to make relative to, do I want to do business with this company. It may be a situation where I think the data they've got about me is wrong and it's having an impact, a negative impact on me and it's something I need to get fixed, or it may be a situation where I feel like they are -- and this may not be a consumer issue, but it may prompt an access request, the consumer or the agency feels like the company is in some violation of their own policy or accepted standards or other rules.

So each of those, if you think about it, has some different dynamics to it. And I'll just warn you before we get started, you're going to hear two words from me fairly frequently. They were introduced on the earlier panel, so they're not new. One of them is context and the other is reasonableness.

MS. YODAIKEN: Gus, you wanted to add something?

MR. ROSSI: Yes, thank you. I think that Katie was right when she was mentioning that maybe some individuals, but not all of them, will exercise their access rights. But we shouldn't miss from the picture that having these rights would allow consumer watchdogs, such as Consumer Reports, Public Knowledge, ACLU, to understand better what is it that big organizations are doing with our data. And then that not only increases transparency, but also enables advocacy, enables consumer protection in ways that is harder to do in the absence of these rights.

At the same time, I think that especially when we consider the relation of individual consumers, vis-a-vis, big organizations or platforms, there is clearly a huge asymmetry of information that deals with the balance of power towards one side and leaves individuals unprotected and consumers often unprotected. So having these rights is also a way to bring some information symmetry to the market which in turn would contribute to make it work better for consumers and also for entrepreneurs.

MR. HO: So now that we've sort of discussed the goals of access, what are the types of information

that consumers should have access to? Is it everything? Are there certain types of data where the costs might outweigh the benefits of providing that type of data?

I'll open it up and see if there's anyone that has an initial thought. Jon?

MR. AVILA: Again, thank for inviting us to participate in this event.

I think there are certain types of data, for example, very obscure data, the benefit of which providing it to consumers may be outweighed by costs. Obscure data are things, for example, on backup tapes, backup media. These are things which were not in active use by the entity and can be extremely costly to produce, restoring the backup media, extracting information, then putting it back into a backup form. That may not be justifiable.

Also, there's certain information I think that's extremely trivial. I mean, if we look at the original purposes of access and correction rights, they apply to situations in which the data could have a significant effect on the life of the data subject, FCRA, various other significant impacts. There may be trivial information which has little or no actual impact that perhaps also is at least not at the core

of the purposes of access and correction rights.

MR. HO: And I want to return back to this concept of trivialness and sort of what the factors might include in sort of determining whether data is trivial or not, but, first, I want to give Gus an opportunity to respond.

MR. ROSSI: Yes. So I think that one of the key challenges of this debate over this use of the rights right now is that it's hard to get into the nuances of these rights and these attributes in the absence of a baseline privacy framework that is the reference that we are all discussing about. So that's why I think that, in our view, the high-level principle should be that users should have access to all of the data and then understanding that there may be circumstances in which data might be harmful for consumers, harmful for security, harmful for the normal processing of the contract, unnecessarily burdensome.

It's reasonable to understand that there may be some circumstances where that might be the case, but I think that we should start from the position that assuming that users should have access to everything and then organizations that have the data should justify and should explain maybe in the process

of debating legislation, maybe in the process of explaining to the FTC or whatever regulator in charge of enforcing legislation, why there are some pieces of information that should not be shared with consumers.

MR. HO: Why don't we go with Jennifer and then Ali.

MS. BARRETT GLASGOW: Yeah, I think it was Pam that brought this up in the earlier meeting, the connotation of use of the data I think is extremely important in thinking about this, partially because the systems that we would be drawing the data out of are driven a lot by use, and by that, I mean things like is it required or part of placing an order or fulfilling the transaction or handling customer service associated with the business, that kind of is one big category of use that you can say, well, what kind of access do you need to do that.

Another is internal operational use. Some of it may not be personally identifiable, but depending on the industry, it may be. That's another type of use. We also mentioned earlier this morning fraud and risk data that the company is engaged in as being something that typically we don't allow access to. I mean, a bank is not going to allow access to their fraud detection systems to make sure that the

transactions -- to the algorithms that are looking at the transaction. So we might make different choices there. Sales and marketing. Maybe there should be because we want to give the consumer more rights or choices to opt out.

Research, data that you've got in your possession that you're working on for research purposes, is that subject to access and correction or deletion? And then, finally -- and I call it data monetization. This is where you're using data about individuals to actually -- either sharing it or selling it or allowing third parties to use it within your own enterprise. You're monetizing or making products out of data, in other words. And that's another category that might have, again, some reasonable expectations in it.

MR. HO: Ali?

MS. LANGE: Actually, I think this is an awesome discussion. I really agree with Gus's instinct that for the most part data should be available unless it conflicts with another sort of purpose. I think Jennifer laid out some really good examples. You know, you might have a legal obligation to keep some forms of data, you might have -- and so not let it be deleted. You may have some reasonable

limits on some other types of access.

But it's interesting, also, to think through -- like we've so far, in this discussion, talked about these three types of controls as if they need to apply kind of all or none. And, actually, if you had portability there, it would be sort of four general things we're talking about. For each type of data, there may be different parts of access, control, deletion, and portability that makes sense for people, that makes sense given the context, that makes sense given the obligations the controller has in other contexts.

But I would encourage us not to be too narrow in thinking about the reason for the request. I think that there's some utility. If you start from the presumption that you should be offering availability as broadly as is sort of reasonable, given those other constraints, we don't need to know too much about the nonnefarious motivations people might have. Obviously, you want to prevent fraud and other things like that. But the sort of beauty of these tools is that they can be applied broadly and you don't necessarily need to have some reason, as the consumer, to exercise them, right? It may just be curiosity, which is a totally valid use case.

The interesting thing that will happen as people become more familiar and there's some muscle memory that's developed around taking advantage of these types of offers is we may see some really interesting kind of examples in use cases and discussions and debate that come out of these tools.

I think it's just worth noting that at Google we do see quite broad use of the tools that we've made available just as sort of a baseline example. We can chat more about some other specifics later. The Google account page, which is where you have your settings and access to all of your other -- kind of the account information that's stored with your account and other tools like that, gets 2.5 billion visitors a year about, or at least last year it did and it's going up every year.

So there's certainly interest in this. There's certainly people who are engaging with things that are available. And I just think that if we think through the three things, you can tease out the four of them a bit more and not necessarily put people in a position where it has to be an all or none scenario.

MR. HO: Chris?

MR. CALABRESE: And just to piggyback on that because I agree, I think the default should be to

have access to these rights. Sometimes I think we think of these as individual rights and they obviously are, but that doesn't mean that we're expecting that the consumer is going to do everything to unpack the value of these things.

So I think a good example of this is in the financial services industry, for years and years we've had financial apps, think Mint, that look at consumer's data held by other parties and help those consumers use that data. For years, they did that using basically essentially you give your password and user name to Mint and Mint would then go to your banks. Tremendously insecure. Nobody loves it.

They're now moving to more of an API-type process and that has the benefit of security, but it also has the benefit of building an entire ecosystem. There's new apps like, you know, Plaid and Yodlee, that are using this information to help people budget, to help people make payments.

This is unpacking value from data. And I think that when we think about these rights, we need to think about them in the context of how we can take this tremendous digital economy that we are at the very beginning of and put it to work for consumers. And I think that if we think about it in those terms,

think about it in terms of what kind of system do we want to build, what kind of world do we want to build for data over the next couple of decades, it becomes really obvious why we want to invest in the front end on the technical capacity and broad use of these kind of rights for consumers.

MS. YODAIKEN: Okay. Well, if I can move it along to that idea of what companies need to invest to set up an ACD system. We had a mention by Jonathan of what's needed to pull up old tapes from the basement. And, Jennifer, you also mentioned a bit about what goes on in terms of the normal processing and this may be something that can be incorporated to existing systems.

So maybe, Jennifer, if you can start us off and talk about what companies need to make something like this happen. But, also, if you can just -- we'd like to hear some comment on the discussion that took place yesterday about whether some companies are going to be better able to do this than other companies because of their size.

MS. BARRETT GLASGOW: Yes. Let me -- I'll put the size question to bed quickly and first and then we can get onto the more complex one.

It really is more driven by your systems

than your size. If it's a legacy system and we never contemplated the need for access and/or correction or deletion, then it can be very difficult. And I'll give an example here in just a minute. If it's a new system that you're designing today, I hope we're beginning to take some of these factors into account as we roll out new technologies. I think we've seen that in certain industry sectors where access is -- tends to be -- we feel like it's more needed.

But another dynamic here to kind of put it into context, as I said, you're going to get tired of hearing that word, is whether there's a first-party relationship with the consumer or a third-party relationship. That came up a little bit on the previous panel. It's much more complicated for a third party to provide access than the first party because the first party has a username and a password or some other means to interact with the company, an account or a credit card or whatever, whereas a third party may not.

In my previous life with one of those big, bad, evil data brokers, I say that literally because I spent 25 years being the privacy officer for one, we put forth a voluntary access and correction and deletion system for the marketing data, but it meant

creating a whole separate repository for that data because the data at the time was not accessed on an individual basis, it was accessed in bulk. People don't want to market one person, they want to market to a group of people that have certain characteristics. That's replicating the data and then keeping that replication up to data with all the changes that are going on in the various systems. So that turned into quite an expensive and time-consuming operation.

So again, I would maybe summarize by saying how new or how old a system is may make it practical or maybe even impossible. And then for certain types of relationships where it's not a first party, it may be hard. And I'll mention one other thing, which I think we may come back and talk about, and that is any access request needs to have an authentication activity associated with it. And that could be fairly straightforward or simple if you have an account. It could be fairly complicated. It also depends on the nature of the data. If the data's highly sensitive, then the authentication needs to be very robust and rigorous. If the data's not as sensitive, you know, giving someone access to it that isn't the person they claim to be maybe has fewer consequences.

MR. HO: Katie and then Jonathan.

MS. RACE BRIN: Yeah, so I just had two followup points building on what Jennifer was saying.

So one of the criticisms about GDPR was that only the big guys were going to be able to comply, right. And that it would end up becoming a competitive advantage because small companies may either remove themselves from certain markets or not engage in certain business practices because they wouldn't be able to have a lot of the controls and requirements that are needed under the law. So I think that is true of any regulatory scheme is that if it's expensive and complicated to comply, then there may be kind of advantages to incumbents or to companies that have more resources.

And then building on Jennifer's point about legacy systems. So my company, we're an education technology company that works with colleges and universities to provide online graduate programs in short courses. So I am constantly talking to university partners. And the legacy system point is a really huge issue for a lot of universities, some of whom have been around for hundreds of years.

Now, there are requirements under FERPA that are similar to GDPR and other -- the California law in

that there are access requests that must be complied with for students to get access to their student records. There are rights to inspect education records. And so universities have been dealing with these sort of rights for many, many years, but the idea of an education record is really cabined in a way that broad definitions of personal data are not. So they are definitely struggling with how to address these -- a lot of these access requests when you have really antiquated systems that may not be talking to each other.

MR. HO: Jonathan?

MR. AVILA: I would like to reinforce both what Katie and Jennifer said. I think the distinction is not between large and small, but between legacy and new. Sometimes -- and even among large companies, that is very much the case. Sometimes we take the large, relatively new, integrated tech companies and treat them as the model for what is easily accomplishable. So we see they've already built a portal through which their customer data is accessible. Why can't every company do that or at least every large company?

And it very much is the difference between relatively new companies that have a limited set of

product offerings directly to consumers with integrated systems as opposed to older companies that may have a very diverse set of product offerings with legacy systems.

For example, if you're a big box retailer, you may be collecting data at your auto center where you have records about people's automobiles. You may be collecting data at your financial services center where you do check cashing and money forwarding. You may be collecting data about consumers where you're selling them cell phones and you're assisting them in signing up for carrier cell phone plans. That data may not be integrated at all. I think sometimes there's a presumption that large companies know everything about all their consumers and they have total knowledge. In fact, that often isn't the case.

So the difficulty of accomplishing an access request, we would have disparate systems and, of course, those systems don't have a hard key match so they are not keyed on social security number. So my name can appear as Jon Avila in one system, Jonathan Avila in another system, J-O-H-N Avila in a third system, and then that's compounded if I've moved from one address to another. This is an issue of data quality, but executing an access request, for example

across all of those systems, is very difficult.

MS. YODAIKEN: Gus and then Chris.

MR. ROSSI: I think that definitely it's going to be very hard for some companies to comply with all these rights and maybe those of their systems. I think that that's why it's important that in [indiscernible] we identify both what's the dress code of obligations for -- depending on maybe the size of the company. I don't think that the system should be the dress code. I think that if a company collects a lot of personal information and it cannot keep it in a way in order to guarantee consumers' rights, maybe that company should reconsider whether or not it can or it should keep collecting so much personal information and that's going to be transition costs to pay.

And I think that a way to diminish the costs of this exercise is perhaps for the FTC to identify which are the dominant players in each sector of the economy that should be subject to a different set of obligations or with more stringency than other players.

So, for example, there have been like -- I think in CCPA, there is a limitation of how often a consumer can exercise her right to data portability,

right, to twice a year. I think that might make perfect sense for a small supermarket. That might not make perfect sense for a nonprofit. It might not make sense to allow Google or Facebook to stop the consumer from asking for that data when the marginal costs of providing that service like ten times a year is zero once you have the system.

I think all those nuances are important as well. And, also, especially considering that how often consumers get to exercise these rights is going to influence and limit both the capacity to exercise the right to data portability and, as Chris was saying before, more importantly, the right to interoperability, to interact with the data from different services. If we start limiting that at large for every player, we may end up like actually entrenching the power of the dominant players in the market and we might end up like making true those fears that if we pass a stringent and comprehensive privacy legislation, we might not end up in an uncompetitive market that we don't want.

MR. CALABRESE: So I'm going to push back a little bit. I think it should have nothing to do with size. I don't think that -- I mean, it's been said many times, Cambridge Analytica was a very small

company. They had a lot of data. I do believe that this is not as big a problem for most small entities. I think that just like you have a third party that handles payroll, you'll have a third party that handles some of these compliance obligations. I just don't think it's going to be that big a deal.

The medium-sized company may end up being the harder one actually because they're big enough to maybe have a lot of data but maybe not quite able to have that kind of bespoke option. But I do think that we should keep in mind, first of all, there is going to be a transition period for whatever law we have. I mean, GDPR's was two years. There's going to be some time. And I also think that reasonableness cures a lot of problems in this context. It doesn't solve every problem, but I think that we should be mindful when we're thinking about edge cases, that there are going to be reasonableness requirements.

We are going to have situations where -- I suspect strongly just from looking at the variety of proposals out there that being unable to comply with the strict provisions of an access requirement, you know, the first month after the law is passed is not going to be a corporate death penalty. It's just not. It may get you a visit from your state attorney

general. You may have to figure out some compliance. But it's not going to be the end of the world.

When you weigh that against the tremendous potential benefit of allowing consumers to have this kind of access, to use their own data, I just think it's a no-brainer and I think we should be careful about cabining the individual rights around short-term use cases that I think frankly can be overcome with some time and some energy.

MR. AVILA: If I might just follow up for a moment. I think Chris is absolutely right. This isn't an issue of should we do this, shouldn't we do this. It's a matter of how regulation is implemented. There has to be an adequate period for implementation to deal with legacy systems. There also has to be adequate regulatory guidance. A situation which, for example, regulations can be issued about how requests will be verified up to two or three months before the effective data of the obligation is not an ideal regulatory system.

As Chris noted, it was two years, the implementation period for GDPR, the text was established at that point. There was some regulatory guidance after that, but the text was reasonably clear and also had been debated for quite a while before it

was enacted. So those transition periods are really vital in these situations.

MR. HO: Okay. So we've mentioned GDPR and we also mentioned CCPA at this point. So there are access and correction and deletion and portability provisions that currently exist in various frameworks and codes of conduct. For those of you with experience with these various laws, GDPR, CCPA, and others, can you point to specific examples where access, correction, and deletion are working in those models, and perhaps you know where some of the challenges lie in those models.

Katie?

MS. RACE BRIN: Well, I'm going to talk about the Privacy Act since as a CPO at the FTC I spent a lot of time thinking about the Privacy Act. So the Privacy Act was passed kind of in the wake of Watergate to provide transparency, which is a word that we've heard a lot today, to citizens about the personal information that Government agencies hold on them. There are certain aspects of the Privacy Act that you see kind of reflected in, you know, both legacy and kind of a lot of these laws that we're talking about and potential regulations that are coming down the pike.

So from a transparency perspective, agencies are required to publish system of records notices, which kind of describe what information is held in which system about individuals, and they have to be updated when the system changes and there are kind of a lot of disclosure requirements, they're published in the Federal Register. And then citizens have the ability to request -- under the Privacy Act to request information about what records agency hold on them, right. So this is sounding familiar with a lot of GDPR requirements, CCPA requirements.

Individuals don't have access -- do not have the right to access any records about anyone other than themselves, right. So it's limited to just information about them. And then they also have the right to correct data that is held in these systems that may be inaccurate. So I think a lot of the -- government agencies have been dealing with a lot of these requests and have been dealing with being able to provide access to their systems since the '70s. So this is -- you know, in some ways, there's kind of nothing new under the sun.

But the way that the Privacy Act, I think, you know, as we definitely struggled with this at the FTC and we're working with our counterparts across the

Federal Government about the Privacy Act, really looked at kind of individual, like an individual file folder that had papers in it about you, and that's not really the way that the world works anymore. We have combined data. We have very complicated data systems. And when a request comes in, how do you deal with that shared data, which I know we're going to talk about a little bit more later and, you know, kind of what's the breadth of the personal data that the individual has access to.

But I think that these ideals about transparency, making sure that organizations are clear about the information that they're gathering, and then having these access rights is something that has been true in the Federal Government context, at least, for many years.

MR. HO: Ali?

MS. LANGE: I actually have a really interesting story that I think helps answer the question a little bit from one perspective and it's about data portability. So when Google was creating the data portability tool that we sort of conceived of over a decade ago and has been iteratively improved on -- or we hope improved on over time, the original kind of idea of it was actually born from a quote from

former CEO Eric Schmidt who said he doesn't want people to be at Google because they felt stuck. So a team sort of took that idea, ran with it and said it should be easy for people to take data and leave the company if they feel they want to do that.

So the system was built. And as it turned out, for the most part, what we've seen over the last decade of making this tool available is people don't, for the most part, use it to leave Google. They use it to download a copy, they use it for curiosity. They're curious what's in their tool or what's in their account. They're curious where they might be able to take that data. They need to move things from, you know, Google to Microsoft One Drive. There's a lot of use cases and sort of the like I'm fed up, but I'm taking my data and then I'm going to go delete it. It turns out to be at least not the dominant use case.

So there's a couple of really interesting insights from that example. One is, as I mentioned earlier, we shouldn't let our imagination or our sort of vision of what these tools are useful for be the end of the day, right. There has to be some room and some consideration and continued observation of how people are actually using the tool. Once we

understood that it wasn't necessarily the primary use case to sort of like leave, but instead to go somewhere else, try something new to have a copy, it really informed the way that we continued to iterate on and provide that tool to make it easier for people to use it for the things they were actually using it for.

And among those things that I think is the most interesting is really the benefit of that type of tool is it enables people to try something new. It makes it easier for you to say I'm not ready to leave this one particular like -- there's a bunch of, for example -- we could take a non-Google example. There's companies that do -- you know, they make a map of your exercise if you go outside and you make a map. I'm not ready to leave the company I'm used to, but I want to try this new one on the market. So maybe I'll take some of my data, put it in there, see how it looks, see if I like it better. If not, I can kind of keep it and switch back and forth or maybe I like to use two of them or maybe I like to use none of them and you can have the rights that apply for that.

For us sitting here in the US, this may seem like, oh, that's really a nice thing to have, but in economies where there is still more volatility around

startups, where there's still more sort of volatility around stability and there's a lot more emerging innovation, it's a really big deal to be able to feel like you don't have to make a choice between trying something new or sticking with what you have, that you can sort of experiment, find the thing that works for you, and as products and tools change over time, to continue to make that decision as it makes sense.

So I think those are -- it's a really interesting use case for both how the creation of these tools needs to be done in a way and observed and modeled in a way that continues to allow the expressed interest in them to become -- to develop on its own and to become the sort of the reason for them to exist, and also that there's utility to the economy of enabling people to try something new and to lower the stakes for that.

MR. HO: Jennifer and then Gus and then Jonathan.

MS. BARRETT GLASGOW: Yeah, I really want to pick up on the concept of what does the consumer want portability for. I tend to not think of it in the same context as access, correction and deletion, but more of a business feature. Am I going to take my American Airlines history and move it over to Delta?

Am I going to take my Marriott Hotel history and move it to whatever one of the other brands are, and I lose track of who owns what now?

MR. CALABRESE: Marriott owns them all.

MS. BARRETT GLASGOW: Right, right. So I think we have to look at it in the text -- and what's the ownership of that from the company's standpoint. Are we providing competitive intelligence by having a consumer doing it and, of course, then the cost to do that if it's not something that the consumer actually wants and can benefit from or has some vested interest in.

So in general, you might try to think of that as if I have contributed data to this or if there is a long track record of data that I may not have participated in contributing or providing, maybe there's some value, if it's just my transaction history at a retail or not. But then you get into unique situations like in healthcare where I do want to take all my medical history records and move them over. But that's very industry-specific and very context-specific. So I think talking about data portability in a real broad general light can lead us down some very troublesome paths.

MR. HO: Gus.

MR. ROSSI: Yeah, I think it's very hard for consumers to understand the value of the data when the data is locked in somewhere. So when you can see it, as we talked before, if you see that you are classified as someone with very low incomes -- a low income, you might start understanding why you're not receiving ads for certain jobs. Or if you see that you're being targeted for publicity regarding your location, then you may understand why you're being discriminated against in certain ways.

So I think that, on the one hand, it empowers consumers in general to exercise their civil rights. But at the same time, given the rights for access, correction and deletion and then, as I said before, I think that GDPR has a great balance for this situation, which is saying that you have those rights as long as those rights don't infringe on other people's rights. So I think that's a very decent kind of principle. It's important.

But that's why I think that data portability is key because it's like -- it's actually a meaningful way of exercising these three rights. I agree with Jennifer that maybe most consumers don't think today that has it any value to get all the flight information from American Airlines or United, I use

United because it's what I have here, and -- but it might have -- for some of them, it might have value for a startup that if you have access to that data, can offer you a better way to book your tickets with United. It might have some value for you to actually go on, if you have billed miles with an airline to go back to a different airline and say, I not only have like this status, these are my regular flights, what can you offer me so I switch.

But I think that the most interesting part of European law that we should try to see as an example is the second payments directive, which basically in the UK has been implemented as the open banking initiative. Basically, the consumer -- the Competition Authority of the UK mandated that the nine largest banks in the UK have to open their data and credit consortium to develop open API systems, to allow FinTech third parties to both interact in real-time with that data, and including for the exercise of payments that consumers have. And I think that's the kind of like access, correction and deletion rights that meaningfully transform the marketplace and empower consumers, put consumers back in control.

MR. HO: So I know we're running short on time so we're going to move on. But we'll give

everyone opportunities to get their thoughts in.

Ruth, do you want to --

MS. YODAIKEN: Yeah. So just to dive into some of the items that were raised, we're interested in some of the particular challenges, the actual challenges to making ACD and portability, if you count that separately, happen. In particular, some of you have raised the issue about authentication, so that and other items. Anyone want to start us off?

Chris, do you want to start us off?

MR. CALABRESE: Sure. So I'll start off by cheating and making the point that I was going to make.

MS. YODAIKEN: I thought you might.

MR. CALABRESE: But it is a challenge, all right. So we have the blue button regulations that are coming forward right now, which is giving people the right to port their information out of their medical record and in somewhere else. Well, we're giving consumers -- we're actually mandating that consumers be able to port their right from a highly secure privacy protective regime, which is to say HIPAA to a wild marketplace that has almost no controls over and protections for that personal information, certainly, as when compared to HIPAA.

That seems like a pretty big challenge. I mean, that's why these rights have to be viewed as part of a comprehensive framework because if they aren't, you have the real possibility that you're going to take information you think is highly protected and bring it somewhere else.

Having said all that, I will now actually answer the question and say I do think that we do have authentication issues. I think that there are a lot of use cases where authentication issues aren't that big a deal, certainly in the Google context where you have a lot of authentication already in place. I think that in the case of third parties, we do have to authenticate data, but it's also incumbent upon the third party as the person who is holding the data and the person who is deriving value from it to make those authentication provisions work.

MS. YODAIKEN: Go ahead, Jonathan, and then Jennifer.

MR. AVILA: If I may, I think one of the most difficult examples of authentication is where you have a third party who is representing the data subject, and children's data is the most obvious one of those. There also are some provisions, for example in the CCPA, that would enable third parties to

represent data subjects. But in the area of children's data, you have not only the authentication of the child, but the relationship between the requester and the data subject, between the parent and the child.

So if we look to COPPA, I think COPPA offers some instructive guidance about how to handle that because COPPA has its own access provisions that permit the data controller to exercise reasonable means of authentication and also provide a save harbor where the authentication ends up being incorrect, where there's somebody who is incorrectly authenticated as the parent of a child. That's in a very sensitive issue -- a very sensitive area of data.

I mean, I think to the degree that we extend rights to third parties to make requests on behalf of data subjects, we have to really consider the risks there because they are exponentially greater than they are in direct data subject or requestor situations.

MS. BARRETT GLASGOW: Let me just give some practical examples because I think sometimes they speak louder than us talking about it theoretically.

Again, in my experience going back a number of years, in fact, this goes back actually to the '90s where there was some self-regulation that ultimately

got consumed when GLBA and other laws went into effect relative to data that was used for risk decisions. Risk systems have a lot of very sensitive data in them. They have social security numbers, they have driver's license, they have the keys to identity theft. I mean, you can kind of summarize it that way.

Giving someone access to that and not being absolutely as confident as you possibly can be that you're dealing with the right person creates a couple of risks. Well, many, but I'll highlight two. The first is, you know, you're potentially putting the actual real party at risk because the state is going to someone that is probably trying to get it for nefarious reasons. The other is that they are -- the risk that the requester wants to change the information for this or delete the information for the sole purpose of getting around its primary use, which is to identify you, comes to play.

So as I mentioned earlier, I think it's a scalable kind of thing, but companies have the right to say I don't have confidence that I'm dealing with the right person. The example that always comes to my mind is the risk data that we used to have where we allowed partial access because if it was wrong, that

was bad. So we needed this -- we had an accuracy component that had to come into play here.

But we didn't allow deletion. And if it was to be corrected, we had to independently verify the correction with another party because the correction is exactly what the bad guys wanted to try to circumvent the system. That's an extreme case and I don't know that it applies in every situation. But I think it's an example of where when you take into account all the factors and put the request, whether it's to access, correct or delete into context, you can come up with a reasonable decision to pick up on your word that works for everybody.

There's a balance between -- I feel like we need to introduce the concept of fairness for both the individual and the company. I think a lot of the discussion up to now has been focused on the individual because they haven't had some of the rights that I think that we're trying to give them in our movement towards more legislation here in the United States. I don't want to forget the fairness to the company while we're doing that.

If the company is deriving all the value and the individual isn't deriving any value, that balance seems off to me to say the consumer needs -- we need

to have the company have fairness, but wait a minute, it's the company that's getting all the value. It seems like they need to be spending more time with the consumer because the consumer's not really getting anything from many --

MS. RACE BRIN: Well, the individual is getting fraud prevention potentially.

MR. CALABRESE: Well, maybe. I mean, or the individual is getting denied credit because they're wrongly being identified as fraudulent --

MS. RACE BRIN: I don't think you can say that there's necessarily no benefit.

MR. CALABRESE: I'm not saying there's no benefit, I'm saying the benefit is pretty sharply skewed. Take people search apps. People search apps don't do a lot for people. They do a lot for people who want to search for people.

MS. BARRETT GLASGOW: Here's where I think you can take a bunch of different industries and come to a different answer on each question when you drill down it.

MS. RACE BRIN: Can I have just one quick addition with a concrete example that I think is helpful? That, you know, I do think companies have to balance whether there are other reasons why data needs

to be retained, so particularly when there's a deletion request. And some companies are so nervous about GDPR compliance that there is perhaps an overdeletion happening, and I do think that there is a real threat of fraud as part of that overdeletion.

So one example from 2U's context is that if an individual applies to one of the 2U-powered programs that we run, we -- and then asks to be deleted, we and the university registrar needs to maintain some minimal record, right, that that person applied, let's say, and was denied. If everything is erased on that individual, then you can see how there's you know, an opportunity for fraud there.

MR. HO: Okay. So moving on to the next question. To drill down and get into even some more trickier and thornier topics, I want to ask about shared data and inference data. So sometimes the information about companies -- the information that companies have about consumers include not just information that consumers contribute themselves, but what might be contributed by other users as well, you know, photos, you know, that are tagged, for example.

On top of that, companies might use the data that consumers have provided to create new types of data inferred, and we heard a little bit about that in

the last panel. So when we're talking about this balancing, Katie, how should firms look at that? You know, what are consumers' rights with respect to either type of information and whose rights sort of ultimately win out?

MS. RACE BRIN: Well, the way that we've looked at it is we've tried to distinguish data that just pertains to one individual. So think about like the papers in a file, you know, not actual papers in a file, but something that can just be tied to one individual, and then shared data. And so 2U holds tons of shared data.

So as part of all of our programs, we have live classrooms courses, right. So we have 20 people logging into our learning management system who are interacting with a professional who are chatting, who -- there's video, there are images, there's a voice recording. And so if somebody asks for that video to be deleted, well, what about the other 19 people who have rights to go back and look at that lecture when they're studying for their final exams?

So the way that we deal with that is we look to see how or if personal information of any particular individual can be obfuscated and, you know, hopefully, in many cases, it can be, but there are

cases when it cannot be. And I think in those cases organizations need to balance the right of other individuals who may be impacted by the deletion of that sort of data and, you know, again, make a reasonableness decision. There's a balance here, how do you balance the rights of two individuals who may have different interests.

MR. ROSSI: I agree. I think that it's important that organizations can balance the request regarding the rights of all their consumers and also legitimate business interests. So, for example, the execution of the contract, preventing fraud, obviously good reasons. At the same time, I do think that it's important to keep in mind that these principles make sense in the context of a comprehensive privacy bill that also empowers some regulator to both protect consumers when they "recourse" decisions of organizations because otherwise it doesn't work. It's very easy, in the absence of a law and a regulator that defends consumers, for organizations to simply say, like, no to all requests because it's going to be cheaper, it's going to be easier, it's going to be less complicated, right.

And so like, yes, that brings about like allowing organizations to balance the request makes

sense in the context of a comprehensive privacy bill that details, at the very least, what are the things that consumers have rights for and empowers an agency to police privacy practices by organizations. And I think that something that we should keep in mind is that what's inside this, this comprehensive privacy bill -- this baseline of privacy protection might determine how much information companies or organizations are going to be willing to collect or not. If there is a mandate for data minimization and privacy by design and by default, then things change dramatically.

A problem that we have right now is that the default for many organizations, especially in the tech sector, is to collect as much information as possible and figure out what to do with the data later. And that creates problems for consumers. And so that's maybe something that should be discussed as well because that will change as well the incentive of organizations to collect information and to determine what you have access to and how easy it is to provide this access.

MR. AVILA: I would just note that I think Katie raises a very good point, which I would phrase as the integrity of the historical record. The

emergence of the rights of deletion, for example, in the European Union, the European Union has a very different concept of rights of free expression. The rights as we accept as absolutely normative under the First Amendment don't exist to a large degree under European Union law. There are several notorious, I would call them, cases of the European Court of Justice severely limiting rights of free expression in favor of rights of data privacy.

So the integrity of the historical record I think is important when it comes to rights of deletion. There also is a commercial speech doctrine under the First Amendment in the United States, and that has to be taken into account when considering how these rights would be imported from Europe to the United States.

MR. HO: Ali, and then we have to move on.

MS. LANGE: I want to make a couple of points. The first, without undermining the achievement that the GDPR is, I don't want to give it too much credit for inventing of a lot of these concepts and a lot of this has been around since before the GDPR. Companies such as Google have been confronting some of these challenges in a practice sense for a long time before the GDPR. I think they

provided some good examples that were considered under the sort of guidance and advice given as a result of that document.

And one of the interesting sort of test cases I would provide in this context is, you know, one thing the product teams talk about a lot is the user's mental model. So when you're talking about shared data, I think Katie's example was incredibly rich in detail and an incredibly sophisticated question. But you can even look at something like email. Like is email a shared data type?

And the mental model for email, because email is sort of one of the original data types for the internet, right, is I have a copy and then I send a copy to someone else and now we both have a copy. So mentally we think there's two copies. Like if I send an email to Chris saying, hey, great haircut, and then he deletes it, like I disagree with this, I don't think that I have a good haircut, then I still have that record that I sent that.

And so if I were to access my email or download or do anything to my email, it's sort of a stand-alone idea. You can look at something like what happens now with the cloud where you would share a photo, like if Chris shared a photo and said, hey,

look at my great haircut and he shared it with my account and so I could access it and he deleted it, I would no longer have access, right, and I might choose to remove it from my account, I might say, I don't want to look at this picture, but it's not the same as being able to delete it.

So there's an interesting mental model progression that's happened over time and it's not that we go back and revisit all data types and force them into new mental models as we evolve. But you may have sort of coexisting and competing and different kind of models, and I think Jennifer's use of the word "context" is really important here as well as we're thinking about, you know, what role do legal frameworks or what role do sort of norm-setting frameworks play.

And it's important to keep in mind that at the end of the day, it's really how people are using something, how people think of it, what's intuitive for them. That also needs to be prioritized and also needs to be considered in terms of making a system that responds to those needs.

MS. YODAIKEN: Okay. We're going to switch gears slightly using a hypothetical that you all are familiar with, and it's in front of you somewhere to

see how you would actually apply this and what you think is most important here.

So basically Company X is a video game company. It allows gamers to join group games, make in-app purchases. It collects some information directly from consumers, email, user name, country, profile picture. Users can build profile pages, allow other users to comment, tag photos, private message. And as consumers interact with the games and other players, the company collects metrics about purchase transactions, history, games played, screen time ranking, maybe even IOT device use and scores. The company generates inferences about the consumers, such as skill level, low/high, in-app purchaser, risk taker, and the likelihood that the consumer cheats.

MR. HO: So that was a lot to take in and absorb. But I think we just wanted to, at first, focus in on access and sort of tease that out a little, but, in fact, try to figure out what the different levels of access that the company should provide to consumers for the, A, data that is directly collected about the consumer; you know, B, the data that is shared; and then, three, you know, the inference data that’s generated by the company.

So, you know, we’re drilling down from like

the abstract question that we had to a more specific one. So anyone want to kick us off?

MR. CALABRESE: Sorry, I was going to kick us off with something -- some of my staff actually play video games. I'm not that cool.

(Laughter.)

MR. CALABRESE: So this is not -- it turns out not actually that hypothetical, right. And somebody immediately pointed out to me that there was an article recently where a gamer figured out that he had spent about $10,000 over two years playing FIFA Ultimate, which is a soccer game. He found that out using his access right under the GDPR. And that was almost all in a micro-transaction, very small dollar purchases that came in the game format. So you could immediately say, boy, that's a useful piece of information, right. I might want to spend that money on something else.

You know, it's hard to necessarily know that as kind of like in the moment. But using that access rate, you're able to really unpack valuable information for you. I think that kind of example says, oh, okay, like I might even want to build a little app on top of it that says, you've reached your $500 limit for the month, you know, maybe you should

not have any more micro-transactions for a while.

MS. BARRETT GLASGOW: Can I respond to Chris before I go into the question?

MR. HO: Of course.

MS. BARRETT GLASGOW: I think you're right. It's great to have that kind of knowledge. I'm not sure a right of access is the right way to get it. I would separate business functions from the kinds of privacy rights that we're talking about here. That would be my only comment.

MR. CALABRESE: I'm sorry, you think the consumer should get it, but you wouldn't call it an access, right? Help me understand what --

MS. BARRETT GLASGOW: Well, I think, you know, maybe the app ought to have a feature that shows you, you know, your billing. I mean, think about any other kind of billing statement that might come from a company. A right of access is probably the least frequently used reason to get that kind of information.

But let me go back to the question at hand. I think it's great that we're beginning to look at the different types of information. Information provided by the consumer, information that is generated by the interaction through the company, information that's

observed and then information that's analytically derived, like maybe the cheat score.

Each one of those has some different dynamics that I think need to be taken into account. And this is where things like privacy by design and other things can really come into play when the app is launched and people are beginning to use it. To talk about access to the data that's collected by the consumer, you know, yeah, that seems reasonable. I provided it. I may not be particularly interested in it because I provided it and I know what they've got.

What I tend to be more interested in is the data collected through the interaction. But interactions have an interesting dynamic in that that data is constantly changing. Every time I get on and play the game, my costs go up or the charges to me go up. So the question becomes what is meaningful to the consumer in terms of access to a piece of data that by the time I get it and have a chance to think about it, it has changed potentially or it's moved on to something else. That creates an interesting dynamic.

I think someone in the earlier panel mentioned we haven't figured out the rules -- I think it was Pam -- about artificial intelligence, and while this may not be an artificial intelligence

application, it has some of the same dynamics that we will have to work through, and I don't know that any of us on this panel have that answer today.

When you get into photos and messages, now you get into some of the shared data issues that we're talking about. Then the risk taker, I guess as I was thinking through my answers on some of this, is any of this data shared with a third party or not? That was not specified in the scenario. I think it would alter my answer if it was or wasn't to potentially a small degree.

MR. ROSSI: So, unlike Chris, I am cool and I play video games.

(Laughter.)

MR. ROSSI: I think -- and I play FIFA. I think that -- I don't see any scenario in which -- I don't see why consumers shouldn't have access to all this information, right. They observe, they infer. I think that it's valuable for consumers. Maybe there are some situations in which it's not. I mean, maybe it's bad for -- very negative for the security of the service to allow a user that is a cheater to know that the company knows that user is a cheater. Maybe that information should be withheld, right, but that should be on a case-by-case basis, and then again, it would

be useful to have legislation and oversight.

I think it gets more [indiscernible] when we're talking about a correction, right? So maybe you should not be able to change, in this case, your skill level, right, on correction because that affects the gaming experience. But, for example, in the case of credit rating services, if they have the wrong number for your income and that's affecting your ability to get a mortgage, then maybe you should have the right to correct that. Maybe the right shouldn't be just a click, but maybe you should provide some documentation, but it should be there. The same with the rights on -- with deletion.

And I think that we should consider different cases, right? Like if you are -- you decide you that you don't want to play FIFA anymore, you want to go and play Pro Evolution Soccer, which is the other big game, you should have the right to delete the information that EA Sports, the company that makes FIFA, has from you, or at least most of the information that is not necessarily for the operation of the service, which at the same time it's very reasonable to argue that the information that will be necessary for the provision of the service and proof of service could be anonymous. So it shouldn't be

identifiable data anyway. So it shouldn't be within the realm of privacy protection. And that should be a case as well.

So to Jennifer's point --

MR. HO: I'm sorry, can I interrupt real quickly? I just want to ask one question and then, Jonathan, you can respond.

You mentioned the deletion issue. What about like in this scenario the likelihood that the consumer will try to cheat? Should they be able to delete that information?

MR. ROSSI: I think that, again, that should be a base for if the organization perceives that it's a consumer that is starting to cheat and it's harming the experience for the rest of the consumers. Maybe that's a base for not deleting that piece of information. It shouldn't be an all-or-nothing situation. So understanding that there are like significant nuances and an organization should have the right to balance the rights of consumers with other priorities, but that's a case-by-case basis and that should be forced by an agency.

MR. CALABRESE: I would just offer -- so we talked to some game developers. They said they view this as a cost of doing business. It's anecdotal.

But they view letting people delete it and then having to reidentify it is just a cost of doing business, just for whatever it's worth.

MR. HO: Jon?

MR. AVILA: Just to maybe note a broader point here, I mean, this is essentially a social networking site. That's what gaming sites are. And I think access, correction and deletion rights as opposed to portability rights are different. Access, correction and deletion rights are essentially reflecting the autonomy interest, the traditional data privacy interest of individuals in the controller's use of the data.

Portability rights are different. They recognize what essentially is a sort of quasi property interest in the data. The ability of somebody to move the data from one controller to another controller and the use of those portability rights has a impact not just on the individual, but also on the transferor and the transferee controller, particularly in situations where the recipient controller might seek to incentivize the individual to do something that the individual would not have any personal interest in doing, and that through the use, for example, of sweepstakes entries or points and loyalty programs or

some other method that has very little cost, by the way, to the recipient controller.

So when you have that kind of incentivized portability, you have the potential for anticompetitive effects. I know that we've heard about the potentially competitive effects of recognizing the right of portability, and those may be particularly appropriate in social networking and gaming type situations. But in other situations where what might be ported, particularly on a mass basis, if somebody is incentivizing a whole group of people to do this portability, what you can get is access to what effectively is proprietary and potentially competitive information, pricing, quantity sold, the SKUs that are sold. And that sort of information I think that you have the potential for entrenching dominant market participants if they can offensively use incentivized portability rights against their competitors.

So I think if we look at portability rights, there is a valid justification for limiting them to a narrower scope than we have access, correction and deletion rights to defeat that sort of incentivizes portability and to defeat the anticompetitive effects. So in this circumstance,

this is effectively a social networking site. I think it's totally legitimate for somebody to say I contributed photographs or, you know, whatever you do, I don't do social networking or I don't do gaming, but whatever you do on gaming sites that would be considered user-generated content that may be perfectly appropriate that you be able to move that. But in other situations, we shouldn't mistake the potentially anticompetitive effects.

MS. RACE BRIN: Can I just make one more quick point about the cheating? So, I think it's important to note that both -- you know, I know at least GDPR and FERPA distinguish when an individual has a right to correct their data. There's carveouts for things like opinions, right? So I know ICO guidance has said, look at whether something is a underlying fact or whether it's an opinion about an individual, and opinions, there may be less of a right to correct that. The same with FERPA. It specifically says that the right to correct a student record can't be used to challenge a grade, an opinion, a substantive decision made by a school.

So I think it's important to have these boundaries in place when we're thinking about what exactly correction should reach.

MS. YODAIKEN: Okay. Well, these are obviously areas where you guys and many people here and online can talk about for a long time, but we have approximately five minutes left. So one minute each on your final thoughts of what we should take away from this, starting with Gus.

MR. ROSSI: Okay. So I think that one of the key takeaways is that these rights serve to empower consumers, bring symmetry to the marketplace and make the marketplace more sustainable, bring consumers back in control with their personal data, enable watchdogs to protect consumers, to challenge the behavior of organizations big and small, to question data hoarding. At the same time that we should be aware that in the absence of a comprehensive privacy baseline and strong enforcement, it is unlikely that these rights on their own would provide -- would have the effects that we expect them or we wish them to have.

So we should think in context. As we were discussing all this panel, there are going to be cases in which these rights should be limited and that's -- that's five.

MR. HO: Okay, we're going to have to pick up the pace.

MS. LANGE: Was I being told to talk faster? Because that is not something I struggle with.

MR. HO: Yes, please.

MS. LANGE: So actually the one sort of point I wanted to add -- and I agree with Gus -- is that there -- and I suppose Google has sort of been a leader on some of these issues by the nature of the products we offer. I would just note that people do use these products. Sort of an interesting example is the ad settings. So every hour, every day, an average of 30,000 people are visiting Google's ad settings and just under half of them are actually making changes, including correcting their interests. And I'm saying correcting because it's not a deletion; it's a correction. You might be learning you affirmatively don't want ads for this thing.

So it's really -- it is something that I think it's easy to discuss in the abstract or in the concept of frameworks. But at the end of the day, really it's important to understand that people do use the tools that you build if you build them in a thoughtful way and it does yield useful information for you. And if you're paying attention and you're learning from what's happening, you can improve things over time in a way that benefits everyone.

MS. BARRETT GLASGOW: Just a couple points. I'll reiterate what I started with. I think context and reasonableness are kind of overarching principles that have to be applied here, and I think we've given lots of examples of that during our discussion. I think we're evolving whether we intend to or not. And I think we should be more intentional about this to more industry or use specific kinds of guidance that actually accomplish something as opposed to just putting an administration burden on companies that really doesn't satisfy the objective that's intended.

And while we didn't talk about it today, I just want to highlight it should never increase the security risks of an individual however we go about trying to balance and maintain those.

MR. CALABRESE: This is a unique opportunity to empower consumers, to give them the information they want, to build new services, and to essentially create the framework we're going to be using for the data economy over the next several decades. Let's make it a broad, comprehensive right that serves consumers.

MS. RACE BRING: So I think it is a really important right and tool for consumers for transparency. I think that we also need to include

reasonableness and balance, that it needs to be balanced against the rights of other individuals, against needs from an organization to maintain data that are legitimate and good reasons to maintain data. So we need to factor all of that.

MR. AVILA: And I would say that these are important rights. In the business community, we recognize the respect for customer's data privacy is an essentially element of building customer trust and that customer trust is the foundation of customer loyalty, which is essential to business success. I agree that these are very important rights and that they do require reasonableness and balance and a proper regulatory guidance and a time frame for complete implementation.

MR. HO: Great. With that, a minute to spare, we will conclude the panel. Thank you, the panelists, for terrific thoughts and great conversation. We will return at 1:00 p.m., after the lunch break with remarks by Commissioner Slaughter. Thank you.

(Applause.)

REMARKS - REBECCA KELLY SLAUGHTER, COMMISSIONER

MS. JILLSON: Welcome back. We have a full afternoon schedule today, during which panelists will be discussing topics such as accountability and the adequacy of the FTC's current toolkit.

But, first, FTC Commissioner Rebecca Kelly Slaughter will provide some remarks. Commissioner Slaughter was sworn in as a Federal Trade Commissioner on May 2nd, 2018. Prior to joining the Commission, she served as Chief Counsel to Senator Charles Schumer of New York, the Democratic leader, advising him on legal competition, telecom, privacy, consumer protection and intellectual property matters, among other issues.

I'll turn it over now to Commissioner Slaughter.

COMMISSIONER SLAUGHTER: Hi, folks. Sorry for that brief delay.

Thank you so much for being here. Welcome back to the last half of our two-day hearing focusing on the FTC's approach to consumer privacy. I am Rebecca Kelly Slaughter.

I've had the pleasure of listening to and learning from each of our 11 hearings to date, but this, I must admit, I have enjoyed the most, and I

think it's been one of our most important. I want to thank all of our esteemed panelists who shared their insights and I also want to thank our Office of Policy and Planning for their tireless work on these hearings and BCP's Division of Privacy and Identity Protection for their leadership in planning this event, in particular, Elisa Jillson, Jim Trilling, and Jared Ho.

Before I begin, I want to note that my remarks today reflect my own views and not necessarily the views of the Commission or any other Commissioner.

I'd like to use my time today to speak briefly about three aspects of the FTC's approach to consumer privacy that I see or hope to see evolving: The role of notice and choice, the integration of competition and consumer protection concerns, and FTC authority and resources.

Let's begin with the limitations of notice and consent, or as it sometimes seems, I didn't really know and I had no choice but to agree. The notice and consent framework began as a sensible application of basic consumer protection principles to privacy. Tell consumers what you're doing with their data and secure their consent.

But in order for a notice and notice consent regime to be effective, both elements must be

meaningful. Notice must give consumers information they need and can understand and consumers must have a choice about whether to consent. I am concerned that today when it comes to our digital lives neither notice nor consent is meaningful.

By now, we've all heard the estimate that it would take 76 working days to read all the privacy policies one encounters in a year. It's no wonder then that a more recent study from 2016 demonstrated that 98 percent of potential users of a social media site had no problem clicking "I agree" to privacy policy and terms of service that disclosed sharing with the NSA and paying for the service by signing away your firstborn child. As an oldest child and as a parent, I have to assume this was a close reading failure and not an indictment of the strong and spirited dispositions of so many firstborn.

(Laughter.)

COMMISSIONER SLAUGHTER: Another study showed that a majority of Americans believe that when a company merely posts a privacy policy it means that the company does not share user data. These studies and myriad others simply validate what we all already know. Clicking through these policies presents little value to consumers. They are often long and

confusing, and even when they try to be more succinct, their sheer number places an insurmountable burden on consumers trying to navigate the marketplace.

I'm not saying the privacy policies don't have value. They do. At their best, they force companies to think through how they are treating consumer data and publicize that promise. This is beneficial to the company, to researchers, and to law enforcement, but it provides little to immediate benefit to the consumer trying to access the services she needs while maintaining some control over her privacy.

Furthermore, as we've heard several commenters note over the last two days, we cannot consider click-through consent to present a meaningful choice. The choice is illusory because even if a consumer could read and understand the notice, she often has no choice but to consent in order to reach a digital service that has become necessary for participation in contemporary society. And as the panelists discussed yesterday, even where it appears consumers have given validated consent, that agreement might be a product of manipulative dark patterns. And I just pause to note that in a fortuitous coincidence of timing two Senators introduced a bill to deal

exactly with this issue of dark patterns just yesterday.

It is easy to decry the limitations of the notice and content framework and far harder to reach a conclusion about what should replace it. We could adopt the GDPR approach of trying to cure the problem by presenting more useful information to consumers more plainly. The jury is still out on its effectiveness, but no doubt improved notice and consent over specific practices could and should be debated as part of a US privacy framework going forward.

We could also look to the CCPA's requirements to present consumers with meaningful opt-out choices particularly over the sale and transfer of their data. Or we could impose more concrete purpose limitations where data can only be used by a company for the purpose for which it was provided. The rich debate on this topic this morning and yesterday demonstrates that there are a number of paths to improve the current framework.

In the midst of this debate, I want to put my thumb on the scale for solutions that do not place all or even most of the burden on the consumer. It is the job of the entity collecting, transferring or

using the data to accurately and fairly assess consumers' expectations how their data will be used and to meet those expectations. If the company misuses the data, law enforcement needs to be able to step in to hold companies accountable.

I also want to advocate for solutions that deliver consumers meaningful choices, which require policy holders to consider both consumer protection and competition concerns. The FTC is lucky to have both competition experts and consumer protection experts working together in one agency. Many of these hearings have underscored how intertwined traditional consumer protection concerns are with competition concerns, particularly in the area of data privacy.

The limitations of the notice and consent framework is one such area that raises both concerns. We'd all rather live in a world where digital platforms compete for users on metrics such as privacy, but today consumers often need to cede all control over their data to participate in or use certain service that have become critical to their everyday lives. They don't have the option to turn to a competing more privacy-protective service. This dearth of real choice is a privacy problem, but it is also a competition problem.

Lack of choice is not the only area where privacy and competition concerns collide. The increased risk to consumers arising from consolidated pools of data also raise competition and privacy concerns. In today's economy, when two firms combine, they are also almost certainly marrying large of amounts of personal data as well. Does the emerging firm have the ability to manage that data or related technology safely? Did consumers expect when they share data with Company A that it might one day be combined with data shared by Company B? And will the emerging firm use the combined data sets in a manner that is consistent with consumers' original expectations?

And perhaps most obviously, developing a national privacy framework necessitates balancing competition and privacy goals. We must take care that in attempting to secure increased protection for consumer data privacy, we don't inadvertently further entrench incumbents or otherwise hinder competition and choice. This is a concern that has been expressed frequently by those who oppose new privacy laws. I agree it is a concern, but I do not agree that it means we should stick with the status quo, which provides limited protection of privacy and limited

competition.

As these hearings demonstrate, the FTC is already moving toward more blended debates and dialogues about these issues. I am particularly optimistic that this trajectory will continue through the Chairman's new technology task force, which will leverage both our antitrust and privacy expertise.

Finally, I want to conclude today by spending a minute on the FTC's authority and resources devoted to consumer privacy. One of the questions posed around this hearing is what should the role of the Commission be in the privacy area. The FTC serves many roles. Business counselor, consumer educator, researcher and advocate, but our most critical role is that of enforcer. Thoughtful policy debates and balanced legislation will be to no avail if the resulting statutory framework does not provide for serious enforcement mechanisms and resources to incentivize compliance.

Today, the FTC's privacy enforcement centers around a handful of sector-specific rules -- FCRA, COPPA safeguards and our Section 5 unfairness and deception authority. Our rules allow us to protect children's information online and to help ensure that nonbank financial institutions and the CRAs are

protecting consumer data. But it leaves some gaping holes. Large categories of personal data are not covered by our rules, what we share on social media, what we share with many retailers, including our largest online retailers, and what we share with apps and devices even when we share personal health or relationship information. And this is the data we intend to share.

When our data is harvested and collected without our knowledge or expectation, in most cases, our rules don't cover those practices either. Even when we do have specific rules in place that does not guarantee that we have penalty authority. For COPPA and FCRA we do, but we have no penalty authority under the safeguards rule.

In order to protect consumer data and privacy beyond the narrow fields covered by our rules, we must rely on our Section 5 unfairness and deception authorities. The FTC has been nimble and aggressive in its attempts to use this 100-year-old statute to police today's technology-driven marketplace with many successes. But we face real limitations proceeding under Section 5. We cannot seek monetary penalties for data and security privacy violations in the first instance generally and quantifying consumer injury in

terms of dollar amounts is challenging. Moreover, without specific statutes or rules defining practices in this area, both courts and companies have been left with questions about whether particular behavior is prohibited.

Because of these limitations, the majority of the Commission supports the enactment of a comprehensive federal privacy law that does three things in terms of enforcement. First, empowers the FTC to seek significant monetary penalties for privacy violations in the first instance. Second, gives the FTC APA rulemaking authority to allow us to craft flexible rules that reflect stakeholder input and can be periodically updated to keep up with technological developments. And, finally, repeals the common carrier nonprofit exemptions under the FTC Act to ensure that more of the entities entrusted with consumer data are held to a consistent standard.

But the single biggest change that would help the FTC in its role as enforcer of data privacy laws right now would be an increase in our resources. We currently have about 40 full-time and fully dedicated employees devoted to privacy and data security. We have five full-time technologists, most of whom serve all of our consumer protection missions

not just data privacy. The UK Information Commissioner's Office, by contrast, has 500 employees. The Irish Data Protection Commissioner has over 100. We have a much larger jurisdiction, both subject matter and geographically, and blunter tools than our European colleagues, yet we have a fraction of the personnel.

The FTC's current annual budget is $306 million, and like most organizations, our greatest expense is also our greatest resource, staff. Approximately two-thirds of our current budget is allocated to pay and benefits for staff. If the FTC received an additional $50 million in ongoing annual funding, we could hire approximately 160 more staffers. An additional $75 million would enable us to bring on board 260 more staff members. That would, incidentally, put us around the staffing level we had in 1982 before the internet and still well below the levels in the late 1970s.

With increased staff, the FTC would be able to devote more resources to enforcing our existing rules and any future privacy rules. We would also be able to expand the number of staff dedicated to conducting compliance reviews of our privacy and data security orders. We would be able to do more than

just react to the worst behaviors in the marketplace. Additional staffing could be used to generate additional research or original research, conduct 6(b) studies of industry and, of course, focus on strategic targeting, investigation, and case generation.

The threats to privacy that consumers face in the marketplace are growing and grow ever more complicated. Our budget has not kept pace with these developments and our future as an effective enforcer in the area of data privacy hinges on an expansion of both our authority and our resources.

I thank you again for letting me participate in today's hearing and I look forward to hearing more on this topic from our experts this afternoon discussing their views on the adequacy of the FTC's toolkit.

Thank you very much.

(Applause.)

PANEL: ACCOUNTABILITY

MR. COOPER: Hi, welcome. Welcome to this afternoon's panel on accountability. I'm James Cooper, the Deputy Director for Economic Analysis in the Bureau of Consumer Protection. And moderating along with me is Andrew Stivers, who is the Deputy Director for Consumer Protection in the Bureau of Economics. So we're sort of like doppelgangers. I can't believe we're together on the same stage and not annihilating each other. But, anyway, the symmetry is eerie.

Anyway, we're here today to talk about the concept of accountability. We have a great panel and we have limited time. I'll just give very, very brief introductions. Their full bios are in our program.

So right to Andrew's left is Marty Abrams. Marty is Mr. Accountability. No one has been involved in this or thought about this as long as he has. Currently, he's the Executive Director and Chief Strategist for the Information Accountability Foundation.

Next to Marty is Dan Caprio. Dan is the co-founder and Executive Chairman of the Providence Group. He's an expert in transatlantic data transfer and he used to be an advisor to Commissioner Orson

Swindle here at the FTC.

Next to Dan is Mike Hintze. Mike is a partner at the Hintze Law Firm PLLC, and prior to that, he spent 18 years at Microsoft where he was the Chief Privacy Counsel.

Going down next to Mike is Corynne McSherry. She is the Legal Director at the Electronic Frontier Foundation.

Ari Ezra Waldman is next to Corynne. He is a Professor of Law and the Director of the Innovation Center for Law and Technology at New York Law School.

And then, finally, at the far end is Karen Zacharia. She is the Chief Privacy Officer at Verizon.

Again, so we have a great panel. What we wanted to do to kind of set the stage is ask Marty to tell us a little bit about accountability. Again, there's probably no one who is more associated with the notion or has studied this longer or been involved in it longer than Marty. So what I was hoping is if you could just briefly tell us about accountability. How does it differ from other approaches? What does it really mean to a layperson?

MR. ABRAMS: So first of all, thank you to Andrew and to James and to the Federal Trade

Commission for letting me be here today. Markus was here yesterday. He did a very good job of laying out accountability and so maybe he is Mr. Accountability and I'm just the guy whose been doing this for 30 years.

When I think about accountability, why is accountability important to individuals? It's because the highest and best use of data is creation of knowledge, and the fact is it's new knowledge that drives the innovation, which has distinguished the digital marketplace in the United States from digital marketplaces everyplace else. By the digital marketplace, I don't mean digital advertising. While that's part of it, it's not really it. The digital marketplace is smart cars, the digital marketplace is personalized medicine. The digital marketplace is all of the things that we do with knowledge and data that we were not able to do so before.

And the concept of digital knowledge and the knowledge creation drives what we refer to as inferred data. Inferred data is new data that comes out of the insights that come from discovery using data. I can't think of another way of making sure that that's done in a legal, fair and just way other than through the concepts of accountability and how accountability

works.

Think of the fact that accountability, as we've defined it since 2009, is really about organizations being responsible with what they do with data and then being answerable for being responsible. And both sides of that equation, both being responsible and answerable, are incredibly important.

There was something called the Global Accountability Dialogue that met first in 2009, and it was the Global Accountability Dialogue that defined the modern concepts of accountability which were laid out first by the OECD guidelines in 1980. There are five essential elements of accountability. The first is that organizations have to self-assert that they are accountable, have the policies to truly be accountable. Those policies need to be linked to external criteria.

As my friends at Federal Trade Commission know, if you self-assert, you're then subject to Section 5 of the FTC Act. So no one should say accountability is a self-regulatory system. It's not actually a self-regulatory system. It's a system of organizational governance that then has oversight that goes behind it.

The second essential element is that you

have the mechanisms to put those policies into place. And those mechanisms include the things that we traditionally think about, such as education for staff, training, procedures, et cetera. But it also includes the concept of doing a risk assessment and a risk assessment on what your use of data means to all of the stakeholders who are impacted by that data, not just me as an individual, but all individuals and society as a whole. So organizations need to be able to do that risk assessment.

The third essential element is that organizations need to have an oversight process that goes along with all of the mechanisms that go into place to make sure that those mechanisms actually work. Part of that oversight process is oversight over those risk assessments to make sure that they're done with competency and done with integrity. So the fact is that the internal oversight process is separate from the process of doing privacy by design, for example.

The fourth is that the word "knowledge" and the understanding of the public are important. So you need to have a means for individual participation in the process. So it requires transparency, it requires access and correction where that's appropriate for the

process. It requires that you listen to the voice of the people. It means that, in some cases, you do research on individual concepts and ideas. In some cases, it means you bring in experts. But the fact is that you to have the voice of the people.

And the fifth is -- and this is one of the most important -- is you stand ready to demonstrate your accountable process. By being able to demonstrate that accountable process, you're open for the type of criticism that allows you to know that what indeed you're doing with data is acceptable, it's legal, fair, and just.

Now, there are a number of companies in this room that truly have embraced this concept of accountability. This morning when it was mentioned privacy by design, organizations that do that privacy by design are actually fulfilling one of the requirements of accountability. But if you were to say are most companies at this point -- have they embraced accountability? Do they even understand accountability? In our work, we find that most organizations have some of the elements of accountability, but for accountability to be fully effective, there needs to be a comprehensive program that has all of the pieces of accountability and an

understanding of how those pieces link together.

As Markus mentioned yesterday, the general data protection regulation in Europe actually requires accountability and within the law it has all the elements of accountability, but it never draws those pieces together. Until companies and organizations understand what it means to be an accountable organization and understand how they are going to report to the public on how they are indeed being accountable, then we'll always have this gap.

So let me quit there and say that really what we need to do as part of improving the process is having a description for organizations of what it truly means to be an accountable organization.

MR. COOPER: Thanks. And I just want to just follow up just a tiny bit. So just again -- and this is coming from someone thinking as an economist. I hadn't really thought about accountability as a term of art in privacy as it is. Does accountability -- is the teeth behind accountability ultimately some legal authority? And what does the notion of accountability add to, leaving aside, say, the GDPR which explicitly requires it, but if you think about Section 5 or if you think about the other regulatory regimes throughout the world, what does accountability add

that perhaps would be missing in current legal regimes?

MR. ABRAMS: So the ICO, which is the privacy regulator in Europe, had a meeting with 1,000 businesses on Monday of this week on what she is looking for in terms of privacy compliance over the next year. She said to those folks, she says, if something goes wrong and we come into your house as part of an investigation of an enforcement action, the first thing we're going to ask you is to show -- for you to show us your comprehensive privacy program to establish accountability. For her, the first step in investigation is saying, let me see your program, let me understand your program.

Spain amended their privacy law in 2011 to give the regulator the ability to reduce fines for organizations that were accountable if they had an oops and had something go wrong and it's not a systematic mistake.

So the fact is your own consent orders here at the FTC require organizations to be accountable. So you require that for organizations that have had an oops, but not generally for the market. So the fact is that accountability is about taking organizations to account. Part of accountability, I believe, is ex

ante processes, and maybe if we have time, we can discuss that later. But it's really about the requirement that organizations understand what they are doing with data, understand the risks associated with it, mitigate those risks for other parties that are involved and having the ability to describe that.

MR. COOPER: Thanks.

Andrew?

MR. STIVERS: So as an economist, I'm interested in sort of how the market interacts with this particular concept. At the FTC, we often look at the world as sort of trying to make markets work. And I wonder, Ari, if you can address or give some thoughts on, you know, what is it about this particular set of responsibilities that Marty laid out that isn't part of the -- or maybe it is part of the standard sort of accountability that consumer-facing firms always have to their customers? If they don't offer a product that consumers want at the price that they're willing to pay, then they're held accountable. So can you help us understand what else is going on here, if anything?

MR. WALDMAN: Sure. So thank you, first of all, for inviting me to participate and thanks for everyone for coming. Thanks to the FTC and to our

moderators, James and Andrew.

I'm going to talk for a few minutes about why the market is incapable of adequately allowing consumers to hold companies accountable. There are really three main reasons why, and after going through the reasons, I'm going to suggest a little bit about what we might do in order to address some of those gaps.

The first reason are information asymmetries. Efficient and fair markets require awareness and information on both sides. Consumers need enough information to know if a salesperson is offering them a lemon or bad product or a massive data collection scheme is hiding behind a friendly interface. Instead the digital marketplaces that we have are characterized by enormous asymmetries of information. Technology companies know every single detail about us. Their ability to martial large data sets to identify unique and unexpected correlations in that data allows them to identify what they think we like or what they think we want to buy and tailor our online experiences.

On the other hand, as Frank Pasquale has noted, we have very little background knowledge about how all of that works, what they know, how platforms

use and gather and manipulate and analyze our data. We don't know the correlations between our behavior on those websites and the ability of these companies to create virtual personas of us. Therefore, we don't really know what we're giving up in exchange for the convenience that the digital marketplaces or social networks provide.

A second barrier to market solutions to this problem are psychological barriers to rational choice. Even if we did read those long and legalese privacy policies that so many people here today and yesterday have dismissed as -- have correctly dismissed as completely garbage, we couldn't adequately translate what we learn into a rational decision as any neoclassical model would require. We are all susceptible to what psychologists like George Ainslie and David Laibson have called hyperbolic discounting or time inconsistent preferences. That's our inability to adequately weigh the potential of future risks and rewards against the reality of current rewards.

We are also terrible at what Dan Gilbert calls effective forecasting or assessing our feelings about what will happen in the future relative to today. So if we can't adequately access the potential

of future risks as against the reality of current rewards, either convenience or some minimal reward of using -- of having your name or a cookie -- having your name remembered or a cookie dropped on your computer, how are you going to be able to translate that into rational decisions about our privacy?

That important point leads to the third reason why there's no market for privacy preferences and why the market can't solve these problems. In fact, the market is designed out by the technology companies themselves. We operate in online environments that are designed for us and, in fact, are designed to manipulate our autonomy and maximize our data disclosure. Design is a powerful force that constrains our behavior in a space. You can't make fully rational choices when the environment doesn't let you.

As Woody Hartzog has stated in his latest book, Privacy's Blueprint, the realities of technology at scale, and I'm quoting here, "mean that the services we use must necessarily be built in a way that constrains our choices." Technology companies have their own agenda and that is to collect as much data as possible. And as they are the ones in charge of designing the environment in which we interact with

them and with other people, it will always be designed in ways that facilitates their business success, not our needs or human flourishing. Design nudges us to behave in certain ways. They make us feel guilty when we don't engage and leverages are innate desire for popular feedback or that little thumbs up and takes advantage to our attraction to bright, shiny buttons that say click here and move on.

The point is not that design is bad; the point is that when technology companies have control over design, we, who are their subjects, are not in a position to make fully autonomous, independent, free choices even if we read, understood, and were able to operationalize the privacy policies that they offer us. Given this, technology companies know that there's little risk of users not choosing to share their data. Given the current legal regime, little risk the companies will be held accountable, when users finally realize what happened and then voice their displeasure of being manipulated as so many stories over the last couple of years have shown. So if there is no market for -- if the market can't solve these problems, what does real accountability look like?

My concern with the approach of the five

accountability elements that we've just seen is that it doesn't always hold up on the ground. My research focuses on how technology companies implement privacy laws on the ground, and a lot of times the responsibility for privacy compliance is despite having, at least on paper, adequate systems, structures in place, audits and offices and so forth, all of the things that would meet all of the five requirements of the accountability regime. A lot of those responsibilities are outsourced to privacy technology vendors, to engineers who are trying to create -- who are there to create easily codable or easy-to-use solutions, supposedly easy-to-use solutions that are, as a result, undermining the promises of privacy law.

So what would a regime with real accountability look like? I'll just list a few and then end here and we can move on. I think some of the things that have been said here over the last couple of days and in the Commissioner's brief speech before this panel are correct. A legislative approach must shift the burden of protecting privacy from the user, who can't protect her privacy, to the company, who is in a much better position to. A new legislative approach should deploy fiduciary obligations on

technology companies, as Jack Balkin, Neil Richards, who is here, Woody Hartzog and myself and others have argued, and permit private rights of action when data is misused.

One of the problems that we've noted is that the FTC is understaffed. We need to up the FTC's staff, but to exclusively rely on FTC enforcement when we take away private rights of action is going to be unreasonable.

A legislative approach should incorporate purpose limitation and data minimization which actually are some of the requirements of fiduciaries anyway. A new legislative approach would require technologies be designed from the ground up in ways that chooses the most privacy effective design -- most effective design possible with the most privacy protective design.

A legislative agenda could also track the requirements of Sarbanes-Oxley and make technology companies executives directly responsible for signing off on privacy assessments and hold them liable if they mislead the public or fail to incorporate privacy protections from the ground up. The only way we're going to make a company that has contrary business interests to privacy protections to take our privacy

seriously is to hold them accountable.

A regulatory approach should double down on design. The FTC needs to put its muscle behind a consumer protection agenda that recognizes the manipulative power of design, as Woody Hartzog has argued.

Based on my own research, the FTC needs to look into making sure that its audits are real and enforced and followed up as opposed to permissive assessments that don't allow for any real feedback. A regulatory approach would consider executive public statements as part of a company's commitments to consumers, especially since highly publicized statements by highly publicized executives maybe in front of Congress, for example, are far more likely to become part of consumers' decision-making processes than something hidden in a privacy policy.

The FTC, as the Commissioner noted, needs fining power and easier rulemaking powers to enforce legislation to ensure the company's feet will be held to the fire.

MR. STIVERS: Ari, I'm sorry to interrupt you. We do have a number of other panelists. If you could wrap up and we can move on. I apologize.

MR. WALDMAN: And these are a few of the

steps that we need to put real accountability --

MR. STIVERS: Thank you.

MR. WALDMAN: Thanks.

(Laughter.)

MR. STIVERS: So thanks, Ari, and hopefully we'll be able to get back into that. But, again, we have a short time and several panelists. But I want to move to Karen next. As we think about accountability, we heard from Marty about what it is, what are key tenets; we've heard from Ari about how the marketplace may not provide consumers with the level of privacy they want. There are reasons to think that that may not be the case.

So we see, as Mary mentioned, accountability is specifically of the GDPR. Lots of activities kicking around on Capitol Hill thinking about -- I forget who it was yesterday -- one of the panelists said, you know, we've had our privacy moment this year, the US has had it and lots of legislation is kicking around on Capitol Hill. What do you think the role of accountability should be in any sort of US legal regime?

MS. ZACHARIA: Thanks for the question and thanks for having me here today.

I think in the US we really are at a

crossroads and we have two choices. One is we can continue along the path that we have today where we have some state laws that are governing data breach and privacy. We have some federal sector-specific laws. We have some self-regulatory regimes and then we have accountability programs in companies. Or we can say the time is now, we should have a federal privacy law. And I've been lucky enough to be in this job at Verizon for eight years, and the entire time that I've been at Verizon, we've been advocating for a comprehensive privacy law. And many of the elements of what we think should be in the law really are intertwined with the accountability principles.

I've sometimes described what should be in the federal privacy law as the equivalent to a really complicated maze and there are different ways to get out of it, but there's not just one path. So I'm not going to sit here today and say privacy law needs to have the following 162 provisions in it, but what I would like to do is spend a little bit of time talking about some of the overarching principles and, in particular, how those interrelate with the accountability framework that we're talking about.

So as I said, it should be a federal law, it should be comprehensive, it should apply to all

players in the ecosystem with one federal regulator enforcing it, which would be the FTC. The law needs to be flexible. And why do I say that? We want to make sure that this law can apply to the technologies of future, both the ones that we already know about, whether it's 5G, something that Verizon's rolling out, internet of things or new services and products that none of us in this room could even dream of today.

We also want to make sure that the law will take into account new approaches to protect privacy and it's not so prescriptive that if we have new methods companies can't adapt to those.

So if the law included some of the things that Marty mentioned earlier, things like training requirements or risk assessments, that's exactly what the law should say. Companies should do risk assessments, but it shouldn't then specify how it does those risk assessments.

Other accountability elements that should be in a law would include things like transparency and choice. Companies should be required to be transparent with their customers and to tell them the type of information that they're collecting and how they're using it. Companies should be required to give appropriate choices.

A law should also include accountability elements like data security and data breach. Now, a federal privacy law wouldn't have to include those if there was going to be a separate data breach and security law. So it could be one law, it could be two laws, but we should have a federal law that talks about those issues.

A law should have safe harbor programs. Why is this important? We're dealing with some really complicated issues and sometimes the better way to work out how companies should act and what best practices are is to let companies come together, companies across industries, company advocates, but figure out what those best practices should be, include them in a safe harbor program that meets or exceeds the law, and then companies who follow the safe harbor program are deemed to be in compliance, similar to what we have today in the COPPA world.

Then last, but not least, I want to talk about oversight, another important element of any accountability program. Marty talked about making sure that companies have their internal governance structure in place. That is certainly an important element. And then we definitely need some kind of external oversight. And what we would recommend, as I

said in the beginning, is that the FTC be the federal enforcer. It should have additional civil penalty rights subject to caps and also that State AGs should be able to enforce it.

I think I want to conclude by talking a little bit about incentives. Companies like mine have every incentive to do the right thing by our customers. We know that customers are only going to buy our products if they trust us. So from the very top of the house, the C-suite is very, very focused on customer trust and on privacy issues. But I do think one of the reasons why it's really important to have a federal privacy law is to make sure that all companies are incented to do the right thing.

MR. COOPER: Thanks, Karen.

MS. ZACHARIA: Thank you.

MR. COOPER: So, Corynne, just to kind of follow up on -- Karen is talking about federal privacy law and how accountability would work in something like that. I want to drill down a little bit onto the notion of transparency and if there are any regulatory approaches you think that -- you know, how important is transparency to making firms accountable and are there any regulatory approaches to transparency you think make sense?

MS. MCSHERRY: Sure. So I think we could probably all agree that transparency's kind of job one. You can't have accountability until you have transparency, but I think it's important actually to drill down on what that means. It seems to me, at a minimum, transparency means you've got a window into the actual practices of a company, what it's actually doing as opposed to what it says in its policy and is there actually a match between those things.

But you need a little bit more than that. You need to have transparency into the ecosystem within which that company functions because we all know that the data doesn't just stay in one place. It moves all around and is shared across many different companies depending on the industry. So you need to have a window into that ecosystem.

And the third -- and these are all interrelated -- you need to have a window into the actual nature of the risk. So if I'm a consumer, it's very difficult for me to assess, which is part of the sort of choice problem, it's very hard for me to even know what I'm choosing and what my risks are and what the risks are for my data.

So if I go to Target and I use my Target card or whatever, I know that they know what I buy.

Do I know what they're doing with that information? Do I know who they're sharing it with? Do I know what they can infer from that information like they can infer that I'm pregnant or that I'm not or whatever, I'm an alcoholic, whatever it is? Am I thinking about all that? Probably not and it's probably going to be hard for me to do that, but I should at least have an opportunity to have a window into it or someone that I delegate to handle that for me because I agree, I think a lot of people are saying users shouldn't be in charge of all of this by themselves.

There's a lot of things I don't know. More importantly, I don't even know to ask and I think Commissioner Slaughter made reference to this earlier to the study that I think actually was in my home state of California that a majority of Californians believe that if your website had a privacy policy that meant they didn't share your data. So just the existence of a privacy policy somehow meant this entirely different thing. So they didn't ask further questions because they didn't think they had to. And they're busy people and have other things to do. I don't think we can blame them for not being perfect privacy lawyers.

Again, it's even more difficult for a

consumer to assess risk. So, for example, I might know a little bit about deminimization and I might know a little bit about anonymization and I might think, oh, my data will be only shared anonymously and that will be fine. Do I know anything about reidentification? Probably not, right? And as a consumer, I'm not in a very good position to assess that risk, but the company that's collecting my data probably is. So when we talk about companies being transparent and talk about their responsibilities, I think that's part of the responsibility because they are best placed to know that.

So, anyway, if accountability is supposed to mean anything, it seems to me all of that information has to be available in clear language to me as a consumer or to the expert that I delegate. So what can the FTC do about this? This is one of the things that I was asked to address. I think we're starting to overlap, so I'm going to be quick because I want us to have time for a conversation. But, right now, even before any additional work, it seems to me that FTC settlements could require much more rigorous audits and assessments that don't rely on management statements, but instead by careful investigation of actual practices in context.

I think that assessments and audits should be made publicly available more than they are. There may need to be redactions, but that way privacy scholars, for example, you know, people who actually do police privacy and help keep consumers informed, can do their work in a much more effective way. And I think that privacy policies -- again, privacy policies are terrible in many, many ways, but I do think that part of what they could include would be clear language about the actual risks to consumers so that they know what they're getting into.

But I would suggest that we need to go far further than that. So there should be some additional mechanisms that go beyond the FTC. So I would like to see really robust whistleblower protections so that people within companies who see -- have a window into what's going on feel more comfortable and safer letting the FTC or other regulators know or other lawmakers know because really it's the people on the inside that really understand how the data's being handled and it's not always easy for someone from the outside to do that.

I do think -- I think I've heard a couple people suggest this. I do think we should have a private right of action so -- for privacy harms. That

relates to transparency because one of the things that happens when you have a class action lawsuit is you have discovery and you have investigations and you have lawyers who are empowered and interested in really digging into what the company is doing.

And we don't have to dig into the preemption debate too deeply, but I do think that, for now, we really want a situation where there's lots of different regulators, like attorneys general, state attorneys generals who are empowered to do the kinds of investigations that we need to have real transparency and real accountability.

Now, the final thing I would just note, though, about transparency, in particular, is that -- I'll just state the obvious. Transparency is great, but this is low-hanging fruit, right. Transparency is just your starter point. All the knowledge in the world isn't really that useful to me if there's nothing I can do about it. So that's -- sort of we have to keep building in and that's why I think flexible rules and flexible procedures are very, very important. But they need to be meaningful. They need to be real sticks and not just carrots.

MR. COOPER: Thank you. Would anyone else like to jump in on the transparency issue or any

things that Karen put on the table as well as for what we may want to see in legislation as far as transparency or accountability goes?

MR. ABRAMS: So there is a concept that was brought up this morning that's a very important concept, and that is the concept of setting parameters for what are legitimate uses of data. And the fact is that part of establishing an accountability program is actually part of your assessment saying that you're within the range of legitimate uses. For those who know the GDPR, we're talking about the specification of legal basis to process. We find similar in the Brazilian legislation that recently passed. We would find similar in Argentina when they passed their new legislation. But that is -- but by specifying that, we still get flexibility organization, but we give some parameters around what is appropriate use of data.

MR. WALDMAN: Yeah, I agree with almost everything that Corynne said. I think the point about audits is incredibly important. The FTC says, in almost all of its consent decrees, that there will be an audit and it will be every two years after -- under the life of the consent decree. But, right now, they're not even real audits. They are assessments

that are based in large part on executive statements in regard to the questions that are asked. And I've read them. I've read these redacted ones as part of my research.

They quite literally say things like the requirement is that you are complying with Section 4(b) of the 2000-whatever consent decree and then it says, Please see Exhibit I, and Exhibit I is simply an executive statement that they are complying with Section 4-whatever of the consent decree. That's not an audit. That is just an attempt to create a smoke screen with no substance behind it. So if the FTC is really committed to making its enforcement powers all that it can be, that doesn't even require legislation. The FTC should just take seriously -- could simply first take seriously the powers that it does have.

MR. STIVERS: So transparency is, I think in this context, so far has been discussed as a very positive thing. One could take the privacy policies that various folks already pointed out issues with that, Commissioner Slaughter in her opening remarks, but I'm not sure that I'm quite ready to declare dead.

So, Mike, I was wondering if you could -- you have, I think, written about some of the benefits of the privacy policy. I wonder if you can give us

some of your thoughts on why maybe they're not completely worthless.

MR. HINTZE: Yeah, I would go even farther than that.

MR. STIVERS: All right, excellent.

MR. HINTZE: I have written on that. I wrote a paper a couple of years ago called, In Defense of the Long Privacy Policy. You know, privacy policies are maligned and criticized all the time. People criticize them for being too long. There was this famous study about ten years ago that said that if consumers had to read every privacy policy that they encountered over the course of the year, it would take 244 hours. We heard this morning that privacy policies have only increased in the last several years in terms of length.

A lot of this is tied into that general criticism about the inadequacy of notice and choice as kind of the foundation for privacy regulation. Lots of criticism that many privacy policies -- not the ones I've written, of course -- are confusing and opaque. I think, Ari, you referred to them as complete garbage. Certainly, there's some truth to that. You can find examples of very bad privacy policies out there, very bad privacy statements.

As a result, consumers generally don't read them. I think that's undebatable. Most consumers don't read every privacy policy they come across. But, nevertheless, I think they're very, very useful in creating accountability for a couple of reasons.

One, particularly if we can get away from this pressure on companies to make privacy policies short and simple, I think that's a really misguided pressure to put on companies. Because if they are detailed, if companies are forced to disclose or encourage or incentivized to disclose detailed information about what they're doing, the mere process of creating that document creates accountability. It forces companies to do data mapping, to do privacy reviews, to understand what data they're collecting, and the mere putting in place those processes inside of an organization can be incredibly useful.

Similar to other mechanisms that we're seeing in privacy laws, like under the GDPR, we've got the Article 30 record-keeping requirements and the requirements to create data protection impact assessments for high-risk data processing scenarios. Just that act of reviewing and documenting these practices can be incredibly useful. And the fact with a privacy statement that you have to post it publicly,

it creates that second step of pausing and saying, is this a story I want to tell? And if it's not, it encourages companies to adopt new mitigation strategies, to maybe improve their privacy practices in other ways so that they have a more complete, positive story that they can put out there.

And the fact that consumers rarely read these things, I think, is not a fatal flaw necessarily. There are other entities out there that do that can act as proxies for the consumers and put real pressure on companies more so than an individual consumer can. These are regulators and policymakers that might read them, academics and researchers, privacy activists, journalists, investors are increasingly reading these for startups that might be acquired or that they want to invest, and plaintiff's lawyers, obviously, are reading these as well. All of those actors have an ability to put pressure on companies to improve their privacy practice. So I think that creates absolutely real accountability.

But this only works if privacy statements are detailed. When you look at a lot of the other proposals that are out there to make privacy statements shorter or simpler, whether they are for nutrition label approaches or icons or other

approaches to privacy statements, I think those all fall short in this goal of creating accountability. Those who are pushing them have this idea that privacy can be reduced to these binary choices or very simplified facts and that's not just the reality of most environments where privacy is an issue.

If we're looking at sort of a binary choice, is data shared with a third party, well, that's not very interesting to me. What's interesting is what types of parties is it shared with, for what purposes and what protections are in place around that. Every time companies are sharing data with each other, at least every time I've been involved in it, there's a contract there and those contracts set out privacy and security obligations and restrictions on data use and those are the facts that are interesting. Those are the facts that create sort of the real -- whether there's a risk here or whether it's not, whether it's inappropriate or whether it's beneficial or whether it's harmful.

So if we try to simplify and shorten these things, it's just not going to create that kind of accountability, it's not going to create that kind of transparency that fosters accountability. So I'll stop there.

MR. STIVERS: I would be shocked if folks didn't have some comments they wanted to add to that. So let's open it up for discussion.

MR. WALDMAN: Yeah. I respect Mike and his work quite a bit, but I just think that's wrong. I mean, certainly there is a value to stating your policies and just as Corynne said, you know, transparency is important. But it's not the be-all and end-all. I would say that we ask too much of transparency and privacy policies. We expect that they provide us with the ability to make rational choices. There is nothing that suggests that we can't have one privacy policy that's long and detailed for regulators and other tools, not necessarily a privacy policy, maybe it's visceral reactions or other things that actually do tell users what's going on in a more acceptable or in a more psychologically driven way.

MR. HINTZE: And to be clear, Ari, I'm not claiming that a long privacy policy is the be-all and end-all. I absolutely agree with you that there are better ways and other ways to supplement that that are more focused on the consumer. Just-in-time notices, contextual notices, design factors, I think all of those are super important. But unless you also have the very detailed privacy statement, I think you don't

create that level of accountability because the contextual stuff is fantastic. But if you ever want to go back and figure out what the whole story is it's often very hard to recreate that context and find that information again.

So, again, the privacy notice may have another benefit of like being the one place you can go back to -- you know, say when you agreed or you went through a sign-up process, you didn't have a particular sensitivity and then something changed in your life and you did. It's hard to go back and go through that sign-up process again to figure out those choices you made or what you were thinking when you decided to use that problem. But having a long detailed privacy statement will have that information there.

I should have also pointed out -- I meant to point out -- that having a long is no excuse for crappy design. Things like layering and things like writing clearly, you know, avoiding legalese, all that stuff is important. People should be able to find the information that's relevant to them when they need that information and I think a privacy statement can foster that, but it's not the whole answer and it shouldn't be done by itself.

MR. WALDMAN: Well, I certainly respect that and I agree. I think that the long privacy policy has been used by companies, however, to absolve themselves of responsibility. So my concern would only be with -- I don't think we need to get rid of them. Fine, they're three. But my concern would be perpetuating the ability of technology companies to use them. Of course, in the ideal world, they would be a whole lot better, as you say, but perpetuating them as a false operation where companies are allowed to get away with everything because they know that no one's actually going to read that narrative.

MR. ABRAMS: So this isn't about the length, this is about what is in there. I just want to briefly say that I actually think going forward, when we use information people's common understanding, we should actually be talking about our values and judge us on our values and that should be part of what we're judged on. So I'm actually seeing longer, but that isn't about what's transparent to easily understand by the individual. It's part of the description of what you should be judged on and I'll just be quiet from there.

MR. COOPER: Would you like to add something, Karen?

MS. ZACHARIA: Yes. I think to some extent, you know, everybody is right here. I think we need both. I think we need the long policies for some of the reasons that Mike talked about and, Ari, for some of the reasons that you talked about. We also have to figure out ways to give our customers the information that's the most important to them. The problem is that's sometimes challenging.

Mike gave the example about sharing, right? I think all companies share information with third parties, right? You have to do that for all sorts of reasons. So figuring out how to explain the aspects of that that customers are most interested in is really what companies like mine have to figure out. And you're never going to be able to do it for all of your customers and to satisfy each of their needs because some customers are going to have different views on it. But at least if you can figure out what's most important to most of them and try to highlight that, I think that should be our goal.

MR. COOPER: Thanks. Any last -- Corynne?

MS. MCSHERRY: So this might be a place to interject something that I think is kind of complicated here. I think that a lot of times when we are talking about privacy in this context, we're

thinking of really straightforward consumer privacy, someone collecting information about what I buy. And we lose sight a little bit that privacy means a lot of different kinds of things that overlap. I wonder as we think about privacy policies, one of the things I think where they fail is they're not particularly good at grasping that and communicating that.

So just to give an example, so I might have a privacy policy that tells me your data, this is the kind of data that we're going to collect about you and here's how we handle it and I say okay. But I'm just thinking of that, and the company assumes I'm just thinking of that, in terms of advertising and marketing. Maybe I don't realize that this database can also be targeted by law enforcement or maybe I don't realize that this database can also -- I don't know -- if I'm in a messy divorce that there might be a subpoena for my information in connection with that.

So I've just sort of thrown a wrench in the whole thing, but I do think that as we're thinking about privacy and accountability, one of the things that we have to put on the table is understanding that privacy means a lot of different things. And we don't always unpack that as we're trying to think about -- as we're trying to think about consumer risk, for

example. So I just want to put that on the table.

MR. COOPER: That's actually a good segue to move to Dan, who's been a shrinking violet on this panel, strangely, but get you involved in -- draw you out a little bit and draw you into this conversation. Speaking of -- this is something you've thought about in the context of risk management and informational injuries, so the idea that privacy means different things to different people.

We talked a little bit about -- this was discussed on the panel I moderated yesterday and some other panels, this notice of informational injuries, that there are certainly some things we care more about than others and it's baked into at least the US law with children and health and so on versus broad commercial data security under Section 5.

Can you talk a little bit about how accountability mechanisms work in this context with respect to risk management?

MR. CAPRIO: Sure. And thanks, James and Andrew, and thanks to the FTC for including me.

As Marty mentioned at the beginning and Markus Heyder mentioned yesterday very eloquently, there are many accountability mechanisms to manage risk and there seems to be a consensus on the broad

contours of privacy accountability, the acceptance of responsibility for privacy protections, the ability to demonstrate that privacy promises are being met, effective governance that ensures an organization has the proper focus and resources to meet its privacy promises and, of course, compliance with law and regulation.

There's also a recognition that the use of risk management, that those approaches provide a sound foundation for developing accountability. Privacy professionals are now well-versed in many of these risk management concepts through the important work done by the National Institute of Standards and Technology, NIST, the National Telecommunications and Information Administration, NTIA, the Office of Management and Budget, and, of course, the FTC.

Some of the more well-known risk management concepts include organizational governance structures, such as the appointment of a chief privacy officer, the development of policies and procedures, the application and monitoring of privacy controls, and workforce training and education. These risk management tools are necessary for an accountable privacy compliance program, whether it's internally created to meet privacy promises made to consumers or

through government regulation, but they are not sufficient for a mature risk management program.

So why are they not sufficient? Too many risk management programs generally, and privacy risk management programs in particular, do not employ the tools necessary for thinking about emerging risk, that is risk that may not be recognized today, but may well become a reality in the foreseeable future. Why is it then that risk management programs tend to be limited to current, especially compliance risk? Well, the simple answer is because thinking about the future is hard.

There are tools, however, that can help and should be part of any risk management program for accountability. These tools have been tested in national security, corporate strategic planning, and product development. They include scenario development and analysis, war gaming and design thinking. Are these tools a crystal ball into the future? No. But they do help organizations overcome biases to imagine the possible futures in which they must operate and they help break down communication barriers between organizational functions and silos in order to plan for emerging risk effectively.

So I think accountability for privacy

management -- for a privacy management program to be fully accountable, it must not only ensure that it meets current compliance requirements, but it also must take into account the potential future impacts it has on privacy and society.

MR. STIVERS: So there have been a number of really interesting questions that folks have brought up and unfortunately we don't have all afternoon, though maybe we will take a little extra time if nobody minds. That probably won't work out.

But there are a couple questions that I would like to raise. One is one that I think is kind of lurking behind all of this, but we haven't really addressed it directly and I would like to get the panelists' input on this. We've been talking about the responsibilities, additional responsibilities that we think that firms should take on here. I wonder if the panelists could address the questions of cost.

As an economist, I have to bring this up, of course. It's in my contract. I wonder if the panelists could bring up what are the potential downsides of this regime? Are there none? Is this really sort of an everybody wins sort of situation? And if it is, then kind of why isn't it more widespread? Why are we having this conversation about

the requirement of accountability and just sort of saying, well, you know, it's all good, people are doing it? So I'll open this up to everyone.

Marty?

MR. ABRAMS: So bright-line rules that say you can't use data because we're afraid of the outcomes that come from the data -- and we see some of that in the GDPR -- is much more costly because that restricts our ability to create new concepts, new ideas, new insights, new ways of creating value. So, yes, having the operational elements of accountability in your organization has expense. It is much cheaper than giving up discovery of new ideas, new concepts, new knowledge that will then drive innovation. So this is much cheaper than bright-line rules.

MR. STIVERS: Dan?

MR. CAPRIO: So a couple thoughts, Andrew. This is sort of thinking at the senior corporate level. I think it's important for the FTC and for companies to think of data as an asset, number one. Number two, when you think about accountability, as I mentioned, that good risk management is not just about being compliant, that accountability tends to be a very good mechanism for looking backward, but we need to think of ways creatively to think of it as we go

forward.

And then three, I think we need to figure out ways or examine ways to incentivize organizations, to mitigate the risk of harmful uses or exposure to our personal data. And we had a whole panel yesterday on deidentification. So I think that's a fruitful area.

MR. HINTZE: I would say of course there's costs. It takes time and personnel and resources to put these kinds of measures in place. But it pales in comparison not just to the opportunity costs that Marty talked about, but to the costs of a privacy screw-up. I mean, once something goes wrong, the cost of dealing with that reactively is orders of magnitude greater than the proactive approach.

MS. ZACHARIA: The other kind of cost I'd like to mention is when laws aren't clear or when we get interpretations of laws, sort of too late, it becomes very challenging for companies to implement them or they go down one path or they spend a lot of time churning about one path and then there has to be a switch. So some kind of clarity is important and interpretations in enough time to be able to implement.

MR. WALDMAN: Near the kind of arguments

that Mr. Abrams made earlier about what some of the costs are in generation of new ideas and innovation, I think this whole conversation yesterday began with a presentation about how there were costs to innovation from privacy restrictions. There are tons of studies that demonstrate that that's not the case. Privacy regulation does not stifle innovation. There's a new paper by Katherine Strandburg coming out. There are papers each year from behavioral economists that show that there is no binary choice between privacy rules and innovation and generative ideas.

So I would caution us from taking that as an assumption, because even in the neoclassical model, what regulation is supposed to do is guide innovation, guide new ideas and new opportunities and guide opportunities to fill demand based on the values that society highlights.

MR. ABRAMS: So I'm not trying to suggest that you'd forget privacy, but anybody who's working with trying to make research work in the European context today knows what I mean about the lack of the ability to free up data for data-driven research because the rules are just designed not competently. So you can cite the research, I can cite the real on-the-ground results in Europe today.

MR. COOPER: In the couple minutes we have left, I wanted to get a question from the audience. The idea here is that the notion of accountability -- we've heard a lot about sort of internal processes, but does accountability, in any way -- and this touches on, I think, something that Ari discussed about, it's related to the idea of maybe an information fiduciary or a fiduciary relationship. Does accountability embrace the notion that you should safeguard data and use it in ways that doesn't cause harm and how would we think what those harms would be?

Anyone?

MR. WALDMAN: I think it's important to not see -- for regulators and the law to create this idea in our consciousness that data is not merely an asset. Data is responsibility. To suggest that data is just an asset means that we can buy and sell it, we can do pretty much whatever we want subject to small limitations. But given the way and the importance in which data flows have to our interactions with each other today and basic human flourishing, having data, using it, wanting to make money off the amount of the data that you have and wanting to make use of the data that you collect is a responsibility. And the way to recognize that is to impose fiduciary-like obligations

on companies that ensure that you're not using that data in a way that harm -- at a minimum, ensures you're not using it in ways that harms customers or consumers so you can benefit yourself.

MR. COOPER: Dan, do you want to jump in?

MR. CAPRIO: So part of this reminds me of the conversation we were having yesterday about GDPR and the 4 percent fine for global turnover. And it was said that, you know, that's gotten the attention of the C-suite. Well, I would agree with that, but I would argue to this point in the wrong sense.

So what we're trying to do, and we're talking about valuing data, is getting companies -- in terms of mix management, getting companies to think about privacy strategically. So the idea of a lot of proscription and fiduciary responsibilities, we run the risk of having the same problem that we have with GDPR, which is this becomes operational control and it becomes a compliance cost and it goes way down in the bowels of the organization and the company just sees it as a cost. So I think we've really got to flip it and see data and privacy as a value.

MR. COOPER: I'll let you have a -- real quick, but we are --

MR. STIVERS: Out of time.

MR. COOPER: We have triple zeroes.

MS. MCSHERRY: Just a final thing. I think the idea of information fiduciaries has a lot of value to it as long as we don't assume that that's going to cover all the bases. We're going to need more than that concept, it seems to me, to ultimately protect consumer privacy. What I like about it is I do think it encourages thinking about information and thinking about data as something more than an asset, but rather something that's actually important information about a person that they may care deeply about having shared or not shared.

MR. COOPER: Well, thanks. That's going to have to be the last word. Join me in thanking our panelists for this great discussion and we'll be back in 15 minutes for "Is the FTC's Current Toolkit Adequate, Part 1.

(Applause.)

PANEL: IS THE FTC'S CURRENT TOOLKIT ADEQUATE?, PART 1

MR. TRILLING: Good afternoon. My name is Jim Trilling. I am an attorney in the Division of Privacy and Identity Protection, and I will be co-moderating this panel along with Maneesha Mithal, the Director of the DPIP.

Our panelists today are Christine Bannan, Consumer Protection Counsel at the Electronic Privacy Information Center; Marc Groman, Principal at Groman Consulting Group and a former Chief Privacy Officer of the FTC; Jane Horvath, Senior Director of Global Privacy at Apple; Stu Ingis, Chairman of Venable; Peter Swire, the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business; and we may be joined by Jon Leibowitz while the panel is in progress.

With that, Maneesha is going to kick things off.

MS. MITHAL: Okay. Good afternoon, everyone, and welcome to our panel. So as we've kind of been preparing for this panel, we're going to divide up our discussion into kind of four parts. The first part we're going to talk about how we measure success at the FTC. Second, we're going to talk about

gaps in our existing authority under Section 5 of the FTC Act. Third, we're going to talk about gaps in our remedies. And, finally, we'll talk about additional tools and resources that the FTC may need. So we'll try to roughly divide that up into equal parts. And so if somebody has something on a later discussion, if you could save that comment for later.

So, first, the first question I wanted to throw out to the group is what should be the FTC's role in the privacy area, what would define successful FTC intervention, and how can the FTC measure success? And as you're answering this question, I just want to note one thing that I think we've heard over the last two days. We've heard a lot of panelists and public discussion around the fact that a lot of these questions that we're asking over these two days involve similar questions to what we were asking 10 years ago or even 20 years ago, and there doesn't seem to be any more consensus today than there was then.

So is the FTC doing something wrong? Is there something more we should be doing to either develop that consensus or to protect consumers' privacy generally? And I'd like to throw out that question in the first instance to Marc Groman.

MR. GROMAN: Great. Well, it's a pleasure

to be here, and that's a really interesting way to tee it up by looking back at the workshops because I want to focus on that as well. There's no easy way to do metrics or measure success in the area of privacy. I've been trying to do that for 15 years to various bosses. I've had "privacy" in every title I've ever had.

And so, you know, looking to things like the FTC Privacy Report, where we report on -- we -- you report on things like number of cases filed, consent agreements, dollars gotten from civil penalties, that is -- maybe it demonstrates that you're using taxpayer dollars efficiently or effectively, but that is not a metric for success in privacy.

And so tying to what you just said about the workshops, and I don't mean this to be flip because I'm dead serious, is that how I would measure success is that you have hearings in five years and the conversation is completely different. And if that occurs in five years, then I think that we have -- we can evaluate it and look at success.

And what do I mean by that, what should be different? This will shock you, but let's have some fun. We're not talking about privacy because that word does not capture half of what we discussed over

the past two days. It is far too narrow. We're also no longer discussing what is personally identifiable data or not. That debate's over. And we're talking about what are the impacts of data on people, whether one person or a group, but we're done with this discussion and fight over what is PII. We're not using innovation as this thing to balance against privacy. It is so overused. Innovation means change. That's what it means. And so what we want is responsible innovation, not innovation at all cost.

On the tech front, what I'd like to see is more presentations on deeper issues in technology, and I'd like to see it done by the FTC staff, meaning that you are at a level of technical competency that you are doing the presentations and not bringing in others to do it. We're talking about data more granularly like others did today. We're recognizing that data, whether it's provided by individuals or observed or inferred, have different levels of sensitivity, and we're taking that on and we're doing it head on.

And then just quickly on the notice and choice, we'll have success if in five years the US Chamber of Commerce is caught up to the rest of the world and not still pushing for a notice and choice bill.

MS. MITHAL: Okay, so a lot to unpack there. I would invite all the panelists to chime and respond to anything that Marc said, but in addition to that, I'm going to just throw out another question, picking up off of one of the things Marc said. So Marc said that, you know, we're sometimes measured by the number of cases we've brought or the civil penalties we've obtained, and we can try to measure in concrete numbers, which may not be the best level of success or best measure of success.

So I guess the followup question would be how can the FTC get feedback on whether it's using its tools appropriately to sufficiently protect consumers? And let me just kind of add a question onto that, which is that some people claim or we've seen kind of public statements about some people saying that even though the FTC's been using its tools in this space, we consistently see privacy failures. So does this indicate a lack of FTC success?

So I throw that open to anybody on the panel or anybody to react to Marc's comments.

Okay, Stu.

MR. INGIS: Let's see if I know how to work this. Well, thank you for having me participate on this great panel. And I thought -- as always, I can

see a lot of value in Marc's comments. I would just add a couple points. I think the FTC's role in privacy has been a huge success. It could always be improved, like anything, and I would measure that on two fronts: how companies treat data and how far they've come based on the FTC's enforcement.

And the FTC actually took a statute that had nothing to do with privacy and has created a whole series of cases and law and effective responsibilities of serious companies and serious professionals. And to do that in an age of such unbelievable change and innovation I think is really, really hard, and I would argue there's probably not an analogous example in the development of kind of the society we live in.

So the other way I would measure it is continuing to be at the center of this dialogue, showing the leadership through multiple commissions on a bipartisan basis. Look at this meeting today. There's a full room here, and there are hundreds, if not thousands, of people around the country -- hello to all of you -- watching all of this. There's a bunch of folks back in my office watching this. And I think you've shown great leadership in keeping this debate and important societal value front and center. So I would compliment you.

On Marc's point, I would agree, it's time to evolve and continue to evolve the debate. We're calling -- in the groups I'm working with, Privacy for America -- we're calling for a new paradigm to really tackle some of the new and next generation, a lot of things Marc mentioned.

MS. MITHAL: Great. And I think you'll get a chance to talk about that in a second.

Christine, did you want to add something?

MS. BANNAN: Yeah. I'll say that I think we should measure the FTC's effectiveness. The enforcement of orders, I think when particularly Facebook and Google consent orders were announced it was really seen as a sea change and people were really expecting a dramatic change in how the companies' privacy programs operated, but we've only seen, you know, in the year since then, more privacy violations by the companies. And I think any upcoming action that the FTC takes to enforce the consent order against Facebook based on the Cambridge Analytica story will be a litmus test for effectiveness.

MS. MITHAL: Okay, and just picking up on that point, I think that kind of gets to the question I was asking about is the existence of privacy failures in the marketplace some sort of a yardstick

by which the FTC should measure success, and, if so, how. So anybody want to comment on that? Jane?

MS. HORVATH: I would just say you could also look at a measure of privacy successes in the marketplace. I think that over the last 10 to 15 years, you've seen an evolution towards business models that are looking not at how much data can we collect but at how can we first protect our customers' privacy while we innovate and build new products.

And I would say the FTC's work, the workshops and the ongoing papers, et cetera, have given you really good guidance for that. So I think that is one of the successes as opposed to looking and saying, oh, there's a market failure, the FTC is obviously not successful, look at all the companies that are successful building privacy into their business models.

MS. MITHAL: Okay, thank you. So I think one kind of -- something that goes hand in hand with how you measure FTC success is the question of what should FTC's goals be. And there was a lot of discussion yesterday about what the goals of privacy protection should be, and I just thought -- let me just ask for a show of hands on the panel.

I jotted down four things that people said.

One goal is preventing harm. Another goal is improving transparency and consumer choice. A third goal is avoiding surprises, slash, I wrote down this, slash complying with consumers' expectations. And fourth is kind of promoting innovation and the benefits of technology and competition. Now, you can raise your hand for more than one of those, but I'm just very curious.

So how many people on the panel believe that preventing harms is a primary goal of FTC?

Okay. Consensus?

Okay. How many people believe improving transparency control is a measure of success?

MR. GROMAN: This is motherhood and apple pie, by the way.

MS. MITHAL: Okay, okay. What about avoiding surprises and comporting with consumer expectations?

Okay. And, finally, promoting innovation and benefits in the marketplace?

Okay, all right. So we have consensus. I think our work is done. Okay, but does anybody want to unpack any of those issues, talk about some of the relative importance of each of those, vis-a-vis each other? Yeah, Marc.

MR. GROMAN: Well, one thing that going off of what Jane said, and I don't know how we exactly measure whether it has worked or not, but we want good policy to drive incentives for industry and commercial actors to engage in best practices, and we also want to see incentives for new technologies. And so, again, what would I like to see in five years, I would like to see a small army of companies that have new technologies and privacy-enhancing technologies.

There is not the incentive to do that now, and so I think that goes to the effectiveness of the FTC and others. I do not think the incentives today are adequate to push companies to invest a lot of money in privacy-enhancing technologies.

One of the benefits or positive outcomes of GDPR, in my view, is that it has driven investment in that kind of technology. There are problems with it, but that is good measure of success -- are companies incentivized to do best practices or deterred from negative outcome.

MS. MITHAL: You know, I think it's curious that all of the panelists raised their hands when I asked if one of the goals should be improving transparency and consumer control. I feel like for the last 10 years and including today the idea of

notice and choice has been quite vilified. So how do you reconcile those two things -- consensus there should be transparency and control but there shouldn't be notice and choice? I'm not quite sure how those terms are different. Peter, can I --

MR. SWIRE: It's necessary but not sufficient.

MS. MITHAL: Okay.

MR. SWIRE: You have to have notice or else the company doesn't know what it's doing and the consumers don't know what they're doing. There's choice at various points, but to say that that's all in privacy is missing many, many other issues.

MS. MITHAL: Okay. Anybody else?

Let me just again unpack one of the goals I mentioned, which was kind of avoiding surprises and comporting with consumers' expectations. What do you say to those who say, well, you know, there's a lot of surprises in the marketplace that are actually good. There are certain things that consumers didn't realize they wanted, but they actually do want it, and that's what the marketplace is providing.

And any reactions to that or any rejoinder to that criticism? Yes, Marc.

MR. GROMAN: I think there's a lot of

consensus that context matters, and so we want to make sure that is baked into an analysis of risk and that consumers do have reasonable expectations and that uses of data that are outside of those expectations in some kind of framework need to be treated differently.

MS. MITHAL: So, again, this was brought up on a panel yesterday. How do you measure consumer expectations?

MR. GROMAN: I think we have to look at risk. So I think that focusing on conversations on like what is sensitive or not, right, that's sort of a small element of a larger discussion that we ought to be having, which is when you have a kind of business practice that is, surprise, outside of context, what risks are we presenting to individuals? And putting individuals at the center of that risk analysis I think helps drive us to the a good outcome.

MS. MITHAL: Okay. I want to turn it over to the next part of the discussion, but one thing I want to ask the panelists to think about as we loop back to this in a further discussion is the idea of if we were thinking about crafting legislation. You know, we hear that it's important to kind of, you know, not surprise consumers and comply with consumers' expectations, but is that something that

would be possible to legislate? Is it something that we should be recommending that Congress be considering? So I'm not going to ask for answers for that right now, but I tee that up, and let's pick up on that thread later if we could.

So why don't we -- Jim, do you want to do the --

MR. TRILLING So we're going to move on to discuss gaps in the FTC's authority. The FTC has general authority under Section 5 of the FTC Act to prevent unfair or deceptive acts or practices. Stu mentioned in his opening comments that the FTC Act itself could be characterized as not textually having anything to do with privacy.

What are the limits of unfairness and deception as the primary tools for FTC privacy enforcement? And are those limitations keeping the FTC from protecting consumer privacy adequately? So I'm actually going to ask Peter to take the first response to that.

MR. SWIRE: Yeah, thanks very much, and it's great to be here as part of the continuing FTC efforts to do the workshops and think this through. I play the role of old man in these rooms sometimes. I wrote a book on EU/US privacy 21 years ago and was chief

counsel for privacy beginning 20 years ago, so I have some historical perspective on FTC successes. And I'm going to highlight three legal developments that make some of the earlier FTC victories not as impactful today, so things that were authorities in effect but don't work well today.

And one's deception; the second is consent decrees; and third is Article 3 standing. So on deception, the FTC had a huge win in the late '90s getting people to post privacy policies. And you can see the statistics, and companies posted them. And when the companies posted them, the companies at that point didn't really know very well what their data flows were, and they made lots of mistakes. So there was ripe fruit for enforcement actions in the early days under deception, lots of good consent decrees got written.

But over time, two things happened. One is that companies learned what their data flows are, so they stopped over-promising; and the second thing is the companies hired lawyers who had more and more practice in making sure they wouldn't get caught for the company. And so deception as a tool doesn't work as well because companies aren't over-promising as much as they did before.

A second gap is problems in consent decrees, which have had all sorts of success, and Dan Solove and Woody Hartzog have their articles about the common law of consent decrees, and it was very hopeful about what these would produce. And it has produced big 20-year agreements.

But I think after Windham and LabMD, my sense among litigators is if they have a "bet the company" kind of case that they're going to fight the FTC, that the easy days of consent decrees are not going to be there. And the FTC is going to find it harder to stretch the limits of its authority. Companies are going to push back. And the FTC has finite resources, so the FTC is going to have to be a little bit careful pushing the limits of its unfairness policy, and I just said deception doesn't work as well.

And the third one, again briefly, is Article 3 standing, which maybe is less familiar here. A lot of people who follow the class action cases see that a lot of federal judges have been saying that for data breaches and things like that there's not really Article 3 standing, that there isn't the right kind of injury in fact. But in the Spokeo case, there was some of that same kind of litigation that came back to

affect the FTC, and I had my quotes.

So the Supreme Court said that Article 3 standing requires a concrete injury, even in the context of a statutory violation. So if the company flat out violated a law, that isn't enough to make sure there's standing even for the FTC. And it also said that Congress is well positioned to identify intangible harms that do meet minimum Article 3 requirements.

So if you're thinking about what Congress might do, one thing Congress might do is define intangible harms so that there would be Article 3 standing. And the second thing is to the extent you want individuals to bring suits, which some people want and some people hate, the states don't have Article 3 limits. States can bring intangible harm suits, but a lot of federal judges think in the federal courts those intangible suits will fail.

So there may be in the preemption debates reason to keep some state causes of action if you want those intangible claims at all because the federal court standing rules restrict not just the FTC on statutory violations but private plaintiffs when they think they're injured.

So a lot of the things that were there

probably won't be as effective going forward, and that's a reason to rethink what the FTC's powers are going to be.

MR. TRILLING: Thanks Peter. So let's continue along the lines of the same topic. So what are actionable privacy injuries under the unfairness prong of Section 5 of the FTC Act? And are there gaps?

MR. SWIRE: Unfairness under deception?

MR. TRILLING Under unfairness.

MR. SWIRE: Unfairness under privacy, I'm going to let a former chairman explain when that wins. It's a pretty hard claim, I think. People have a hard time in some settings, many settings finding an unfairness claim.

MR. LEIBOWITZ: Well, certainly in our common law of privacy we enforce through settlements. We use the unfairness prong reasonably effectively. Now, you might say that it doesn't reach some of the -- that we didn't use it with respect to monetary remedies. Those are, of course, much harder when you're dealing with harms like a breach of privacy.

But you know, I tend to think that -- and I don't think I'm in disagreement with you because I think you raised actually a very important point. But

I tend to think between the FTC's unfairness authority, its deception authority, and its -- and really the unscrupulous business conduct line of cases that we used in at least one matter, the Intel matter a few years ago, that you can reach a lot of the conduct.

I think one of the issues that I think policymakers in the Commission, and I don't want to jump ahead too far, is facing today is sort of whether the remedies are strong enough, I think, and then two is whether you need ex ante rules rather than just ex post enforcement as a way of protecting consumers and giving them more control over their data.

MR. TRILLING: And we'll come back to remedies. So some panelists -- let me talk about a specific type of injury. Some panelists have suggested that emotional injury is or should be a basis for bringing unfairness cases. Do people have reactions to that as to whether under existing law the FTC can base unfairness claims on emotional injuries and whether the FTC should be able to base unfairness claims on emotional injuries?

Marc.

MR. GROMAN: Well, I think that the bigger question which you're teeing off is simply that -- or

to answer the other question is that there are enormous gaps with unfairness and there are an enormous number of practices that are not addressed by unfairness and can't be. And, in fact, that's the way the law works. I mean, it's sometimes hard to explain that to people, but not every bad thing can be addressed by the FTC or FTC Act. And that is definitely true in privacy where even as an attorney you're often trying to shoehorn factual allegations into the three prongs of unfairness, and one of the most difficult ones is the injury prong, where it can be a small injury to lots of people or a big harm to some people, but we need to figure that out.

And I think just saying is it emotional injury, you know, I think that, you know, begs the question of what are we talking about, how significant could it be up to, you know, serious anxiety or demonstrable -- it doesn't -- the concept in and of itself doesn't bother me. We have to get down to more details and to assess whether it's substantial in a context, which goes to the bigger question. We need to -- we, legislators, need to sort this out and figure out what are the scope, the full scope of adverse consequences from data use that we want the FTC or some agency to address.

MR. TRILLING: Do others want to weigh in on the ability of the FTC to reach injuries like emotional injuries under the unfairness prong of the FTC Act?

Peter.

MR. SWIRE: I think that's part of why I was raising Spokeo with the federal court skepticism of injuries unless they meet all these words like concrete and particularize. And then in unfairness, it's even a higher burden many times because it's not just the flat-out statutory violation, which was claimed in Spokeo, but you have to meet those prongs in the unfairness test, which was designed to be relatively strict in the 1980s so that the FTC wouldn't get out of control. That's why it was written in the 1980s.

So I think unfairness -- let me put it this way. I think it would be fair to say there's litigation risks for the FTC if you go up with a straight emotional injury claim and nothing beyond that.

MR. GROMAN: But in a privacy case -- so let's take a case where there is a camera in a home and the company turns on the camera and is filming or observing you inside your home.

MR. LEIBOWITZ: And, indeed, we had that case in about 2011.

MR. GROMAN: Right. So, I mean, what is the harm? It's not financial; it's not identity theft. It's some form of what, embarrassment or emotional harm or a feeling that my home has been, right, invaded because this camera went on and shouldn't have. There seems to be uniform agreement on the Commission that that's a good case. Well, what is the injury? Isn't that a kind of an emotional injury? Cameras went on in my home and I didn't expect them to.

MR. TRILLING: So that's a good segue into discussion of the FTC's Vizio case in which the Commission alleged that the collection and sharing of granular, individual, or household viewing data without knowledge or consent was unfair. Do people have thoughts on the FTC's pursuit of unfairness in that case, the issue of viewing data in particular and how you would categorize the harm that may be at issue in that type of undisclosed collection and sharing?

MS. HORVATH: I'd just like to make a more general comment that I think that harms are going to be evolving as more and more things go on, you know, happen in the digital realm, there will be an evolving

understanding of what is harm in that realm. I think that if we look back historically, the court may not have found concrete harm, but as more and more is taking place in that realm, there may be more of a willingness to see a concrete harm in an emotional scenario.

MR. TRILLING: So in this particular case, then-Acting Chairman Ohlhausen wrote a concurrence in which she called on the Commission to examine more rigorously what constitutes substantial injury in the context of information about consumers. The Commission subsequently had an informational injury workshop in December of 2017. Informational injury has also been a topic in this current series of hearings on competition and consumer protection. Should the Commission take additional steps to examine informational injury, and, if so, what types of steps should the Commission take?

MR. SWIRE: There's silence on that, but I come back to this point that if Congress were to pass a statute and were to say that certain things counted as injury that you're in a stronger position in litigation on standing going forward as something Congress could do to help.

MR. INGIS: I would add I think you could

actually -- the Congress or through rules if you had the authority to do it, the FTC had the authority to do it, could define bad practices in a way that the statute would lay out where you wouldn't even need to get into a debate about the harm. You can enumerate the types of practices that often have been the rulings in consent degrees.

And then as to harm, I think -- and I agree with Peter's comment on that. I think you could enumerate things beyond economic harm that are harm. You know, the emotional one gets challenging, but it's not impossible. And, in fact there are legions of court cases in other contexts that define what constitutes emotional harm.

One of the things that we've been looking at in detail is to look in other areas of common law, law, for example, around defamation where you could assess what are the criterion, what is it about defamatory remarks that should be considered about harm, how do courts find that, and is there something that can be clearly articulated beyond economic harm that would be built into a statute.

MR. TRILLING: Let's shift gears and talk a little bit about deception. So the FTC deception statement says that the materiality of expressed

statement should be presumed. Is this true if the statement is buried in a privacy policy? Does the presumption of materiality make sense when it comes to statements about privacy practices? Or is there something different about privacy policies and other statements about privacy practices?

Christine.

MS. BANNAN: I think that the statements made in privacy polices have to be considered material. I know EPIC and many others today criticize privacy policies, but if we can't even hold companies to the policies that they're publishing to their consumers, then I'm not sure what purpose those are serving.

MR. TRILLING: Does anyone disagree with that? Does anyone believe that the presumption of materiality should not apply to an express statement about privacy practices?

What are examples of privacy violations that don't violate the FTC Act but should be illegal, and I want to sort of feed into the question that over the last few days we've heard discussion about price discrimination as a possible issue that stakeholders connect to the collection and use of data.

We've also heard reference to dark patterns.

We've heard reference to differential pricing. Are any of those violations or are there other violations that there may be questions about the applicability of Section 5 of the FTC Act that you would identify as gaps that policymakers should think about filling. Peter?

MR. SWIRE: I guess -- one is the whole area of algorithms -- algorithm transparency and discrimination. That's not really a deception claim. You could argue that it would be an unfairness claim, though the triggers for what's unfair there is not simple to define. And so a huge amount of the privacy writing, if you go to privacy law scholars, is on sort of the uses of big data and machine learning and such.

So how FTC is going to get there with unfairness and deception, I think, is something that I haven't seen clearly done. And then I think there's more and more public discussion about the intersection with the antitrust and privacy, price discrimination among economists. There's lots of times when they think it's efficient, and there's sometimes when they think it's not efficient. So just saying price discrimination is not nearly enough to establish an antitrust violation.

But in Europe, at least, there's a lot of

discussion about dominant platforms and dominant players once you get to 30, 40, 50 percent of a market. The rules around contracting start to change under European competition law. The US hasn't gone there previously, but there's going to be, I think, a tremendous amount of discussions about what the right way to do that is, and so I would guess that's an area that will get lot more attention.

MR. GROMAN: So I think that two areas to think about, these are complicated but -- and difficult to articulate, but one is when practices impact behavior. And so it's not that there's a clear injury, but let's say when Facebook changes -- uses algorithms to change an emotion or change the things I perceive or alter choices in a way that is outside the scope of my expectations, not in every case that presents a problem, but it could in many cases, but particularly when it's very large, and I don't know that that would fit within the FTC Act.

And then what I would call chilling effect, which is not in this case government, but I would hope that we all want consumers to reach out and use the internet for the amazing things it's there for, which is to find all kinds of information. And I don't want people to not reach out for it and get data because,

you know, they'll be viewed -- you know, there's a consequence that they don't know about for very particularly sensitive areas.

MR. TRILLING: With that, I think we're going to move into the remedies portion of the discussion.

MS. MITHAL: Stu, did you have your hand up? Did you want to say something on that before we move on.

MR. INGIS: No, go ahead, keep going.

MS. MITHAL: Okay.

MR. INGIS: Thank you.

MS. MITHAL: Okay. So we've talked a little bit about potential gaps in the unfairness and deception authority of the FTC Act. Now let's move on to potential gaps in the remedies that we seek. And so I'd like to divide the discussion into the kind of injunctive/behavioral remedies that we typically seek in our orders and then monetary remedies. And so why don't we start with the behavioral/injunctive remedies, and if I could ask Christine to comment. Do you think that the FTC is using its existing toolkit effectively in crafting remedies in its orders?

MS. BANNAN: I don't think that it has been effective. I think especially -- I know, it's

difficult for us to say because of the privacy assessments, because they are so heavily redacted, so EPIC has used the Freedom of Information Act to get the FTC's privacy assessments that are under consent order, and that's really been, I think, the center of what's been held up in the consent decrees as comprehensive privacy program that's really going to change internal business practices and really change the nature of how the company is conducting its data protection, but we really haven't seen in the time since those big firms have been under consent order that those practices have really changed. So I think that is an indictment to us that this type of process isn't really having the effect that it was intended to.

MS. MITHAL: Okay. Does anybody else have any reactions or response?

Okay. Christine, can I just ask you a followup question? And the followup question is do you have specific suggestions for other remedies that the FTC should be pursuing or things that the FTC should be looking for in these privacy assessments?

MS. BANNAN: Yeah, so one thing I think would be bringing those assessors or auditors under sort of control of the FTC rather than control of the

one being audited. I think just one example, like Facebook's first assessment, the assessor, PwC, flagged an issue that the company wasn't assessing service providers' compliance with the stated use policies that made it more difficult to detect issues with third-party developers. And instead of like remedying that problem, the next biennial assessment, Facebook was able to, like, change the standard so that that wasn't being assessed the same way it was the first go-around.

And I think that is an example of how the way these assessments are being carried out the FTC should have greater oversight rather than the one being audited. I think it really compromises the independent nature that those investigations are supposed to have.

And then as far as other types of remedies, I think that FTC should be looking at antitrust remedies. I think even though the bureaus are separate, more collaboration between them and thinking about how antitrust and privacy issues are related would be a really big benefit to consumers. We think that unwinding some of the mergers that have allowed big firms to snap up their competitors and get those -- like that data, that user data that's been so

valuable and allowed firms to grow a lot more dominant and be able to just acquire their competitors before they are a competitive threat. I think privacy should be considered when that merger review was going on.

MS. MITHAL: Okay, go ahead, Jon.

MR. LEIBOWITZ: Can I just add one thing to that, which is sometimes it's even simpler. So when we brought our case against Intel, it started out as a competition investigation. And as we continued our investigation, it became a very strong consumer protection investigation, a UDAP investigation for gaming and benchmarking systems to make Intel's chips look stronger than they otherwise would have been, at least that's what we alleged in the case.

And I do think that there is a fair amount of -- there's a fair amount of investigations that would benefit from having both parts of the FTC house sort of working together. I noticed in the new technology task force, there is -- there appears to be some role for the Bureau of Consumer Protection. I just came out of an enforcement meeting -- and I apologize for being late -- with Bruce Hoffman, and I saw Daniel Kaufman walking in. So I thought that was a good sign.

And I do think that sometimes if you pair

your sort of antitrust competition thinking with the consumer protection, I mean, Peter's written about this, too, that you might come up with a better remedy and sort of an innovative case.

MS. MITHAL: Okay, so I think two threads have come out of this discussion. One is kind of what are the appropriate remedies, and the other is intersections between privacy and competition. So one of the things that we have heard from some panelists from some public discourse is that there's somehow -- there's some ways in which privacy and competition may be at odds.

So, for example, if you are requiring opt-in choices for information then maybe you are entrenching incumbents and not allowing smaller new entrants to come into the marketplace. I'm wondering if people have responses or thoughts on that, particularly since we're talking about intersections between competition and privacy.

MR. LEIBOWITZ: So I guess I would say yes, there are sometimes some tension between competition and a consumer protection approach to a matter. That doesn't mean that you shouldn't -- and certainly, for example, the early returns on GDPR, you know, are that it may raise barriers to entry, it may be innovation-

stifling. I don't know that we know that for sure yet, but that's certainly what we are beginning to hear.

On the other hand, if some entity is engaging in a violation, you know, you ought to go after it, and if you can tweak a remedy -- going back to remedies -- if you can tweak that remedy to make sure, you know, sometimes it's with licensing, sometimes it's with open sources, sometimes it's neither of those things, to make sure that there's less tension from the consumer protection side or vice versa, I think it's probably good.

And I think you guys have -- you know, think creatively in that context, or have and will.

MS. MITHAL: Peter?

MR. SWIRE: So I have a historical example of a tension between privacy standards and antitrust. When I got to spend a year with Stu Ingis and a bunch of other people on "do not track," we were trying to come up with a privacy standard. And at one point, we were quite close to having an agreement, I thought. And at that point, there were going to be privacy rules that the browsers had agreed to. And as part of that, the FTC wondered were there antitrust concerns having the browsers talking to each other in this way

and coming up with standards.

And so the week before one of the plenary sessions for "do not track," I basically did a two-hour moot court with the FTC on why we thought it was not an antitrust violation to have this "do not track" privacy rule. But apparently I wasn't persuasive, and so the next week when we went to our meeting for "do not track," we were told that if we went out with a proposal that somebody from the FTC would stand up and say the FTC had serious antitrust concerns about the proposed agreement. This is highly relevant to -- Stu wasn't in the room for that part. He has no blame for all that --

MR. INGIS: This is news to me. I was wondering why you pulled out of that deal at the last minute, but now it's clear.

MR. SWIRE: Well, it was the spring of 2013. We had what I thought --

MR. INGIS: Jon doesn't seem to know about it.

MR. SWIRE: It was after Jon had left.

MR. INGIS: Oh, after Jon.

MR. SWIRE: So there's a lot of talk about can there be self-regulatory standards, can there be industry efforts to come up -- informed by consumers

with good privacy practices. But at least in this instance, there was a decisive antitrust objection from the FTC to the deal.

MR. LEIBOWITZ: Well, I just want to -- defending my agency, of course I was gone by then, I would say that if there was a will to reach a "do not track" accommodation, there should have been a way to avoid -- I mean, well beyond Noerr-Pennington but should have been a way to avoid serious antitrust concerns. That's actually an interesting news flash.

MR. INGIS: It is a news flash for me, too. That's water under the bridge, I'm teasing.

MR. SWIRE: It's long enough now that I'll talk about it publicly, but it was very annoying at the time to have the deal fall apart.

MR. INGIS: Indeed it was, I'll say. But I think Peter is right. Forgetting about, you know, how -- you know, the history was written, maybe we should have a book written someday about it. But I do think Peter is right, and I think that that point actually is more acute now than ever before.

Whether it's true in motivations or just the reality of very successful businesses, if you allow one, two, or three companies to set rules, whether it's -- whether they reached conclusions that are

against public policy or not, there will always be that perception from competitors. And there's always that possibility and potential. And so when you're looking for solutions for some of the privacy challenges, which could very easily be put with one, two, or three companies, it raises, I think, significant competitive issues.

MS. MITHAL: Marc, did you want to --

MR. GROMAN: Yeah, I just wanted to just push back on the actual question, right, because the question was, does privacy cause a competition problem. No, privacy does not cause a competition problem. Responsible use of data does not cause a competition problem. What causes a competition problem is our current -- today we have a sectoral approach, and so different sectors of the economy are regulated differently, which means that any change in the framework by definition necessarily is or likely to benefit some sectors over others.

And we saw it play out today. If your company, already subject to opt-in, then you are very eager to see everyone else get opt-in. If you're not, you might want a different approach. We're going to have to grapple with that as we create that framework. But it's not privacy itself. It is the current rules.

MR. LEIBOWITZ: Yeah, and if I can just follow up, you know, look, I agree there can be some tension between rules that are easier for the largest players to follow and sometimes dampen new entry. I think there are ways to avoid that, by the way. And I think we have tried to avoid that, or the FTC has tried to avoid that in many of its cases and in its thinking.

But I certainly hope that if Congress, and I certainly hope Congress will move forward with some privacy legislation that will empower consumers, and if at some point there's a group from the business community that begins to say, you know, well, you know, this is going to entrench large businesses, I would look under the hood to see who those businesses are -- or, you know, who in the business community is actually objecting, because very often it is -- and I hope that won't happen. I'm not so sure it will happen because I think there's a clearer -- I think there is a clear problem that we want to solve for, which is consumers need more control over their data. Some companies do it really well; some companies don't.

And I just don't inherently see a federal approach that might have opt-in for sensitive

categories of information, opt-out for other categories of information, inferred consent. I mean, this is just sort of along the, you know, more rights of deletion and access and maybe correction depending on the context.

Again, I apologize for going to the end, you know, from the middle, but -- of our panel, but I just -- we have to solve for a bigger problem, and I don't think that -- and sometimes those types of objections, and it sounds like you believe that it was the case in "do not track," can be pretextual.

MS. MITHAL: Okay. So let's just jump back to remedies for a quick second because I do want to set up the last part where we're going to talk about what tools do we need to fill in gaps, but just sticking with the gaps and remedies for right now, just to provide some context to the audience and to the panel, so I think I jumped into the remedies question without laying the foundation for what remedies do we seek in our orders. And I think they're typically things like data deletion, prohibitions on misrepresentation, certain cases to have a privacy or data security assessment and get outside -- to have a comprehensive privacy program and get outside assessments of that program.

And so we heard from Christine the kind of limitations to that approach. We also heard from Christine ideas for additional remedies we should be including in our orders. Does anybody have any other comments on that piece? Are there additional remedies we should be including in our orders? Christine had the idea -- or she mentioned some other remedies, including kind of unwinding mergers and other competition-based remedies.

Anything else that we should be considering -- so I think the premise for this question is that, you know, we can talk about legislation, and there's been a number of groups that have recommended legislation, but until legislation passes, we have the authority we have. And so what I'm looking for is kind of ideas, tips for filling in gaps in a way that's consistent with our legal regime. Comments?

MR. LEIBOWITZ: Well, I guess one thing is, you know, that you might think about, and I understand that resources are a difficult issue, but you might think about some allocations of resources to making sure that the behavioral remedies associated with an order are adhered to.

MS. MITHAL: Good. Okay, well, why don't we move on to the related topic of monetary remedies.

And so I guess two questions under monetary remedies. One is should the FTC pursue monetary relief under the existing regime in our cases. And, if so, how could we measure -- so, again, just to provide context, we can currently seek equitable monetary remedies -- disgorgement, redress -- and so should we be seeking more of that relief in privacy cases, and, if so, how would we measure that?

Can I ask Jon to start just to kick us off on that?

MR. LEIBOWITZ: Sure. So do I think you should be seeking monetary remedies as a form of equitable relief in privacy cases? I think you should. I think there are circumstances where, you know, there's a harm to consumers or unjust profits to malefactors that make a lot of sense.

I do think when you are looking at -- and, then, of course, if you have, you know, a privacy violation that is statutory, could come out of COPPA or that is so clear and that's the case of the people sitting in the back office watching cameras, you know, on the computers that are -- watching people in their bedrooms, then, of course, you should.

My own sense, though, is that it is hard to reach. It's hard to reach the kinds of harms that

relate to people's true privacy and dignity. With a monetary remedy, that doesn't mean you shouldn't try, and I kind of think of Vizio as being an attempt to sort of, you know, to try to do that.

But I guess my view is that probably a better way to do that would to be sort of think about giving the FTC some type of up-front -- and not everybody agrees with this -- some type of up-front fining authority.

MS. MITHAL: Anybody else? I think there are two kind of paradigmatic examples of the types of privacy cases. One is kind of somebody has a network data breach and, you know, how do we seek monetary remedies in those cases. And I think the other is kind of a company has sold a product like an IOT product or a smart TV in the case of Vizio. And I think -- you know, I think we've heard that there are challenges, people have mentioned challenges in both scenarios. Anybody have any comments on that?

MR. SWIRE: I'm not sure it's exactly on point, but to the extent that the consent decrees have litigation risk associated with them, which we were discussing earlier, having a new statute from Congress that made clear that monetary fines could be pursued for injuries that Congress helps define would really

address that litigation risk. And I think the FTC would then have a much stronger hand when they see something wrong to say it's not like you're going to pay the second time, it's that we really have a problem right now.

I think a wide range of people from different parties have called for some monetary penalties at this point, and it would address some of the weaknesses we've seen in the litigation.

MR. LEIBOWITZ: Well, here's something else that you could do, and I should have thought of this before, is actually the Justice Department -- and I'm not necessarily an advocate of this, but it's the kind of thing you should be thinking about it. The Justice Department's Antitrust Division has gone to a preponderance standard for order violations. They've inserted that in orders.

Now, it was not by companies that are on the receiving end of that, it was not particularly appreciated. But I certainly remember thinking about order violation cases when I was at the FTC, and it's a clear and convincing standard, isn't it? And, you know, we had to proceed with some caution, recognizing that there was a very high -- that there was a very high burden on the agency.

MS. MITHAL: Stu, did you have a comment?

No, okay. Okay, the last question, and then we'll move on to the last part. So the FTC has other tools besides enforcement. It has kind of the power to convene these types of workshops; it issues reports; it does 6(b) studies. To what extent should the FTC be doing more or less or something differently in these kind of nonenforcement realms?

Jane?

MS. HORVATH: I think the workshops are helpful, and I think allowing consumers generally more access to the FTC, so I might consider going out of Washington and visiting -- and holding some workshops across the states so you can hear from different consumers more generally than the privacy complex that we usually see at these meetings. You might actually get some consumers in the room to talk about their concerns.

MR. SWIRE: Just words of praise for what the FTC has done in this area for the last bunch of years. We're here today, and you have people with busy lives flying in from lots of places to be here. You have a national webcast, and there's a history of ideas being floated at these workshops that then get put into the stream of what people should consider.

So it's clearly been an area of leadership, I think, for the FTC.

MS. MITHAL: Christine?

MS. BANNAN: I'll say -- I mean, I would never argue against more workshops and research and reports, but I think, you know, that the FTC is the only one that really has enforcement authority in the federal sphere, and civil society and academia can pick up the slack if the FTC isn't able to hold as many workshops or do that sort of work, and I think the focus should really be on enforcement.

MS. MITHAL: Okay, Jim.

MR. TRILLING: Okay, so we're going to wrap up the panel by discussing the possibility of additional FTC tools and resources. Why don't we start off by talking about potential new substantive privacy legislation since that's come up a number of times during the panel. If Congress does enact comprehensive privacy legislation, what should it look like? Should it be based on the fair information practice principles and how might a comprehensive law based on the FIPPs account for differences in uses of data, and/or sensitivity of data? And, Stu, can you start off that part of the discussion?

MR. INGIS: Yeah, thanks. Working with a

lot of companies and leading trade associations that are in the consumer economy, we launched just on Monday an effort called Privacy for America, the details you can see on the webpage. I don't want to make it a sales pitch about it, but you can look at it. But it was all intended to start and push forward and improving the consumer experience based on a premise that the consumer experience is broken, the transparency has -- it's important, it's sufficient, but it's not enough. It doesn't give enough to consumers, and it's too much, whether it's opt-in or opt-out, the consumer experience. They're tired of all the clicks, particularly in what's happened in Europe, the "I accept."

And the approach that we have been pushing and working through on details are what we call a new paradigm because it's different from the old paradigm of just transparency and choice. And the new paradigm would have much more in the way of specific prohibitions. Many of the things we talked about on discrimination and other things on that point tied to an earlier question.

There are all those laws that other agencies enforce on those areas but none of them have the focus that I think in this day and age

should be specifically on data and the enforcement tools behind that. So you could put that within the FTC. And then you'd have appropriate practices, define stuff that benefits consumers, retooling particularly the stuff of the nonsensitive advertisements that benefit and give consumers things they're interested in at a relevant time.

So in the announcement, we called for a nationwide standard, prohibitions on certain practices, creation of a new bureau of data protection within the FTC that would resemble -- in many ways, I think the closest analogy is the FDA. There was a time where drugs and different things were being put out in the world without the right regulation, and many people in the pharmaceutical industry would tell you that saved the industry. And the level of benefit that can come from data justifies just that, and it requires just a much broader new paradigm, really a lot of what Marc was saying at the beginning, step back.

I won't go through more details now but I'll just make one point for many of us, certainly on this panel that have been in this debate for many years. I think the opportunity is actually here now for a law. I think there is consensus. Maneesha, you highlighted

some of it earlier. But there is consensus. The details matter. We've got to get them right. And we've got to do the hard work on that, getting beyond the rhetoric.

But I think there is consensus that it is the time for a national standard that could really redefine both the limits and benefits and framework around data in the information age.

MR. TRILLING: Does anybody want to respond to that general description of what privacy legislation might look like? Peter?

MR. SWIRE: Professors talk too much.

MR. INGIS: It's lawyers, not just professors.

MR. SWIRE: And it's worse if you're a law professor, right? Okay.

So the issue of preemption gets talked about a great deal and it can be relevant in this setting. So I wrote a couple of articles on the history and issues and preemption for privacy legislation earlier this year for IAPP. And Pam Dixon and I are working on a possible proposal, just as a thought experiment, for preemption maybe being a carrot, a reason to come in to industry defined with advocates participating but then with FTC approval if you have basically a

clearly strong set of standards there's a reason to maybe say yes to those standards because then you'd get the preemptive effect.

Having straight-out preemption is going to be controversial on the Democratic side. Having preemption if there is demonstrated strict standards and somebody watching the standards might be something where both sides could end up thinking that's better than the alternatives. So we're trying to see whether something in that direction might be a way to -- and it wouldn't just be industry-defined standards.

There would have to be some ability for notice and comment and for participation from different points of view. But that may be a way to change -- to adapt over time what the standards are and to address the new things that come up in the data economy.

MR. TRILLING: Jane, did you want to weigh in?

MS. HORVATH: Sure, I'd be happy to. And thank you so much for inviting me today. I'd also like to stress that we would be looking for something that's globally interoperable. You know, as a global business, you want to build your privacy compliance framework around strong global principles. And so

that's something we'd be looking at, and I'd like to outline a few of those principles that we would be looking for in a federal privacy law.

We'd like to see that it's generally applicable across different technologies and industries and business models so it sets a baseline of protections. We'd like it to apply to all persons acting in their personal capacity with a definition of personal information that is consistent with the other laws such as GDPR. And we do think there is a need for a controller-processor distinction. There should be different obligations placed on them depending on their relation to the data.

And there should be a distinction between personal data and sensitive personal data, a higher level of protection around sensitive personal data. We do think there definitely needs to be transparency and notice, and we think that there is room for innovation in this area.

And one of the things that we've recently innovated on is we've introduced a new privacy icon, and whenever you start a new product or service that collects your personal data, you'll see the hand shaking, and right under that icon is all the key privacy information that you need to know before you

actually start that new product or service. And, importantly, the icon won't show if the product doesn't collect personal information. So that's one of the ways that we're trying to be innovative in transparency and choice.

Next, I would say data minimization, crucially important. There's so much data out there. And we should really challenge businesses not to collect data unless they need it, and if they need it do they really need to collect it associated with a personal identifier? There's a lot you can do with random identifiers when you're collecting data up to your servers like, for example, Siri and Apple Maps both use random identifiers that are generated on your device, and then we're able to sync that data across your devices using an encrypted cloud. So Apple doesn't see your data, but your devices are smart.

We'd also say that the privacy law should require that the processing has a legitimate legal basis. I actually think the GDPR was sort of innovative in that area. It's not just a notice and choice law. Again individual rights, rights of access, correction, deletion, and the right to objection to processing, and then a robust security program.

I also think that it's time that we handle data breach notification consistently across, and it's an opportunity to put some consistency there. I'll just finish up with the data brokers provision and then I'm finished.

MR. TRILLING: Can I throw out one question and then we'll go to you, Jon? One of the things I want to drill down on, Jane, that's one of the few mentions of data minimization during the hearing. Can data minimization be legislated in a meaningful way, and how beyond telling companies to not collect what they don't need? And I would add to that who defines need, and how would policymakers or an enforcement agency look at need?

MS. HORVATH: I think we've been in a black-and-white place for the last decade where everybody has been arguing, we need all this personal information to create really cool services, and that personal information needs to be identifiable. But I think there are a lot of other ways -- pseudonymization, what I mentioned with randomly rotating identifiers for maps.

So the data is not identified -- it's not connected to an identified person. So you can do data sampling. There's a tremendous amount you can do

without collecting strongly personally identifiable data to comply with data minimization. So I think a law should require businesses to collect the minimum amount of data that they need to achieve the purpose of collection. I think it's very reasonable.

MR. TRILLING: Jon?

MR. LEIBOWITZ: Yeah, I actually think Jane has -- she's been thinking about this for a long time, and she has some very, very good ideas. It immediately occurred to me that you could take some of those best practices and turn them into a safe harbor. I would rather have the FTC thinking about this with a delegation of authority from Congress perhaps than Congress trying to write this into a law, other than an admonition to the FTC that you should figure out a way to implement this. But we'll see.

I guess I would say that you can -- just listening to what the other panelists have said, and I agree with a lot of what they said, that, you know, that Congress if it moves forward with legislation, it can learn something from GDPR and even from California, right? It's lawmakers who actually, or elected officials who actually passed legislation protecting privacy. They're flawed in some ways, but, you know, it is in many ways provoking that debate in

Congress now, which is a very, very good thing.

You can learn a lot. I see Julie Brill sitting here, and you can learn a lot from the Washington State bill as it moves forward or doesn't move forward, but as it proceeds. And, then -- but I also think, you know, this Commission can look at its own work product going back to the 2012 report that we issued and then subsequent reports that build on that because it really gives a framework that I think actually articulates the notion of empowering consumers to control their data, right? It is opt-in for sensitive categories and information, opt-out for other categories with the exception of inferred consent.

It's platform neutrality, which is critical. It's rights of access and deletion, and I think minimization is talked about in that report as well. It's enforcement authority for the FTC that would include fines. Some rulemaking. Not -- you know, enforcement authority for the FTC is something that will come in federal legislation. It's not exactly in the FTC report, as might some degree of rulemaking authority.

Increased resources. This agency is smaller now in terms of FTEs than it was in 1980 when the

population of the United States was 125 million people smaller, and, you know, the ability to -- and the ability to investigate a case was, you know, monumentally simpler.

I don't think -- I think we do need one strong federal standard. I think that is appropriate. Data doesn't travel -- you know, data doesn't remain in a single state. And I think most people, you know, not everyone, but I think most people from -- in the consumer movement sort of recognize that if you could -- if you could have a strong federal privacy regulation or law that protected consumers in every state, that would be preferable to a handful of states.

But I don't -- I sort of think of sort of preemption that we -- and by the way, in California, it's worth noting that when California passed the CCPA, it preempted all municipal privacy regulations, right? And GDPR has -- they way GDPR is implemented, you don't have lot of competing nation regulations, you have implementation by them. So it wouldn't be unlike the FTC and state AGs, you know, engaged in joint enforcement efforts which they do under COPPA, but it sort of strikes me that you can't get to the preemption question without having a strong bill

behind it, right, or without building a strong piece of legislation that would really protect consumers.

MS. MITHAL: Great. Thank you.

Marc, did you want to add something?

MR. GROMAN: Just in terms of legislation looking forward, any framework that we look at has to obviously take into account the future, not where we are today. And I think the future is data that is inferred about people. It is not data that is provided. It is not -- I'm not worried about the data I gave to a company through a website. That's 10 years ago. We need to focus on observed data and inferred data and make sure that any framework captures that.

I am a huge advocate -- this surprises people -- of a risk-based framework. I think that is actually what we're going to have to do given range of business models and be able to evaluate risks from any model.

And, finally, the question about minimization, when you talk about FIPPs, the way I envision a framework is that companies need to have some options here, and based on risk, I look at the FIPPs as tools or dials, and so you can ramp them up or down to provide different levels of protection

given a different model. The downside with that framework is that it requires people to think.

MS. MITHAL: Okay. So we have very few minutes left. I'm going to give each panelist an opportunity for a less-than-one-minute wrap-up. But we're also going to try something fun here. In addition to your one-minute wrap-up, you have a very illustrious set of panelists on the next panel, and we're almost all the way through the event.

So if there's one question that has not been answered or one issue that has not been discussed that you would like us to tee up on the next panel, because Jim and I are going to be moderating it, let us know during your final comments. So why don't we start on the end with Jon and move our way.

MR. LEIBOWITZ: You know, look, I think these --

MR. SWIRE: Him or Vladeck?

MR. LEIBOWITZ: What?

MR. SWIRE: Him or Vladeck?

MR. LEIBOWITZ: David Vladeck, yes, I think it's an excellent idea.

(Laughter.)

MR. SWIRE: Bring it on.

MS. MITHAL: This is your chance.

MR. LEIBOWITZ: Yeah, we'll have a few different options for that. We can turn up and down the dials as Marc just said. For me, no, I think this is great. I think you guys should -- oh, I would say one more thing, I think you should get very engaged. I think you're sort of starting to do this, but I think this agency should get very engaged in thinking through privacy issues with Congress. If Congress moves forward -- chance this year -- big chance if not this year then in a couple of years -- you want to be present at the creation and you want to influence that process.

The other thing I just want to mention is that while I do represent a few tech companies and broadband companies on privacy, a lot of broadband companies on privacy issues, I'm speaking as a former official and not in any client-related capacity.

MS. MITHAL: Peter.

MR. SWIRE: I'm also speaking as an individual. So is Justin Brookman here? I think he's on next?

MS. MITHAL: He's on the next panel.

MR. SWIRE: Okay, then -- well, he might not hear this, but I want to know if Justin's work at Consumer Reports, if there's a way that can or should

be incorporated into law by reference. If so, if we have really good consumer ratings on privacy, is there some way to give it even more teeth? I don't know if that's good or not, but that's my question to Justin.

I think, though, I'm trying to say some things that I think if Congress moves forward, and there's reasons why it should, having good findings, having good hearings, building a record will be important to how that law survives in the courts later on. The recital's in GDPR, but for instance on preemption, there's hundreds of different state laws, and there needs to be work done on issues like that to build a record so people know what's covered and what isn't. And unless that homework's done, there will be tremendous problems after passage of legislation.

MS. MITHAL: Okay, 30 seconds, Stu.

MR. INGIS: Well, congratulations on another successful couple of days. As I indicated, I think that there is -- it is the time now for a bold and strong new paradigm, a different approach, building on the successes of the various issues, the various laws. There are some pros, some cons to all of that, but I think this is the time, and I think we all need to work together on the details.

MS. MITHAL: Jane.

MS. HORVATH: And as the representative of industry on the panel, I think I will just reiterate that we are very, very much in favor of a federal omnibus privacy law. We think it's good for business and good for our consumers most importantly.

MS. MITHAL: Marc?

MR. GROMAN: First I want to say that given your current resources and authorities, I think the FTC has done an extraordinary job in this space, given what you have as authorities, and your statutory framework is incredibly impressive.

And then I am going to have a question for the next panel. So here's my question. If we have federal privacy law, there's been lot of discussion about preemption for states. I think equally difficult is if you have a federal privacy law, what happens to GLBA, HIPAA, FCRA, cable act, BPPA, FERPA and the other 18 federal privacy laws that all have different standards that contradict each other and are inconsistent, and when you remove them, you are going to have competitive effects. So when we do a federal privacy law, what do we do with the other federal privacy laws?

MS. MITHAL: Christine.

MS. BANNAN: Well, I want my last point to

be arguing against preemption. I think states are a lot more agile than Congress and are able to respond to emerging privacy threats a lot more quickly. No one thought that all 50 states and the territories would be able to enact separate data breach legislation before Congress could pass a bill.

So I think it's really important to preserve the state roles, and states have been a lot more effective than the federal authorities historically in protecting consumer privacy.

MS. MITHAL: Okay, with that I want to thank all of our panelists. Please join me in giving them a round of applause.

(Applause.)

MS. MITHAL: And we have break until 3:45, so please return at 3:45.

(Recess.)

PANEL: IS THE FTC'S CURRENT TOOLKIT ADEQUATE?, PART 2

MR. TRILLING: If everyone can please be seated, we're ready to start the last panel.

Okay, we are in the home stretch. We're back for Part 2 of our panel on the adequacy of the FTC's current toolkit for dealing with privacy issues.

Our esteemed final panel includes Julie Brill, the Corporate Vice President and Deputy General Counsel for Global Privacy and Regulatory Affairs at Microsoft and a former FTC Commissioner; Justin Brookman, the Director of Consumer Privacy and Technology Policy for Consumer Reports and a former Policy Director of the FTC's Office of Technology, Research, and Investigation; David Hoffman, Associate General Counsel and Global Privacy Officer at Intel; Lydia Parnes, a Partner at Wilson Sonsini Goodrich & Rosati and a former Director of the FTC's Bureau of Consumer Protection; Berin Szoka is the President of TechFreedom; David Vladeck is the A.B. Chettle, Jr. Professor of Law at Georgetown University Law Center and also a former Director of the FTC's Bureau of Consumer Protection.

I'm Jim Trilling from the FTC's Division of

Privacy and Identity Protection, and my co-moderator is Maneesha Mithal, also from the DPIP at the FTC. So we are going to start off the same way we started off the last panel which is to talk about metrics for measuring the success of the FTC's privacy work.

Julie -- I'm sorry, Lydia, I want to start off with you. How can the FTC and how can the public and stakeholders in general measure FTC success when it comes to privacy issues?

MS. PARNES: So, Jim, thank you. And thanks to both you and Maneesha for inviting me to participate in this panel. I just have to say what fun to do this after listening to the fabulous panel that went right before us discussing these same issues. So, you know, I think this will be really terrific.

So, you know, I agree with many of the sentiments that were expressed on the earlier panel about measuring the FTC's success, but I want to call out Marc and Stu in particular. I totally agree with Marc, I always have about everything, but, you know, on this point that it is very hard, maybe even impossible, to actually measure privacy, measure the effect of the FTC's efforts in the privacy area.

But, you know, I also think, as Stu said,

and, you know, I would imagine that almost all of us agree with this, the FTC has been extraordinarily successful in this area over the past, you know, 20 years, 25 years. Just it's been incredibly impressive that it has developed this -- what is referred to as this common law of privacy. It has done so because the staff is incredibly creative and also, I might add, because the people who wrote Section 5 really were brilliant. It is broad and it gives the FTC exactly the kind of authority to deal with issues that were never envisioned.

So, you know, when our panel met, Maneesha said this was going to be a really hard issue, and it is. So I've tried to kind of unpack it a little bit differently. You know, when you talk about the effectiveness of a privacy program, the first thing I think you have to do is define what the goals of the program are.

And to, you know, kind of set goals for any program, an agency like the FTC really needs to define goals that are recognized, you know in the community, by its important partners and stakeholders, and so valid with the Commissioners and the staff obviously, but also with businesses that have to implement these privacy programs, academics and others who study these

issues, the other government agencies who are engaged in adjacent enforcement efforts, you know, and also, honestly, the Commission's Congressional oversight committees. I mean, they are important stakeholders as well.

Starting at a very high level, I think you would get agreement that the FTC's core mission in consumer protection and in privacy as well is advancing consumer welfare in the market. I mean, those are the basics. It's very general, but it really is core. And I think it is such a central principle that you always really need to kind of come back to that.

I think the way it's played out in the privacy area is that, you know, it's really been about the FTC staying ahead of the curve. You know, the Commission, Commission staff has looked at the market, they've identified new technologies as they've been coming -- as they've been, you know, kind of coming to market. They've been internally noting what they think are potential problems and perhaps gaps and maybe misunderstandings at the business level of how the law applies to these new technologies. And they've been thinking very hard about what -- how old law should apply to these new technologies.

And then they've gone out, they've convened workshops and hearings like the one we're at today. They bring together stakeholders. They define what the standards and the guidelines should be. They articulate them. And then they set out expectations, they, you know, kind of translate all of this into understandable language so the consumers know what to expect. You know, that's a pretty complicated process. But really when you start thinking about measurement, that process seems easy.

I think it really is a challenge. We don't -- you know, I know that each portion of this panel only has a few minutes. So what I'd like to do is just lay out a couple of things that I think are worth having the Commission consider. You know, I started out, I was thinking about an article that Deirdre Mulligan and Ken Bamberger wrote in 2010, it was called "Privacy on the Books and on the Ground." And it reported on research that they had conducted. They interviewed, you know, kind of dozens of chief privacy officers who were -- had been identified to them as leaders in their field.

And among other things, they found that the emergence of the FTC as privacy regulator in the mid 1990s really had a very significant impact on

Corporate America's kind of effort to go out and hire chief privacy officers and invest in privacy -- in privacy programs within their companies. And companies and these chief privacy officers called out enforcement. They said, oh, yeah, we really pay attention to FTC enforcement efforts and we want, you know to, kind of do our best to have programs in place so that we don't get -- we don't get called out.

What Deirdre and Ken basically concluded is that then, I think as Marc pointed out, there was -- you know, in the ‘90s, there was this same debate we're having now about, you know, is privacy on the books adequate. And what Ken and Deirdre said is that while people were busy arguing about that, privacy on the ground was actually growing, and it was growing in very large part because of efforts that the Commission had entered into.

So I just want to kind of make one quick suggestion about a way in which the FTC can actually attempt to measure success. When the Commission steps into an area, identifies a new area, and like mobile apps was a good example of this, they are really investigating what this market looks like. And then they intervene, and then they see change. And I think in mobile apps is a good example. They did see, you

know, kind of no privacy disclosures and then after intervention very significant privacy disclosures.

I mean, this is something that I think the agency should do much more frequently and build it into reporting as well.

MR. TRILLING: Thanks for leading us off.

David Hoffman, do you have thoughts on how the FTC and other stakeholders should be measuring the FTC's work with respect to privacy?

MR. HOFFMAN: Yeah, absolutely. And I think Lydia's comments are fantastic. I would say that privacy on the ground has grown tremendously. A lot of that has been caused by the great work that the Commission has done implementing Section 5 of the FTC Act. I think as Marc Groman said on the earlier panel, I think the FTC has done a tremendous job given the resources and the authorities that it has.

I think, though, while privacy on the ground has grown, the risks have likely grown even more. And I think if we want to take a look at the risks, people in the United States are right now saying there's a privacy crisis. They want people to step in to provide better protections for them. That's why we had the voter referendum in California, that's why we now have the California Consumer Privacy Act. That's

why we have similar laws being created in over 20 states that would potentially create a nonharmonized patchwork that frankly, running a privacy operation for a large company, I have no idea how we would potentially implement.

I think much of this is driven by the fact that we have a completely unregulated industry of data brokers that don't get their information directly from individuals, I think, if you're looking for an opportunity to measure, measure and take a look at how advances in data analytics and data availability are transforming that data broker industry and the risks that they're creating and measure whether you're able to reduce that.

MR. TRILLING: Justin?

MR. BROOKMAN: Yeah, I would just say that I think, one way to -- or at the very least, I think, what would you need to do is there needs to be better alignment between consumer expectation and understanding or maybe even preferences and then actually privacy practices, right? Because I think today there is a huge disconnect between what actually happened. People have, like, a vague sense that their privacy is being violated, but they don't really know how, they don't really feel any urgency agency.

And so I think there's, like, a couple ways you could do that. One, you could kind of try to constrain data collection and sharing practices to be more consistent with context, to kind of get to where people expect it to be today. Or you kind of go the other way, get, you know, full transparency and make sure people understand what's going on. There's buy-in for this kind of dystopian surveillance of all against all. You know, Facebook's listening to our conversations. But the idea that, you know, pointing to the mobile app ecosystem as a good example of privacy on the ground and think people understand what's going on and then it's limited data collection and sharing, I think is a somewhat startling idea.

So we're doing actually some research right now into consumer understanding of privacy, and it's kind of like an arc you see every 20 years. Kind of starting out, people very cautious, nervous about being online, to people get kind of comfortable, social media becomes big. And then it's kind of coming back around, people starting to feel less comfortable, feel that their privacy, again, is being invaded in these ways they don't understand and they resist and rebel against but don't really understand what they can do or how to make the situation better.

And so I think narrowing that gap, however you want to do it, is necessary, maybe not sufficient.

MR. TRILLING: One of the related questions that has come up repeatedly during the hearing is how should the FTC or how can other stakeholders -- for example, how is Consumer Reports undertaking the task of learning what it is that consumers expect?

MR. BROOKMAN: Yeah, so, Peter -- one of Peter's questions was, you know, what the law needs to do to allow us to do our jobs. So Consumer Reports, in addition to advocating for better privacy laws and regulations, also tries to evaluate products based on privacy and security. We've done a number of those ratings. Some of the challenges we're running into -- so one, transparency. I'm sure we're going to talk about this with deception today, but, you know, companies have privacy policies. They have privacy disclosures. They're not really required to say much in them.

So if I'm looking at two apps' privacy policies, I don't know, it's really -- actually really quite challenging to say which are better. I know there is some debate around what the role of privacy policy should be. Should they be super simple and easy to read, right -- the Kennedy-Klobuchar bill does

that -- or should they be really detailed, not for consumers but for folks like the FTC or for Consumer Reports or for academics. And I lean very much toward the latter, that you should be required to put more detail about what you're doing.

Two other things that I jotted down in response to Peter's question. One, the deception statement today talks about deceiving consumers. I think that concept should be broadened to deceiving testers and maybe regulators as well. So, again, like the Volkswagen case, an example of, like, you know, running -- you know, secretly trying to figure out what's going on and changing how you perform in different environments. You know, we don't know whether what we're testing in the lab is performing as it would for a normal consumer, so maybe clarifying that as well.

And then just making things more testable. It's really actually hard to test a lot of stuff. And so, I mean, one, the law actually kind of just discourages it or makes it illegal in many ways. Getting rid of those prohibitions, but also maybe making some obligations of testability, opening up APIs so third parties can hold folks accountable. And I know Microsoft talked about this idea a fair amount,

would be a great idea.

MS. MITHAL: Okay. So why don't we move on. So I think the next topic that we want to cover is what are the gaps in the FTC's existing authority, because I think what we eventually go towards in this panel is what additional tools or resources does the FTC need, and we can't have that discussion without having a discussion of what the current gaps are. So, again, we're going to divide this discussion into two parts: gaps in our authority over unfairness and deception, and gaps in our remedies.

So I'm going to tackle the gaps in unfairness and deception. Now, I've heard really two points of view about unfairness and deception. One is that, well, you know, you can go after companies that deceive consumers, and you can go after harmful practices. What substantive rules do you need, and are there any other privacy practices that should be violations that are not violations under Section 5? So that is one point of view that the status quo is the right approach to protecting consumer privacy.

The other point of view is that unfairness and deception have severe limitations. They don't get at all privacy violations, and, therefore, we need a substantive privacy law.

And I just wanted to ask the panel where you fall on that kind of divide and if you have any thoughts about the limitations of unfairness and deception in this context. And maybe I could ask Berin to kick off that discussion.

MR. SZOKA: Sure. Well, let me start by just noting that the only two people of the eight privacy lawyers on this panel that have not worked at the FTC are David and myself. There's a lot of experience on this panel and a lot of people who have been in the trenches. And I would commend all of them and all the people who have worked at the FTC over the years on privacy but also consumer protection. I mean, the roots of what we're talking about here today go back for decades. And I think it's really important to take a moment to acknowledge and appreciate everyone who has done that work.

Lydia mentioned that the people who wrote Section 5, you know, specifically, she's referring to the Wheeler-Lea amendment of 1938, they were very forward-looking. But if you really want to go back and look at where the FTC gets its ideas today and to start to answer your question, Maneesha, I think you have to go back and look at the fundamental policy statements that have guided the FTC to where we are

today.

So I'm just curious, as I get started here, I just want to get a sense of the room. Tell me where you think this quote came from: "There are many more or less sentimental considerations that the ordinary man regards as important." So do you think that was something that David said or something you hear today from a democratic FTC Commissioner? Any guesses?

Well, I'll tell you, you might be surprised, this came from the Republican FTC in 1983, in the deception policy statement, all right? So if you go back and you read these fundamental documents -- and I try to do this whenever I re-engage on FTC issues in a deep way. I go back and re-read both of them. There's a lot there, a lot of distilled knowledge about how consumer protection law evolved in America.

And one of the things you realize when you read those documents is that some of the things you think of as partisan today, they're not. They're really about how to think about harms and how to measure consumer expectations and vindicate them.

And it's often said that the FTC's job is to protect consumers against harm. Well, that is the primary thrust of the FTC Act, and that's what unfairness requires, and that's what you see in the

1980 unfairness policy statement. And you'll see language in there that expresses some skepticism about nonfinancial, nontangible harms, and there are real questions about how to measure those things. But if you go back and look at the deception policy statement, which was issued not by the Carter FTC, as the unfairness policy statement was, but by the Reagan FTC, you see the sentiment that I just expressed to you.

And the reason that the Commission gave that weight, quoting the statement on torts in that particular quote, gave that weight to subjective considerations was that they understood that if you looked at those through the lens of what affected consumer behavior, of what was material, of what caused consumers to make decisions based on something that was told to them or something that should have been told to them -- an omission -- that you could get at a lot of the problems of consumer protection law that were otherwise insoluble, that required too much direct evidence, that a regulator would never be able to show to be an effective cop on the beat for consumers.

So to go back to your question, Maneesha, I put myself in the middle. I think that we don't give

enough credit to the people who wrote those two policy statements and to what actually could be done under the frameworks of deception or unfairness today. The discussion on the last panel about materiality really illustrates the point. We can talk more about this later, but I think people have not really thought about materiality in a rigorous way because the deception policy statement allows the Commission to presume materiality in cases of explicit statements. And because they've done that, the only cases where the Commission's had to really demonstrate materiality have been in omission.

So number one, I think if we thought more about that, we'd actually start to have an analytical lens for thinking through these problems. But, two, even if you think that the current approach to unfairness or deception are too limited, it doesn't mean you should throw them out and start with something completely new.

From my view, the history of consumer protection law in the United States is that Congress has come around again and again and enacted specific statutes that build upon those concepts, that effectively say that certain practices -- like for children's information or credit reporting -- are

presumptively harmful or are presumed to be material to users.

And if you take that approach, you can see an approach that evolves out of those concepts. Now, it doesn't break with them, but it grounds whatever it does in those terms, and in particular, it means that if you're going to craft a flexible standard, like respect for context, say, that you do that in thinking about materiality. And if you do that, I think you wind up in the middle.

MS. MITHAL: Okay, thank you.

So let me follow up with two questions to anybody on the panel. So the first question is, is unfairness and deception enough, or are there gaps that substantive privacy legislation needs to fill? And the second question I want to pull on one of the threads that Berin mentioned about presumptions of materiality.

So we had a case a couple of years ago where we had different statements from Commissioners involving a deceptive statement in a privacy policy. And some Commissioners said that we should not presume expressed statements and privacy policies are material because consumers don't read those privacy policies. And so I think they were highlighting a potential

limitation of deception.

So I wondered if anybody had a comment on that. Again, the two questions, the more general question and the more specific question about deception. Does anybody want to take on either of them?

David? David and then Justin.

MR. HOFFMAN: Yeah, let me start with the unfairness policy. First of all, Berin is plainly right that the FTC Act has been augmented over the years. I think there are now more than 70 statutes in addition to the FTC Act that the FTC is charged with enforcing. So it's not just an accretion. It's been sort of a landslide of the statutes.

But, you know, these statements take on a life of their own. There's a common law of unfairness and there's a common law of deception. And I think that, you know, it's interesting, the first of these hearings, Tim Muris talked about the unfairness statement and cited the Pfizer case, which was a case in which there was noneconomic injury, but it was an unfairness case. It was not a deception case.

My own view is that's the right reading of the unfairness statement, but that's not the way the Commission has been viewing it for the last decade.

And so it may be that we need to retool or tinker to get back to what, you know, an originalist would call the original intent. Because if Tim and I agree about how to read the unfairness statement, it's got to be right.

(Laughter.)

MR. HOFFMAN: So that's the first point. With respect to materiality, I think -- I think the question that Berin raises is a fair one, but I think the reason why the statement is written the way it is is simply out of, again, a history in which materiality was easy to prove. There's always a defense that a statement is nonmaterial, but the Nomi case, which is you're talking about, was just a lie. It wasn't deception in the sense of a misstatement. It was just a lie.

People were told that if they did certain things, if they wanted to opt out there, they could do it, but if not, they could opt out when they go to the store. That was just not true. It may not have been their intent, but it was a false statement. And under FTC law, false statements ought to be actionable.

MS. PARNES: I'll promise that we'll argue about this later over drinks.

MS. MITHAL: Okay, Justin.

MR. BROOKMAN: Yeah, so, I mean, I think you can cram a lot into unfairness, right? I mean, I think the Vizio case that's been talked about is a good example. That's a case where effectively saying the collection of -- you know, first-party collection of sensitive data without clear permission is illegal, right, and if that really is the case, then, like, again, the mobile app ecosystem, where geolocations are traded all the time, maybe that's all illegal today, right? If TV viewing is sensitive, then why isn't web browsing, right? So maybe you could get to all that. I think it would probably be better to have a dedicated law clarifying what the obligations are.

I mean, we can try to do it in unfairness. But maybe let's do it more consciously and try to decide what actually is there. Again, things like access, correction, deletion, you can argue, I guess, that it's unfair to do that. Again, I think a dedicated law would be better.

Getting quickly to the point around materiality -- and it does tie into what I said around testing -- again, privacy policies aren't for real human beings. They're for folks like me. We rate products based on privacy policies. We are the -- we distill that information to consumers to digest that

in reasonable ways. If companies are allowed to lie at will in privacy policies, we can't convey that information to them, and, therefore, it translates to misinformation in the marketplace.

I know this is the hobbyhorse of barons, I have never understood it, but having some sort of affirmative obligation to say to the world what you're doing so folks can hold people externally accountable is a fundamental idea.

MR. SZOKA: Well, may I try to explain? This is a false binary. I'm not arguing that privacy policy statements can't be the grounds for deception actions. The question that Maneesha asked us is should we presume that every statement in a privacy policy is material. And my answer is no, that the FTC should have to prove that. And the reason is you go back and read the deception policy statement, and you read Central Hudson, the Supreme Court case that set forth the commercial speech doctrine, which was quoted in this deception policy statement, the Court specifically says, in the absence of factors that change the incentive to make the statement -- yes, we presume that a statement made in an advertisement is material.

But what they and the deception policy

statement made clear is that we're only presuming that because that makes sense in the context of something that a producer says to convince a buyer to buy the product.

Where that relationship does not hold, you can't make that presumption. And if you do, you dispense with the entire analysis by which the Commission got to that point. This is just clear on the face of the deception policy statement.

Now, again, I think that you should be able to pretty easily show that these things are generally material, but not always. And the Nomi case is really important, and I wrote a long paper about this with Jeff Manney, the key detail in Nomi, yeah, I agree it was a problem, right, and it could be actionable, but the thing is that the statement they made was a statement that -- made on the website -- that you could opt out in the store so that anyone who went to the website who saw that thing had the ability to opt out right there on the website.

The Commission's argument was, well, what about the consumers who went to the website and didn't want to opt out there but might have wanted to opt out at the store; when they got to the store, there was no opt out? Oh, come on. That can't be material. It's

a false statement, apparently the result of negligence by the part of Nomi to implement that system.

MR. VLADECK: You can't be negligent when you make a false statement --

MR. SZOKA: But hold on, my point -- my point is that you're conflating, David, the idea of the misleadingness of the statement with the ability to presume without evidence that it's material. And what this really gets at is that the Commission, because of this presumption, has not developed a concept of materiality, an empirical methodology, that would be useful in other cases that we see today, like Facebook didn't tell anyone about the Cambridge Analytica thing. Was that material? Seems so to me, but I don't know what to point to in showing you what the methodology looks like. I would like to see more of those cases litigated.

MS. MITHAL: Okay, as much as I would like to continue this, I'm going to call on Julie next, but let me just throw another question into the mix as we're contemplating this issue, which is that it does seem that people have said that there may be some limitations in unfairness and deception. And so let's assume -- you know, we're going to talk about kind of potential legislation -- but let's assume that it

takes years for Congress to enact legislation or Congress doesn't enact legislation right away. And so we have the unfairness statement and the deception policy statement. Should we modify those statements to take into account privacy issues?

So, Julie, you wanted to chime in, and you can chime in on this question or --

MS. BRILL: Sure. So first of all, thank you for inviting me, and congratulations on not only this set of two days but also the entire set of hearings. I think they're incredibly interesting and really raising some great questions. If we were to take this conversation and bring it to Brussels or bring it to Beijing or bring it to Sao Paulo or any other capital, it would be very, very foreign. This notion that we should be focused on unfairness and deception is a conversation that the rest of the world is not having about privacy.

So if you wanted to really think about an appropriate metric for privacy, one argument would be to what extent is the FTC affecting the actions in boardrooms? To what extent is the FTC the topic of conversation in C-suites? I'm a big, huge fan of the agency. This has nothing to do with you all. It's really about, I think, the laws and the relevance of

the laws today.

I'm also a big fan of Deirdre's book that Lydia talked about. It was written in 2015. This was before GDPR. It was, like, kind of as GDPR was kind of going through some of its final stages. I think if that same book were written now, it would be -- there would be a very different reaction in the C-suites, even among CPOs and whatnot.

It is true that in America we have a deep culture around compliance, and that is a very big difference here in the United States than it is in some other places of the world. But right now, when people are thinking about compliance, they are not thinking about the FTC Act. They're just not.

They're thinking about other laws around the world, and in particular, about GDPR. So if we really want to have a metric that says the United States and its enforcement agencies are going to have an impact on the way data is used and on the way that privacy is treated, I think that we really need to modernize our notion around harm and around unfairness.

So I would say, first of all, I hope your hypothetical is wrong, okay? I do think that Congress needs to enact a law. And if Congress doesn't do it, I think the states need to do it. And so we can

debate about preemption later on perhaps, but we need to have baseline privacy legislation, whether enacted in the states or enacted in Congress, that is going to engender more trust, is going to bring the United States back to relevance in the conversation around how data is used, and that really looks at the data economy as it exists today.

So when you think about the data economy as it exists today and you think about the materiality -- sorry, the unfairness test, one of the big problems is around harm. I, when I was a Commissioner, I was always worried, as Maneesha knows, that we didn't bring enough cases that were pure unfairness cases. And the reason, often, was because there was debate at the very highest levels of the agency among the Commissioners as to what was appropriately deemed to be harmful.

So I think that, actually, we should take this out of the hands of the Commissioners now. I think the Commissioners shouldn't be debating this anymore. This is a policy question that Congress should decide or that state legislatures should decide, because we need to see action. We need to see some guardrails put around some of this activity.

MS. MITHAL: Okay, David, last word on this,

and then we'll move on to the next topic.

MS. BRILL: Okay, but I didn't get to your real question. So I'm happy to go on. But I actually think that if there is -- sorry, David -- if there is no action by Congress, then I think the FTC needs to look much more broadly at harm, because otherwise, you know, you won't have any role in how data is being regulated going forward.

MR. HOFFMAN: Real quickly, I just want to say I completely agree with what Julie said. And I want to bring up some of the things that Julie actually said while she was a Commissioner, where she really was addressing issues around the lack of ability for people to have any obscurity in situations where they're participating in our economy and in our democracy.

It is, in my opinion, completely untenable in the United States right now that we have victims of domestic violence who change their names, move across the country, and for less than $10, people can go to a data broker website, associate the old name and address with the new name and address, and for those victims to have to live that way.

It's unconscionable for police officers to have to worry that their children's names are put on

the internet. And it's completely unreasonable for judges to have their home addresses put on the website. Do we have to wait until people take action and commit violent acts because of that? Or do we get to recognize that there are concepts around harm that haven't been identified before and that need to be included. If we can't, I completely agree with Julie, the time is now for federal privacy legislation that gives more authority and resources and focus for the FTC.

If we can't have that, we need to take a look and say these actions are completely unreasonable in an environment where more data is being made available. Particularly it's important for society to have more data for the training of AI algorithms to benefit society, and our level and ability for doing data analytics to derive things from that data and to sort that data has greatly improved.

MR. TRILLING: Before we -- oh, go ahead, Lydia.

MS. PARNES: Kind of one really quick comment. You know, I -- Julie, I complete -- and David -- I completely agree that the time is right for federal legislation. You know, I can't imagine, you know, on the panel before us where everybody just went

right down the line and everybody supports this. I don't remember a time when that occurred.

But, Julie, one thing. I mean, I think that -- I agree with you. I don't think that people in the C-suite think about unfairness and deception. They don't think about those statements. But they do worry about FTC enforcement. They really -- they do --

MS. BRILL: No, they don't.

MS. PARNES: People who are responsible for privacy --

MS. BRILL: They don't. I mean, look, I -- if the -- if the lawyers come to the CEOs and they say, okay, we're being examined by the FTC, then, yes, it becomes an issue that they worry about. I do agree with that. But it's not in everyday planning about how data is used. It's not in developing products and services that people are sitting back and saying, oh, gosh, what is Maneesha going to say about this?

That's what I mean. I'm talking about thinking about the guardrails that are put around activity before you engage in that activity. That is where the C-suites are -- honestly, they're just not thinking about the US restrictions.

MS. PARNES: So I -- you know, I completely agree that this is the time, but, you know, day in and

day out, we're counseling companies on exactly what to do before they roll out products. So -- and they are concerned about what the FTC reaction will be.

MR. SZOKA: And the FTC has been much more aggressive on enforcement than the European DPAs have.

MS. BRILL: I agree that the enforcement regime and the compliance regime is -- I don't disagree with you, Berin. I do think that things are changing in terms of the European regulators, and I think that they are becoming more aggressive. Just look at the last, say, six to eight months, and there's been a sea change there. But the tradition in the United States has been one of taking a look at activities, coming within the radar of the FTC's sort of, you know, enforcement regime, and then people start to pay attention.

MR. TRILLING: That's a good segue to talk about what the FTC has been doing in terms of its enforcement work and what its orders have generally looked like in the privacy space. And I want to start off with David Vladeck for your general thoughts on whether the FTC is using its existing toolkit effectively in FTC enforcement actions.

For example, we heard on the last panel, and we've also heard others in the hearing express the

concern that the core of the FTC privacy orders, the comprehensive privacy program provision that requires an independent third-party assessment of a defendant or respondent company's privacy program is not rigorous enough, that the effect of being under order does not do enough in terms of providing public information about the company's practices. What are your thoughts on those issues, David?

MR. VLADECK: So, you know, I think the one -- there are two serious holes in the FTC's remedies. One is the lack of initial fining authority, which may be why Julie thinks that the people in the C-suite really are not worried about the FTC. If you can't fine them for the first shot across the bow, that's a real problem.

The other is the inability to get damages because most of the privacy cases we bring, the FTC brings, there's no financial remedy. If there's no civil penalty, there's no remedy. The only provision for damages in the statute is in Section 19, which is rarely used. But the statute ought to authorize damages, real damages, in Section 5 cases, in Section 13(b) cases.

And so in a case like Google Buzz, where the rollout of Google revealed all sorts of personal

information, the Commission should have had at least the option of seeking damages because civil penalties are not available. That might have been a deterrence. And it's very hard to quantify any other form of information -- any other form of damages. So in terms of -- and, of course, I think the agency needs notice-and-comment rulemaking.

In terms of how the agency is using its authority, there's more that could be done, but there's a tradeoff. The FTC could require admissions of liability. It traditionally does not, but if you wanted to increase the pressure on companies and get Julie and her colleagues in the C-suite worried, that would be a tool to use.

You know, there are more personal liabilities. You know, the agency does not often go far down the chain in terms of personal liability. And in terms of the -- you know, I helped design the first reporting requirements in privacy cases, and I think the Facebook problem and others have shown that it's not sufficiently rigorous. I think there needs to be -- and I haven't seen the current versions -- but there needs to be greater transparency. They ought to be more frequent than every three years. I mean, I think the agency really ought to rethink

whether the transmission belt that was designed in the first generation of these orders needs to be ramped up.

LabMD I think is an irrelevant case because it's the only litigated data security case. No one who's ever consented to an FTC decree would have the chutzpah to say, I just didn't understand what I did. In that case, they should sue their lawyers, not the FTC, but the consequence will be, I suspect, that there will be much tighter orders going forward.

You know, the agency can write tight orders. We did this with -- with ad substantiation. There's no reason why the FTC, if the industry says it needs more guidance -- though I'm sure no respondent in any case would ever say that -- but if the industry needs more guidance, the agency can provide it. So I think there are all sorts of tools the agency has to toughen up its practices.

Let me just say one last thing about comprehensive privacy legislation. I think there's a lot Congress ought to do without privacy -- comprehensive privacy legislation to bolster the FTC. I mean, the resource issue is just enormously -- it's enormously overdue. Congress should have addressed it

a long time ago.

But, you know, one of the concerns I have is federal legislation is essentially inevitable anyway because you have the California law. Once another or two other states pass statutes, you're never going to have the dystopian sort of -- I forget what David called -- you know, a disuniform state law because the dormant commerce clause is going to kick in. That is, at some point, when the second or third state tries to regulate companies that are doing business nationwide, they're going to sue under the dormant commerce clause and win.

So the question isn't whether there's going to be federal comprehensive legislation; the question is when should it take place. And, you know, my own view is let a couple of other states pass their statutes. Let's see what kind of experimentation there is in the states. Because, ultimately, at some point, the dormant commerce clause will force some sort of uniform national law.

MR. TRILLING: Responses or reactions, especially to what David said about the remedies issue in particular? Berin.

MR. SZOKA: Yeah, I'm looking forward to David joining us as an amicus in our challenge to

those state laws. I'm not so confident it's going to work out so easily. And by the way, the term "patchwork" is the wrong metaphor because a patchwork is, you know, every state has their own laws for inside their state, which is what happens for data breach notification. What we're talking about for privacy is every state regulating everyone. That's not a patchwork. It's an enormous pile of many, many layers of regulation, so it's even more of a problem.

Anyway, but getting back to the question of remedies. Look, there's a lot going on here. First of all, it's a problem whenever we start saying that appellate court decisions are irrelevant. They're not irrelevant. They constrain the agency. And in particular, the specific clause that was at issue in the proposed remedy that the FTC was seeking was one -- the same one that the FTC imposes in all of its privacy, in all its data security cases requiring a comprehensive program to have reasonable data security or reasonable privacy in privacy cases.

And the 11th Circuit said you have to have specificity in your order. Now, maybe the FTC can do that, right? But that's going to be -- that's a real change that they're going to have to make in how they handle these orders. But that's only one --

MR. VLADECK: But that's a litigated order. It's not a consent order.

MR. SZOKA: Yeah, I know, but, David, the point is that, you know, sometimes people actually might want to litigate, and maybe we're not just going to have another 20 years of 200 cases not getting litigated. You know, maybe we'd all agree that it would be a good thing if the line in unfairness policy statement by which the FTC promised that it was going to be the courts and not the Commission that was setting the boundaries of the law was actually taken seriously.

Now, I'm not blaming the FTC for that, right? But there are all sorts of reasons why all these cases just settle. And, primarily, it's because privacy is so darn sensitive, because contrary to what Julie was saying, people really do care about their company being put in the crosshairs and being on the front page of the newspaper, right? That's why these cases settle fundamentally.

We can talk more about that, but this remedies issue is a really important set of problems. So on the one hand, David says, well, we should have monetary remedies, even though we can't measure the harms that are being inflicted in privacy cases.

Well, if you can't do that, I'm not sure how you calculate what the remedy is.

And then you're talking about civil penalties. Okay, so if you want to have a conversation about civil penalties, I'm willing to have that. But when you do that, you have to understand, first of all, why the FTC Act today does not include civil penalties for first-time violations, and the answer is very simple. You cannot marry an incredibly broad law that is incredibly vague with the ability to impose penalties upon a company that simply fails to predict where a line is drawn, right? That is bad policy, and it may be unconstitutional.

What is appropriate and constitutional is when companies have notice of what is unlawful, where the violation is so extreme, as it is in fraud cases -- that's a -- that's a, you know, kind of deception case today. In those cases, yeah, sure, it's appropriate to go after civil penalties. But our guiding star in thinking about penalties should be does the regulated party have notice, and where they do, that's appropriate.

Just one more thing about penalties. The FTC has now lost a series of cases, right? And this is now going before the Ninth Circuit, if you're not

following this. There's a Shire case that's about the injunctive order part of this. But Kokesh, I've written about this, is about whether monetary remedies under statutes like 13(b) are, in fact, penalties. And the Supreme Court in Kokesh, in a case not involving the FTC, said yes, they are. And this is now --

MR. SZOKA: Just a second.

MR. VLADECK: This is now before the Ninth Circuit. And if the Ninth Circuit says that the FTC can't get, like, monetary remedies like disgorgement and restitution under 13(b), that's going to be a real problem for the agency in cases where everyone thinks they should be able to get that money, like in hard-core fraud cases. That's going to require legislative action immediately. It's going to be far more urgent. Maybe it will push some of these things over the goalpost, but we cannot simply dismiss these appellate court cases as irrelevant.

MR. TRILLING: Did you have something very quickly, and then I want to go to Julie and Justin.

MR. VLADECK: Let me read a sentence from Kokesh, because Kokesh is actually quite clear in distinguishing between compensatory disgorgement and noncompensatory disgorgement. The court says that a

pecuniary sanction operates as a penalty only if it is sought for the purpose of punishment and to deter others from offending in like manner, as opposed to compensating a victim for loss. So the Supreme Court quite clearly --

MR. SZOKA: It's not clear, David. There's other language -- there's other language in that decision that suggests that if it's not done by statute for the sole purpose of compensation, it's at least in part a penalty.

MR. VLADECK: No, so there are now --

MR. SZOKA: We know how to litigate this case.

MR. VLADECK: -- there are nine --

MS. SZOKA: The point is the Ninth Circuit may resolve this for us.

MR. BROOKMAN: No, they both have 10-page papers addressing their arguments that we can point to.

MR. VLADECK: There are nine -- there are nine cases so far --

MR. TRILLING: I actually was going to suggest that maybe we are developing a theme of issues that panelists need to go discuss over drinks.

(Laughter.)

MR. TRILLING: But, Julie -- Julie wanted to --

MS. BRILL: Well, this -- I hope this won't be the same thing. Just, Berin, I agree with you and disagree with you. So just to be really clear about what I was saying, I think people care about the FTC when especially the FTC comes calling. Nobody wants to be the subject of an FTC investigation.

I think the standards right now are so vague -- unfairness, deception -- that it's really hard to action them. In contrast, when you look at other privacy laws around the world, they are deeply progressive. They have deep relevance to how operations are -- take place within companies. And these laws force the C-suites to be thinking operationally ahead of time about how they're approaching data use. It's just a completely different way of thinking about regulating data.

So, yes, of course people care about the FTC, but, you know -- you know, how many times is the FTC going to come calling any one particular place? So that's one thing in terms of that issue.

But I do agree with you, Berin, that in some ways, we need more definition. And I personally believe that it should not be the courts. I think

that Bill Kovacic makes a great point when it comes to the competition issues that sometimes when you leave this just to the courts, the courts get pretty conservative, especially if you throw in a private right of action or treble damages. They'll get really conservative. And that may be one of the reasons why we're in the state that we're in with the competition laws.

I would much rather have policymakers set policy, the policy here that needs to be set for all the Commissioners so that Maneesha can with confidence go forward with an unfairness case, which I want her to do more than anything else in the world and have for the past 10 years, is to say, you know, give her a little bit more meat, so that when she meets with each of the Commissioners, she can say, well, this is what Congress has said is unfair. You guys don't need to debate it anymore.

Reputational harm is unfair, just as one example. So that -- so I do agree that there needs to be more definition, but I think that it should be Congress that makes that definition or state legislators make that definition, and then the states and the state AGs will decide.

MR. TRILLING: And to give Maneesha the

resources so she that can fight that litigation.

MS. BRILL: Oh, well, we're going to talk about resources in a minute because I have a whole bunch of things to say about resources.

MR. HOFFMAN: I don't disagree with you, Julie.

MR. TRILLING: But first, actually, Justin had wanted to weigh in.

MR. TRILLING: Maybe the moment has gone.

MR. BROOKMAN: Super brief. Super briefly. One, I remain skeptical that privacy programs and assessments are ever going to be super meaningful, so I think reforming that process is -- I don't think you're going to get the benefits from that. I think there are strict liability costs of having a privacy order against you. Having talked to a lot of companies who have them, I don't think they meaningfully changed their behaviors.

I think, you know, doing more fencing in -- again, maybe leaning into your unfairness authority, both, you know, making more aggressive claims and complaints but also an order saying in order to comply with the law you need to do X, Y, and Z. Again, I think it's a knotty substitute for a privacy bill, but I think there's more -- to be more aggressive in

negotiating for fencing-in relief and orders.

Setting aside the law around disgorgement, I'm not sure what the FTC's policy is. I mean, I think there should be more -- I think, as a matter of course, they should try and ask for it in more cases to get disgorgement of ill-gotten games. We filed comments on the Patriot case as one example of a place where they probably should have gotten disgorgement of ill-gotten gains. At the very least, articulate and enforce a policy, because right now, I think there's not a lot of clarity around that.

And, finally, I just want to echo David's point around personal liability in more cases, I think, would be a deterrent behavior.

MS. MITHAL: Okay, thank you, Justin.

We're going to move on to the next segment, which I think everybody has alluded and everybody really wants to get to, which is what additional tools do we. And if we need legislation, what should that legislation look like? So, again, I want to divide this discussion in two parts. The first I want to talk about tools; and, second, I want to talk about what the substantive requirements of legislation should be, all in 20 minutes.

I know we could do a whole panel on that

second one, but let's just hit the highlights for this 20 minutes. So first in terms of tools, David has already talked about civil penalty authority, and I just want to touch on two additional things. One is I want to ask if the FTC -- if you believe the FTC needs more resources, and regardless of whether the FTC needs more resources, what are the areas we should be focusing on? And second, should the FTC have APA rulemaking authority, because that has been controversial in the past, and I wonder what people's thoughts on that were now.

So maybe I could start with Justin on those questions.

MR. BROOKMAN: Yeah. On staff, I'm fairly confident you'll have universal agreement up here that the FTC needs a ton more staff. Chairman Leibowitz pointed out they're about half the size that they were in the ‘80s. The economy and the population has grown tremendously in that time. Meanwhile, other agencies, like the FCC, have kind of dumped their responsibilities on the FTC, saying we're not really interested in this anymore, you all take care of it.

I think it's really a mixture of both lawyers and technologists. You know, especially, there are a lot of libertarian folks who are arguing

you need to litigate more cases. Litigation is really labor-intensive, and so I think even under, like, the existing consent order model, you would need, like, to increase their staff tenfold. If you're going to make them litigate every case, you need to increase it a hundredfold.

Also, I think you absolutely need more technologists at the agency. Yeah, I think this has been a recurrent theme that you've heard from a lot of folks over the years. I'm a little bit disappointed that there has not been a chief technologist appointed to guide the agency during this time. You know, my group, OTEC, when I joined the FTC a couple of years ago to help kind of bring more technical expertise to the Federal Trade Commission, you know, never got higher than more than 10 people, now I think down to maybe 5.

And so, again, like, getting it up to 10 is not going to solve all the problems. They need, again, orders of magnitude more. But, again, there are FTEs out there that should be filled to help do the best that they can right now.

Just quickly on APA rulemaking, I think -- in general, I think they should have discretion authority. I don't think they should be directed to

issue regulations, but especially if people are concerned around fair notice, you know, the best way to give people fair notice is to have more precise rules around evolving issues. So I think it absolutely makes sense to give the FTC rulemaking authority around privacy.

MS. MITHAL: Okay. Anybody else want to chime in on this?

MS. BRILL: I'd love to chime in on resources. And I understand that everybody says you need more resources, but I think it's important to sort of look at this in a global context of what is happening, again, around the world. Chairman Simons recently said, Maneesha, you have 40 people on your team. I can't believe what you're able to do with 40 people. You are definitely like the proverbial wizard behind the screen, don't look at the man behind the screen in "The Wizard of Oz." You are amazing with what you can do, but I want to put it in context of what's going on around the world.

So that means that with 40 people and a population of 329 million, that there's one employee on your team per 8.2 million Americans. Okay, so let's keep that in mind -- 8.2 million Americans. The Irish, which have become the lead data protection

authority for many companies in Europe and are a very significant regulator, have 180 employees, a population of 5 million, which gives them one employee for 28,000 citizens. Again, they have a global responsibility, but, obviously, so do you, given all the companies that are here. So one per 8 million in the United States versus one per 23,000 in Ireland.

Let's add in the UK. We're not exactly sure where the UK is going to wind up, whether it's going to be in Europe or not in Europe, but still they have 65 million people in the UK, 180 employees. And that means -- I'm sorry, 700 employees, one per 93,000 British citizens.

I mean, these numbers just are remarkable when you put in context the resources that you have. And when I think about resources, I completely agree with Justin. It should be lawyers. It should be technologists. It needs to be economists. I think that these teams really need to work together. I think you need litigators and you need people who are sort of subject matter experts. It needs to be sort of a robust team.

But the notion that the FTC as the sole regulator here in the United States is governing, you know, thousands and thousands of companies that are

affecting not just people in the United States but also globally, and you're the -- you're the lead regulator with, you know, 40 people, it's -- remarkable.

And then the other thing that happens in Europe that does not happen in the United States, I think most people here are aware, but, actually, the European data protection regulators are required to work together when there is a cross-jurisdictional issue. By statute, by the regulation, they're required to work together, which means they get to augment their resources with each other. There's no requirement here that the state AGs have to work with Maneesha's team or that Maneesha has to work with any particular state AG. And often -- sometimes they do and sometimes they don't.

So we can't -- you know, when I have conversations on the Hill with senators and representatives and their staffs, they look at me and they say, well, those are really interesting numbers, but what about all the state AGs? And I say, well, you know, there's no requirement that they work together. So you can't really, like, lump them all together.

So the resource question is just out of

control. And I just hope -- whether there's legislation enacted or not, I really hope in some budget context or otherwise that this is taken care of.

MS. MITHAL: Anybody disagree with anything that's been said?

MR. HOFFMAN: I don't disagree but I have one thing to add, which is I just think we shouldn't lose sight of the tremendous responsibility that the FTC should have on educating people and the resource requirement that would be required for that. Too often, we say that privacy regulators should just be focused on enforcement. Individuals could really use a lot of education in this country about how data is being used to harm them.

MS. BRILL: The 40 doesn't count, the people in the consumer --

MS. MITHAL: There's a big team.

MS. BRILL: Yeah, there is. Yeah, yeah, yeah. Just to clarify.

MS. MITHAL: Throughout the agency.

MS. BRILL: I don't -- I disagree -- I agree with your fundamental point, absolutely.

MS. MITHAL: Okay, Lydia and Berin, and then we'll move on.

MS. PARNES: I actually want to raise a question. You know, folks have talked about APA rulemaking authority across the board, and, you know, I think in this area, I don't know if the FTC got across-the-board APA rulemaking authority and then adopted a privacy rule whether it would address one of the real challenges, which is preemption.

I think that needs -- I'm kind of raising that as a question because the FTC has never had across-the-board APA rulemaking authority. But I don't know that it could issue a preemptive rule on its own.

MS. MITHAL: Yeah, and I think -- I was really asking in the context of legislation. So assuming specific privacy legislation was passed, should we have APA rulemaking authority.

Berin, I'll give you the last word on this and we'll move on.

MR. SZOKA: Yes to more resources, especially for technologists. On the question of rulemaking, as with civil penalties, it's not a binary. The question isn't whether the FTC should have more rulemaking. Congress has always passed statutes that give FTC the rulemaking authority, but that's the right way to do it, to focus the grant of

rulemaking authority on a clear set of problems.

What I have a problem with is marrying rulemaking authority with an incredibly broad standard like unfairness, right? That becomes, then, a blank check by which the FTC becomes, as it was in the 1970s, the second national legislature. Let's remember, it was not some sort of libertarian crackpot, Reaganite band that tied the FTC's hands on rulemaking. It was a Democratic Congress in the Carter Administration, okay, and for good reason.

So rulemaking, like civil penalties, needs to focus on clear, specific problems. And once you have those safeguards in place and the FTC has a lane to work within, sure.

MS. MITHAL: Okay, so now, let's move on to kind of substantive requirements of legislation, on the last panel, I did a thing where I asked people to raise hands, and I'm going to ask people to do that again. Maybe I should have quit while I'm ahead, but I'll do it anyway.

So throughout the two days, we've heard about potential goals for privacy policymaking and privacy legislation. And we -- I think there are four of them, and, please, feel free to add if you think this is not kind of -- if this doesn't encompass the

goals. Thank you.

The first is preventing harm. And you can raise your hand for more than one. I'll go through them first. Preventing harm, improving transparency and consumer control, avoiding surprises, complying with consumers' expectations, finally, promoting competition and technology and the benefits of technology.

Okay, so how many people on the panel agree that preventing harm is one of the goals of privacy policymaking?

MR. BROOKMAN: The primary goal?

MS. MITHAL: One of the goals, one of the goals.

MR. BROOKMAN: A goal.

MS. BRILL: So we can vote for all of these?

MS. MITHAL: You can vote for all of them.

Okay, improving transparency and control.

Okay. Avoiding surprises, comporting with consumers' expectations.

Okay. And promoting competition and ensuring the benefits of -- okay.

Wait. Did somebody -- okay. So, okay.

MS. BRILL: But I don't think that's everything.

MS. MITHAL: Okay, please, what is missing from that list?

MS. BRILL: Accountability. I think that you need to instill accountability in companies. I think that focusing solely -- and I'm not saying that you've left it out, necessarily, but I think it needs to be called out specifically that we need to move away from sort of a notice and choice regime where everything is placed on consumers and they have to make every decision with every website or every, you know, IOT device that they use. And, instead, I think -- excuse me, in addition, I think we need to also add in corporate accountability.

MS. MITHAL: Can I just follow up with that? Okay, so let's -- can you kind of give us any ideas of how that could be included in legislation? So we know that in GDPR, there's a DPO that's required, there's risk assessments that are required, there's kind of a regime built around that. And we've heard -- you know, again, that may be one thing for companies like Microsoft, but how do you legislate it for a broad range of companies, a broad range of sizes -- and it's not sizes --

MS. BRILL: It's not sizes.

MS. MITHAL: -- it's how much personal data

they collect.

MS. BRILL: Right. Well, and it's also -- so there are things like requiring some kind of person in the company to be responsible for this is a good idea, but I don't think it's necessary. I think the risk assessments are really the key. And risk assessments, like having to surface an individual's data, having to give them access to their data or allowing them to delete their data, these two things coupled together, the data subject rights plus risk assessments -- do a tremendous amount for data hygiene. If you have to surface data for an individual, you have to know where it is. And you have to be -- you know, you have to either tag it or figure out you don't need it anymore, you're going to delete it. It promotes data minimization. It promotes all sorts of great data hygiene.

Similarly, risk assessments require companies to take a look at what they're doing and to explain to themselves first, is this okay?

MS. MITHAL: So, okay --

MS. BRILL: But in terms of the size of the company -- I just want to say one thing real quick -- Cambridge Analytica was -- had 100 employees. It was a small company. The issue should not be about the

size of the company. The issue needs to be about the type of data, as you pointed out, but also the agility of the company.

What we find -- you know, we have millions of customers, all different sizes. We find that the smallest companies actually in many ways have the easiest time with some of these new global laws because they get to build to them. They are agile. It's new. They say, okay, this is our -- this is what we -- what our standard is. It's the midsized companies that have legacy systems that have been around for a couple of decades, they have the hardest time.

MS. MITHAL: So this is interesting, and, Justin, I want to kind of raise this with you because you -- several panelists on this panel and the last panel have raised concerns about the privacy assessments in our orders. Those are risk assessments. And so if we think they're effective in the context of GDPR and not effective in the context of FTC orders, is there a disconnect there? Is that -- and, Justin, you don't have to answer that question. You can answer what you were --

MR. BROOKMAN: That answers the question. No, I think risk assessments are not -- when

substantive protections in a bill are tied to risk assessments, I think that's really bad for both consumers and for small business. So, you see -- you see a fair number of bills out there that say, you have the right to delete your data. If the company conducts a risk assessment and says you have a privacy risk or you have the right to opt out of processing or sharing, if they do a risk assessment and there's privacy risk and it's not outweighed by their compelling interest.

I think those sorts of bills that pair high levels of process are good for big companies and for law firms, but they're bad for consumers and small businesses because they don't have clear obligations, or even very strong rights. And so I'm definitely concerned by -- if that's what you mean by accountability, then I think I strongly disagree. If you mean, like the classical notion of accountability, which means you get in trouble when you break the law, then that I'm all in favor of.

MS. BRILL: No, what I'm talking about -- what undergirds the risk assessments will be unfairness and deception, unless you decide to create a different standard. And there are discussions around creating a duty of care, duty of

confidentiality, a duty of loyalty. That's one concept. Other concepts -- you know, there are other concepts out there about what you would build to undergird the risk assessments. Clearly, there has to be something that you're assessing, right. There has to be something that you're looking at. So it's not sort of free-founded.

In terms of small companies being able to comply, listen, you know, we're -- that happens to be what Microsoft does, is we provide these tools to small companies, we provide them to medium-sized companies, and we provide them to very, very large companies. I think the idea that this is hard should not be a reason for not going forward. We still need to go forward, and we need to get small companies, medium-sized companies and large companies to understand that data is really important and that they need to protect it.

MS. MITHAL: Okay, so I think you kind of responded to my next question, but I'm going to ask the rest of the panelists, which is if you could name one thing that you think that US federal privacy law should take from GDPR or CCPA and one thing that US privacy law should avoid from GDPR or CCPA, what should they be? And I didn't tell you I was going to

ask that question, so I'll give you a minute to think about it. It doesn't have to be one thing.

MS. BRILL: Well, I've got one thing that should be avoided from CCPA, but go ahead.

MR. VLADECK: Yeah, I think the one thing that I would take from the GDPR is the notion that privacy is a right. I mean, the only right of privacy that Americans really have is the Fourth Amendment, which is the right of privacy against the government. The statutes that we have do not create -- are not, by and large, rights-creating, as we use that term.

And so one thing I would hope that if there's federal legislation, we turn -- we talk in terms of rights creation. The other thing I would mention is we also -- we need to deal with data brokers. So when you're talking about privacy legislation, that has to be on the table.

MS. MITHAL: David?

MR. HOFFMAN: Yeah, just to follow up on that because it's right in line with David's last comment. The first thing I think we need to take from GDPR is it's got it apply to all personal data. There can't be a carve-out for publicly available data or government records because that's the data that the brokers often are using. And I think we need to avoid

this over-reliance on consent and control that you see in CCPA. Individuals just don't really have that. That's a false promise.

MS. MITHAL: Lydia?

MS. PARNES: Yeah, so what I would definitely avoid is the failure to really be clear about what is personal information, what information is covered. I think that -- you know, I think the GDPR tries to do that, but there are real questions about, you know, what is it to pseudonymize data, and I think that the CCPA is incomprehensible on that issue.

And I think, you know, what I would take from both of them is, you know, I think as David was mentioning, kind of the notion of consumer rights, you know, the right to access your information, the right to delete it, you know, right to see what is being held about you.

MS. MITHAL: Okay, Berin.

MR. SZOKA: I would definitely avoid the GDPR's failure to give any incentive to de-identify data, you know, the way in which the law treats all data, essentially equally. That's insane. You asked us earlier, what should be the FTC's goals here, and I would add that one of them should be promoting pro-

privacy innovation, and a big part of that means making sure people have an incentive to treat data appropriately.

The bureau of technology, that I hope will be created here, could be a leader in actually actively helping that someday. So I would avoid that.

One thing I would take, I think that the CCPA is exactly right in preempting municipalities, and for exactly the same reason that we should preempt states. And preempting doesn't mean taking away the ability to enforce laws. Go back and look at the Obama 2015 proposal. I think that was a very reasonable proposal for having a single federal framework in which, yeah, state AGs would have a role in enforcement, and there would be coordination, but you wouldn't have a situation where the states made their own laws. You would look to the federal law.

MS. MITHAL: Justin?

MR. BROOKMAN: So I think I'd agree with the last panel that I think data minimization or focused data collection kind of tied to the context of the interaction is the most important element of it. You know, you buy something online; they have to take your credit card information; they have to collect some information; they shouldn't have to get a separate

consent, yes, I agree to this.

There should be some reasonable, carved-out, first-party, secondary uses, and I think like the original iteration of the FTC Privacy Report with commonly accepted practices would probably be a pretty good place to start with that, but then the idea about your information is going to be sold to data brokers, I think by default we should expect that that actually wouldn't happen.

The idea I would not want to transport from GDPR is the idea of legitimate interest, which I think can end up trumping any privacy rights or obligations that -- if it's interesting to you -- which is obviously an overstatement of what it does but it’s not too much of an overstatement. So I do not want to see that concept incorporated into US privacy law.

MR. TRILLING: Okay, so we are reaching the end of our time. We want to give everybody 30 seconds or so to wrap up, and I will leave it to David Vladeck and Berin to decide whether they want to use that time to revisit where I had interrupted them previously.

MR. VLADECK: No, let me just end -- let me just sort of -- I guess I have two comments. One is I think the FTC has done a terrific job given the resources it has, but the root problem I think remains

the lack of, you know, significant enough resources to do a comprehensive job. When I was a bureau director, I thought I was really simply a triage nurse, trying to figure out which fire was the most important one to put out. And I suspect others have had the same feeling.

So, you know, until the FTC gets the resources that are actually adequate to its job, there's going to be -- there are going to be concerns. And so I think to me, the most pressing issue is resources. It's one that's been pressing since 1983, but it needs to get solved.

MR. SZOKA: I agree with everything David just said.

MR. VLADECK: So we can end.

(Laughter.)

MR. SZOKA: For me, the big issue here is providing notice proportionate to penalties. We're always going to face the same problem that the FTC has always faced under unfairness, which is that there are too many practices to anticipate with specific prescriptive rules. We're always going to be relying on a vague standard. Maybe it's not going to be unfairness and deception. Maybe it’s going to be risk and context or duty of care or fiduciary duty or

whatever you might call it.

But in those scenarios, you've got to have a scenario and understanding that you can't penalize companies for not anticipating where a line is drawn as a general matter, right? You can deal with process concerns, but the first relief is going to be injunctive, and you can hold people responsible once a violation is clearly established.

MS. PARNES: Okay. So I totally support more resources. The FTC should definitely seek them and Congress should absolutely give the agency more resources for privacy in particular. You know, I think that the -- that the agency needs to have a voice as federal legislation is being considered. You know, I know that the FTC often kind of listens and reacts on -- when federal legislation is being considered. But I would hope that out of these hearings, certainly comes some recommendations, and even before a report is written that, you know, folks here sit down and talk to people on the Hill and have an opinion about what legislation -- what form it should take.

MR. HOFFMAN: Yeah, I echo that. The FTC should be calling for comprehensive federal privacy legislation that gives them more resources, gives

individuals more rights, and more authority for robust, harmonized, and predictable enforcement. Intel wrote a draft that we posted to a website at usprivacybill.intel.com to try to keep that conversation going around a bill that could look like that.

We need to get down to the specifics of talking about language that can link together. These issues are hard when you get to the point of actually trying to put language in place. Let's get to that point and start talking about what the bill should look like.

MR. BROOKMAN: Yeah. So, I agree with the other panelists. The FTC, I think, has done a strong job with their limitations that they have. I think there's more they could incrementally do, but I think fundamentally they need new law and new resources. And I think they should be more explicit about that.

I think the FTC -- and we debated this when I was at the FTC that we should be -- we should say, you know, we can't do this without more. I understand the desire to kind of convey, hey, we're good, we got this, we're doing a strong enough job, but you can't. And I think it needs to be explicit to the world that in order to do the job that needs to be done, you need

more.

MS. BRILL: And I would just -- I definitely agree, the FTC needs more resources, both in terms of actual dollars and people, but also in terms of better laws, better laws that are more fit to purpose. And I really think the US needs to take a step back and recognize that we're really not fit to purpose right now in terms of the modern data ecosystem.

We need to recognize that consumers have lost trust, and we need to rebuild that trust. And I'm talking about consumers in the United States and consumers around the world who are really asking a lot of questions. We need to answer those questions, and part of that answer is going to be the FTC is the right agency but it needs many more resources.

And we need to start thinking about what the world is going to look like, not just in a few months, but in 5 years and 10 years. And we need to lengthen our horizon in terms of building that trust.

MS. MITHAL: Okay. Thank you to all the panelists. We're at the end of our time, so please join me in giving the panelists a big round of applause.

(Applause.)

MS. MITHAL: And if you guys could just stay

up here for two more minutes, if you could stay here for two minutes, I'm just going to wrap up the day just with a couple of observations.

CLOSING REMARKS

MS. MITHAL: So, first, there's a lot we didn't get to today, and so I would encourage everybody to take advantage of the comment period. The public comment period will remain open until May 31. We would encourage submissions on anything that you've heard over the last two days, and in particular any empirical research or data that you can provide to us would be really helpful.

So I just want to kind of wrap up with just a couple of observations. One of the things I started thinking about as we kind of went through these last two days is kind of what is new. You know, we've done this rodeo before, and we've done this -- we've done privacy hearings many years ago. I see many people who worked on them in the audience.

But -- so what has been new really over the last 10 years? And I think there's really a lot of new things that have taken place over the last 10 years. We have new laws. We've talked a lot about GDPR and CCPA and other new state proposals. We haven't even had a chance to talk about laws like PIPEDA and other laws that are non-Europe, non-US, but there's a lot of new laws out there.

There's new technologies. We talked about IOT. We talk about kind of home assistance, generating lots of data, big data, artificial intelligence, machine learning, connected cars, that whole gamut of issues, the idea that there's a lot of passive collection from sensors, that there's a lot of inferred data about people. So these are kind of some of the new technologies and business models that are out there.

And we've heard some new concerns. You know, we hadn't heard the phrase "dark patterns" even a couple of years ago. We hadn't heard the phrase "algorithmic discrimination" 10 years ago, and that's something that I know a lot of people are focused on now.

So with all of these new concerns and new technologies, was there any consensus over the last two days? And so let me just kind of float three areas of consensus that I heard over the last two days. The first is the consensus on the goals, so consensus on the goals of privacy protection. We've talked about protection from harm, beyond financial harm. We've talked about transparency and choice. We've talked -- but not as the sole goal. We've talked about the transparency and choice as a goal.

We've talked about the need to promote competition and innovation in this space. So there's a lot of consensus around the goals.

There also seemed to be secondary consensus, which is consensus towards the fact that there should be federal legislation. And we've seen a lot of proposals for federal legislation, and we've heard a lot about them over the last couple of days from entities as diverse as the Chamber of Commerce, CDT, Apple, Intel, World Privacy Forum, the coalition of companies and trade associations that Stu Ingis talked about.

And then the final area of consensus is that it does seem that there's consensus that the FTC needs new tools and resources. I even heard the representative from the Chamber of Commerce earlier say that Section 5 is not enough. So I think those are the kind of very high-level points of consensus. I think the hard work is yet to be done to drill down on what some of these proposals should look like.

But let me just close by thanking all of you who stuck it out until the end, all the audience members, the 50-plus panelists, all the public commenters. I'd like to thank some particular offices that helped us here: Office of Policy Planning,

Bureau of Consumer Protection, Office of the Executive Director, and Office of Public Affairs.

And mostly I would like to thank the three team members who were completely responsible for all of the heavy lifting on this event, and that's Jim Trilling, Jared Ho, and Elisa Jillson. So if you could give all these folks a round of applause.

(Applause.)

MS. MITHAL: And, again, thank you very much for coming, and we look forward to seeing your comments. Thank you to the panelists.

(At 5:06 p.m., the hearing was adjourned.)

CERTIFICATE OF REPORTER

I, Linda Metcalf, do hereby certify that the foregoing proceedings were digitally recorded by me and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, not financially or otherwise interested in the outcome in the action.

s/Linda Metcalf
LINDA METCALF, CER
Court Reporter