FTC Hearing #1: Competition and Consumer Protection in the 21st Century
September 13, 2018
Segment 3
Transcript

BILAL SAYYAD: All right, I think let's get started. It's the last panel for the day. And as I mentioned at the beginning for those who haven't read the website or were not here at the beginning, because of at least the potential for weather difficulties tomorrow, we're going to reschedule tomorrow's sessions till probably sometime late in October.

So this, we turn now, from mostly anti-trust, but not exclusively, to a consumer protection issue. And James Cooper now with the FTC will moderate this panel.

JAMES COOPER: All right, thanks, Bilal. Welcome, everyone. Good afternoon.

I'm James Cooper. I'm the deputy director for economic analysis in the Bureau of Consumer Protection here at the FTC. And it's my great pleasure to be here and take part in these hearings and moderate this august panel. Before I get started, I have to-- recently I'm on leave from academia, so I'm not used to doing this, but I'm going to try to say zero of substance today. And on the off chance I'd do, anything I say is just my opinion only and not necessarily that of the Federal Trade Commission or any individual commissioner including the one sitting next to me--

MAUREEN OHLHAUSEN: Most especially not.

JAMES COOPER: Most especially the one sitting next to me.

MAUREEN OHLHAUSEN: James and I have worked together many years.

JAMES COOPER: All right, so as you probably already heard today, nearly 25 years ago Chairman Pitofsky, when he began the FTC's journey on the path to become the nation's privacy and data security cop, along the way much has changed. When this all began, things like the iPhone, Facebook, and Google didn't even exist. But today, we find ourselves in a digital economy that lives on consumer data.

Clearly, this evolution has provided tremendous value for consumers. We know vast troves of information at our fingertip. Most of us can't get anywhere with our phones anymore, myself included. And we can connect with millions of people instantaneously, as I'm sure many of you are doing right now via Twitter. I could go on.

But at the same time, the fact that consumer data is so tightly woven into the fabric of today's economy, it's presented a unique consumer protection challenges. Part of what I think makes these issues so tricky may stem from the fact that there's no agreed upon framework for analysis. As we've heard a lot today, antitrust is married up with microeconomics. It has been for about the past four decades. Privacy and data security, however, have yet to find such similarly suited mates.

So the FTC-- or clearly economics is an important role in shaping privacy and data security policy. For example, the seminal work of the economics of information that garnered Nobel prizes for people with names like Akerlof, Spence, and Stieglitz, teaches us generally that reducing the cost of information flows typically improves market performance, because it helps consumers make better choices. But at the same time, privacy and data security policy also involves significant consumer values, such as dignity, the right to be let alone, an autonomy, which are really difficult to balance in a typical benefit cost framework, though, they're equally important.

Never one to shy from a challenge, the FTC has been in the forefront of trying to tackle these complex and weighty matters. So I mentioned before, beginning in 1995 when Chairman Pitofsky convened a series of workshops designed to educate the FTC and the public on consumer protection issues surrounding the online use of consumer data and continuing with the 2012 policy report and subsequent reports and workshops examining issues like big data, the Internet of Things, data brokers, and most recently informational injuries, through what former Chairman Bill Kovacic called policy research and development, the FTC has continually attempted to calibrate its enforcement posture to balance consumer interests and privacy and data security with the remarkable benefits that the digital economy provides. And I think that these hearings will continue that tradition.

So this brings me to the subject of our panel today. Today, we appear to be at an inflection point. Many of the same undercurrents that are animating the challenges to the anti-trust status quo that were addressed earlier today and that will be addressed in other hearings, coupled with catalysts of high profile data breaches, the use of social media to attempt to influence the 2016 election, Cambridge Analytica, and the coming online of GDPR have caused many to question whether the current privacy and data security framework needs a rethink.

For example, some have suggested the US should adopt a more European-like approach. And it appears that California has already taken up the mantle. And we see legislative proposals in various forums kicking around Congress. So today, we hope to work through some of these thorny issues, examining where we are, where we might go, and what that might mean for both consumer privacy and the digital economy, which has provided us with so much.

So we're very happy, we should all be happy to have an all-star panel to help us on this journey today. To my immediate left is Maureen Ohlhausen. Maureen's currently commissioner of the Federal Trade Commission. She was acting chairman from January 2017 through April 2018. Before that, Commissioner Ohlhausen was partner at Wilkinson, Barker, Knauer, where she focused on FTC issues, including privacy and data protection. She also served at the FTC for 11 years prior to that, where she was the director of the Office Policy Planning. And prior to that, she was a clerk for Judge Sentelle on the DC circuit.

So next to Commissioner Ohlhausen is Howard Beales. Howard is A professor of strategic management and public policy at the George Washington University. Importantly for the purposes of our panel today, Howard, from 2001 to 2004, served as the director of the Bureau of Consumer Protection. In addition, in his earlier stints at the FTC, he helped think about and

really develop a lot of the framework today for how we analyze informational issues surrounding consumer protection.

Next to Howard is Daniel Solove. He's the John Marshall Harlan Research Professor of Law at the George Washington University. Daniel is one of the leading privacy scholars in the country. In addition to writing some of the seminal articles in privacy, he along with his co-author Paul Schwartz are the author of a casebook on information privacy law that everyone, including me, uses to teach that subject. He's also the CEO of Teach Privacy and runs a myriad of privacy programs, which unfortunately for us may mean he has to cut out early-- I don't think he will-- because he's got something going on tonight, including his annual privacy forum, privacy salon, things like that.

And then finally last, but definitely not least, David Vladeck is the AB Chettle Jr. Professor of Law at Georgetown University Law Center. And he, like Haller, was the Director of the Bureau of Consumer Protection from 2009 to 2013. And before that, he spent 25 years with the Public Citizen litigation group.

So we're kind of lucky here, I mentioned, you know, to have both Howard and David because in their time frame with Lydia Parnez in kind of in between as well, really helped usher in the era of the FTC being involved in privacy and data security and really kind of being at the helm of that in large part.

So what I want to do with this format today is we're just going to have a discussion. We don't have any presentations. But we want to drill down on some questions. And we also will have, if you have questions from the audience, we will be taking note cards. I guess there are designated people to take those questions. And we'll certainly save some time at the end to address these.

So let me let me get started. And the big picture, headline question of this panel is kind of take stock of where you are in the privacy and data security regulation in the US and where we need to go. And I think if we're going to assess that, maybe at sort of a higher level, we should think about what would be the goals of a privacy and data security program.

So at a high level, what should privacy and data security program be concerned with? What sort of values should it be protecting? And how might we think about measuring whether that goal's accomplished? So Maureen, I want to have you take a first crack at the question and invite others to respond or react.

MAUREEN OHLHAUSEN: Great. Well, thank you, James. And I'm delighted to be here. Thank you to the organizers for including me in the panel.

This is a topic I've thought a lot about. What are the values that we are trying to protect and pursue in our privacy and data security enforcement in the US? I would say one of the first values-- because our authority under the FTC Act that is deceptive or unfair acts or practices in or affecting commerce.

So first of all, it's commercial. Everyone forgets that one at the end. But it's in commerce. And then deceptive, that means that there was a promise made to a consumer that isn't kept. Or unfair, which means there was an act or a practice that caused substantial injury to a consumer that the consumer couldn't reasonably avoid that is not outweighed by countervailing benefits to competition or to consumer protection.

Now, of course, the FTC isn't the only actor in this space. We already have lots of other or certain number of other privacy laws. You think about HIPAA. You think about financial privacy. You think about this the CPNI rules for communications data. So those are areas, where, in a way, if you think about it, we've already as a society through our political system decided there are special buckets of information that need special protection. So where does the FTC fit in there?

First of all, to talk about deception, I was actually at the FTC back when we brought the first online privacy case. Dan Caprio was there with me, as well as some other people in the audience probably too, under Chairman Pitofsky in the Geocities case. So they had made a promise about how they would collect or use data, and they didn't keep that promise.

And we brought lots of privacy cases alleging deception since. And what we're trying to protect there, I think is twofold. One, it's consumer sovereignty. The consumer made a choice. And that choice wasn't respected. So I think that's the primary thing.

There is also a competition element there, because you certainly want to allow the marketplace to operate in an efficient way where you have someone not getting a competitive advantage because they've lied about what they're doing and they actually aren't adhering to it. Maybe it's costly. I mean, that was like an Uber case that we brought. It was they had initially promised that they were going to do certain things the data. And then it turned to stop accessing it. Then it turned out to be kind of expensive to keep that promise. So we had to modify our order.

So I would say the first thing is consumer sovereignty. But then the second thing I think that we are supposed to be protecting is protecting consumers from substantial injury. And that is captured in our unfairness authority.

Now, what is substantial injury is really the question. And you don't always need a promise made to consumers. In fact, unfairness I think works particularly well when there hasn't been a promise made to the consumer. But there is sort of an expectation that consumers won't be injured through data collection and use.

So some of the cases that we've brought in that space involve things like collecting and sharing real time location data about consumers, because that can be abused in a way that can be used for stalking. So there's health or safety risk. Certainly, the collection of financial information or the failure to protect financial information, that's sensitive. So it could be used to hurt consumers financially.

We mentioned the informational injury workshop. And so one of the things that I tried to do with that is actually come up with a little bit of a taxonomy of the different harms that we have

addressed through FTC enforcement. And what I came up with in doing a review of all the cases that we've brought in the privacy area, the first one already mentioned, which is the distortion or not respecting consumer sovereignty through deception, financial harms, health and safety-- you mentioned that one already-- and unwarranted intrusion.

So cases we've had some where-- or had to TRENDNet case where there was an internet enabled camera that had a pretty obvious flaw in its software, so that anybody who had the IP address could hack into this camera that was sold to be used for home monitoring, watching your kids. So we think well that is intrusion.

We also had the rent to own-- I think it was Aaron's case. David and I agreed very vigorously on that one.

DAVID VLADECK: It was the DesignerWear case.

MAUREEN OHLHAUSEN: DesignerWear, that was it.

DAVID VLADECK: It was the predecessor.

MAUREEN OHLHAUSEN: Very good. But where the laptops had a program that could turn on the camera and companies could use that or take screen shots.

And then the last one is reputational injury. And my view is that FTC, we've never brought a case purely based on reputational injury. But reputational injury has been certainly present in some of the cases that we've brought, such as the Ashley Madison case. So I would say reputational is a little, I think, more controversial. But otherwise I think those are the types of things that the FTC's approach, the authority that we've been given, those are the values that we should be pursuing in privacy enforcement.

JAMES COOPER: Yes. Would anyone else like to weigh in that? Sort of at a high level, perhaps even leaving aside the FTC's goals, what should we be thinking of when we think about an enforcement program or a regulatory program to protect privacy? What sort of value should it be protecting? What should we be thinking about?

DAVID VLADECK: So let me just add to Maureen's point about the DesignerWear Aaron's kinds of cases. You know, Ashley Madison, I'm not sure is a reputation harm case only. I think part of the struggle-- and I'm glad we had the workshop on informational harms-- is they all sort of generally fit into what we used to think of as an invasion of privacy tort. But they're hard to label. So when Ashley Madison-- you know, marriages were broken up.

MAUREEN OHLHAUSEN: People committed suicide.

DAVID VLADECK: People committed suicide. So labeling that kind of harm is difficult. But I think partly what we want to focus on is the nature of the intrusion. So in Ashley Madison, it's intruding into very personal relationships. In DesignerWear and Aaron's, it was intruding into the

home. I mean, the real problem in those cases was that cameras can be activated remotely while people were sitting on the couch or doing whatever.

And so I agree that it's important to try to see if we can come up with a taxonomy. But a lot of this really just sort of depends on context.

JAMES COOPER: And since David said taxonomy, I don't know if Daniel if you'd like to jump in. Daniel wrote one the taxonomy and privacy, which is kind a seminal--

DAVID VLADECK: It was not inadvertent.

DANIEL SOLOVE: Well, I would say there's obviously protection of consumers from harm, which I think is important. And a lot then depends on how we define harm. I tend to define harm broadly to also include risk, which I think is a very important concept. There's also the broken promises, that it's very important that if a company makes a promise that it be held to that promise. Otherwise the entire self-regulatory regime collapses, because the privacy policies are meaningless then. So it's nice that the FTC has a backstop to that and enforces.

I think there's also an important component to an enforcement regime that I think the FTC can and sometimes has gotten involved in which is consumer expectations. Even if it's not a direct promise, consumers have expectations about how their data is going to be handled and used that are often and sometimes at variance with what's said in a privacy policy or with what companies do.

There's been studies about consumer attitudes about privacy. And vast majority of people agreed with the statement that if a company has a privacy policy it does not share data with third parties. So there's definitely a lot of misinformation out there. Consumers have incorrect expectations. And the FTC can play a very important role in helping to make sure that faulty consumer expectations aren't exploited. So companies knowing that consumers kind of already have this maybe unjustified trust in them, don't exploit that trust, that what companies do that they start becoming at great variance with consumer expectations, that those outliers be stopped.

The Sears case I think is a wonderful example of that, where they installed spyware into people's computers. And this was actually disclosed in the fine print in a very lengthy privacy policy. So it was actually there. But it wasn't very salient. It wasn't very noticeable. So most people missed it. And the FTC said that it was not sufficiently disclosed and not conspicuous enough.

And I think that's great because what we had is a practice that was very unexpected to consumers that caught a lot of guard. And so I think it's very important that consumers can use sites and engage in e-commerce and other commerce and know that what they expect generally is going to be the case, and there aren't going to be unpleasant surprises down the road. And so I think it's very important that the FTC police that, especially because we know from a lot of studies that a very, very small percentage of people actually read the privacy policies or privacy notices. Something like less than 1%.

So we really are in a world that consumers come in with this baggage, these expectations. And I think we have to play in that world and know that that's how people are going to make decisions on how to share their data. And there should be some protection from that being exploited.

JAMES COOPER: Howard, do you want to jump in? One thing just to-- and maybe it will be completely orthogonal to what you're going to say, but maybe it will be related. It sounds, you know listening to David and Daniel, to what extent should a privacy and regulatory framework-- should we think about privacy as sort of a rights-based framework? Or is it something that needs to be balanced with other values as well? Is it something that can be balanced, or is it just a right? And I don't know, it's something just kind of was thinking about as David and Daniel were talking. So anyway, Howard, I'll let you speak to that or whatever you want.

HOWARD BEALES: Well, I did want to comment a little on the discussion that's gone before it. But first, I wanted to take you to task for listing the Nobel Prize winners for the economics of information without lifting the guy who founded the field, which was George Stigler, and first and foremost, but he was one of my advisors too. But I'll forgive.

The attraction to me of the consequences-based approach to thinking about consumer privacy, which is what we developed in the time that I was at the Commission, was that it makes explicit what ought to be there all the time, which is that particularly in the commercial context, this is a balancing issue. There are tremendous benefits that come from the ability to use information, even if it's an unexpected use of the information.

And we don't want to sacrifice those benefits, because somebody didn't think to include that in the list of things that might be done with information in the privacy policy, because it wasn't thought of at the time, that the privacy policy was written. We didn't know this was a possible use of the data. Those kinds of benefits-- we have we have an enormous number of services that are built on exactly those kinds of secondary uses of information that was collected for a different purpose, that may or may not have fit with consumers' expectations.

What we want to make sure of is that that information is not being used in ways that are harmful to consumers, it's doing damage to consumers. And that's where privacy regulation and privacy enforcement really ought to focus. if there's not a harm, it's not something that the FTC in particular should be worried about.

Now, I also have a reasonably broad concept of harm, perhaps not as broad as some. I certainly think that the things that the kinds of subjective harms that fit within the traditional privacy torts are the kinds of harms that are actionable privacy harms. But I note that the tort standard in virtually all of the privacy torts is highly offensive to a reasonable person. At the intrusion or putting somebody in a false light is something that would be highly offensive to a reasonable person, that's an essential element of the tort. Not just any intrusion, not just any false light that might be held out. But including those kinds of harms, I think I think makes complete sense.

We've had two mentions of DesignerWear and Aaron's. And there's a part of that case that I completely agree with. And that's the turn on the camera part of the case.

There's a part of it that I've always found really troubling. And that is this is a computer that when somebody stopped paying, you could activate the software and the computer would call home and tell this company that had rented the computer to somebody who was no longer paying for it where it was. That's really useful.

The complaint says while this is location tracking and location tracking is bad. But the complaint doesn't say why location tracking is bad and especially when it's every two hours. And the remedy that is in the complaint or in the consent order is, well, if you disclose when you first turn this on and track continuously that will comply with the order. So to fix tracking every two hours, you would track continuously. I don't get what harm we thought we were fixing there. And it's that harm that really needs to be the focus.

If we can't articulate why we think this is a problem, we're not be able to adopt sensible and low cost ways to control that problem. We've got to think first about what's the harm we're trying to prevent.

JAMES COOPER: Thanks, Howard. So after hearing kind of a high level view of what sort of values we should be concerned about when we're thinking about a privacy program or a regulatory framework, maybe it's important now to take stock of actually where we are. And so I wanted to turn to Daniel, who as I mentioned before written a seminal textbook on this and lots of articles defining and thinking about what privacy is. So, Daniel, could you just kind of help us characterize the current US system of privacy and data security regulation in about five minutes maybe?

DANIEL SOLOVE: Sure. At the high level, the bird's eye view, my sophisticated way a synopsis of it is it's a mess. We have a sectoral approach with laws that have arisen in various economic sectors over a very long span of time. Then you have common law torts that have arisen, the privacy torts. Plus, there's the forgotten breach of confidentiality tort that I'd like to mention too that doesn't require highly offensive. There are all sorts of other common law torts that could apply in these contexts, such as negligence is making a resurgence in data breach cases.

And then you have various state statutes in the states. You have dozens of federal laws, not as many recently. But certainly in the '70s, '80s, '90s, you had a real series of laws that were passed to deal with various privacy issues and various economic sectors. And then you have the FTC, kind of an overarching, the broadest jurisdiction of any federal agency regulating privacy, that regulates most companies, except for some carve outs.

And that's the US approach. And there are inconsistencies in the various laws. Some of them are a lot weaker than others. On the stronger side you have HIPAA, which is very, very broad, has a broad reach. It follows the data through the chain of its custody. But you also have laws like FERPA that regulate schools, that, by and large, are kind of, for lack of a better characterization, a bit of a joke. They're not really enforceable. They lack a lot of the features that more recent privacy legislation has.

Contrast this to a number of other countries in the world, including especially the EU, they have a comprehensive privacy law, a baseline of protection. So they can articulate here are the basic rules of the road that we follow. Here in the US, it's very hard to articulate, well, how is this particular data protected? We really can't. It depends on, well, who holds it. If it's held by certain entities and it's regulated by HHS, but it could also be regulated by the FTC. And it depends on who enforces. And it depends on what the sectors are.

And the one of the challenges with the sectoral approach is that the sectors change. So in the '70s and '80s, what various types of companies are doing in the sectors make sense then. But now, as we see, different companies are jumping into different areas. And so when we build laws around sectors and they don't stay fixed. And now there's a lot of overlap and companies saying, wow, we're regulated by five different agencies and five different bodies of law, and we don't know what to do. There's so much. Plus, then all the different state laws that are overlapping. And it becomes a bit of a nightmare.

I'm not sure we can dial this back in the United States. I'm not sure we can kind of go and say, hey, we're going to do the other approach. But I think there's some sensible aspects to the other approach that are quite efficient and to some extent I think could be particularly business friendlier than the US sectoral approach, which I think a lot of industries were happy with initially, because they like the idea of a lot tailored to them or they like the fact that laws didn't apply to them and they fell through the crevices. But those crevices have been largely, a lot of them have been plugged up by the FTC, which regulates.

The other problem, too, with the US approach is that we get no respect from the rest of the world. We're kind of the Rodney Dangerfield of privacy in the US. But I think we have some very effective, some really good laws. I think the FTC has done tremendously effective work. We do have a lot of protection. It's just that it's inconsistent. It's hard to articulate. It's very hard to explain to other countries, especially the EU, how the US system works and how information is protected here. It's so haphazard.

So I think the biggest challenge is, what do we do going forward when we have so many laws that are locked into antiquated visions of the economy from 30 years ago and the leadership role has increasingly been ceded by the US Congress ever since I think around 2000, where we really haven't seen a tremendous amount of legislative activity on privacy. It really has tapered off. And we've really seen the states, especially California, and the EU take the lead.

And I think if you ask most large multinational companies what privacy law are they focusing on for their compliance efforts-- GDPR, the new California law. Hardly anyone will say anything about any other US law. Maybe a little bit of HIPAA. FTC, I barely hear whispered these days, although I think a few years ago, the FTC was spoken about a little bit more. But increasingly, what we're seeing, I think, is that companies-- and these are US companies-- not really looking to the law here as to what they're doing and how they're building their privacy programs and practices.

So that's where we are. And I think the big question is what should we do in the US for what's the next step? Do we kind of say, hey, we'll just be regulated by Europe and California? Or will

we have meaningful regulation at the federal level that reflects the balances and approaches that the US would like to have?

JAMES COOPER: Well, thank you, Daniel. I'd like to invite anyone to react to that and also kind of throw out there, it seems as we think about the landscape of the US privacy regime, it seems to be a mixture of ex ante regulation with notice and choice in some areas, HIPAA, COPPA maybe. But then we also see enforcement, private and FTC. What are the pros and cons of those approaches? And what might be-- you think about whether there should be a mixture, if we should hew to one or another. Or makes it sense to mix it up in some ways, the way that we have here in the US. So throw that out to anyone.

DAVID VLADECK: Let me comment on that briefly, because until at least a few years ago, the difference between the EU and the United States was we did a lot of enforcement, but we had this patchwork, this crazy patchwork of laws. On the other hand, in the EU they had, even before the GDPR, they had a general regulation, which was much more comprehensive than any US privacy law. But there was almost no enforcement.

And some scholars have done a lot of work looking at sort of privacy on the ground, both in the United States and in the EU. And they found that the privacy commitments in the EU were met only to the extent that there was a real enforcement or a culture of compliance, which left out large swaths of the EU.

And so I think that somewhere in the middle is the desired outcome. But strict rules without enforcement, at least according to the studies that have been done, didn't work all that well in the EU. And I think that was one of the major driving forces for enacting the GDPR and to basically base the new system on commitments of compliance and enforcement. And it will be interesting to see the extent to which the new GDPR is enforced by the data protection authorities in the EU, who are not used to doing FTC-like enforcement cases.

JAMES COOPER: Anyone else like to jump in on the ex ante versus ex post question?

MAUREEN OHLHAUSEN: I was going to say, while I agree that regulation if there's clear regulation that says, like the Children's Online Privacy Protection Act, Congress drew the lines there and the FTC implement it and enforces it. But one of the things that I think has been a real strength of the FTC's approach has been it's case by case enforcement, maybe a little less predictable in some ways, but it trades that from great flexibility. So a focus on harm in case by case enforcement reduces the need for you to predict the future to design some overarching regulation that foresees all innovations.

Howard mentioned this, and I think we all would agree, consumers have gotten enormous benefits from a lot of these technologies. Consumers have gotten a lot of free content. And they've gotten a lot of information at their fingertips, as you mentioned. So that doesn't mean like anything goes. But I think we need to be careful about coming up with a system that is too regulatory because it can't predict what the new innovation is going to be and perhaps can prevent it from happening.

HOWARD BEALES: Just to pick up a little on the ex ante versus ex post problem. I think part of the problem with the ex ante regulation is that the approaches we have now and particularly the approaches that are embodied in the GDPR and in the California statute are really based on a premise that won't work, that people are going to read privacy policies and pay attention to these notices about what's going to be done with information and make choices based on that.

And Dan says, and I think he's right, nobody reads privacy policies. It's probably a good thing, because there's a study out of Carnegie Mellon that said that if people actually did read their online privacy policies, the opportunity cost of the US economy would be $787 billion. It's just out of all proportion to what might be at stake in commercial privacy decisions.

And with the ex ante approach, that difficult, if you will, the focus on ex post on where have things gone wrong that need to be fixed and what can we do to try to keep them from happening again. It seems like a much more sensible way to approach the problems.

MAUREEN OHLHAUSEN: Howard, I just wanted to weigh in a little bit on your point about people not reading privacy policies. I agree probably the average consumer doesn't. But we have academics in the US-- I bet Daniel read privacy policies. I bet David read privacy policies-- academics and consumer groups, consumer organizations, and competitors--

JAMES COOPER: I don't read them.

MAUREEN OHLHAUSEN: So James doesn't. No, I'm just kidding.

JAMES COOPER: You said academics. I just wanted to make sure that--

MAUREEN OHLHAUSEN: Well, academics other than James Cooper. But I think there are mechanisms for if there is a problematic term in a privacy policy for it to get noticed and surfaced. And that's one of the things we've seen I think with social media, that when something is discovered that people don't like, that news gets out there.

HOWARD BEALES: Well, if that's the goal, then that points to a very different kind of a privacy policy, because you don't want something that's understandable to consumers. You want something that's understandable to geeks and competitors, who can figure out whether there's something wrong going here. That's sort of not where we're headed. It's not where the Europeans are headed. It's not where California is headed. We want simple privacy policies that anyone can understand that tell you nothing and mostly unread. I mean, no doubt some people read them.

DANIEL SOLOVE: A while ago, I wrote a piece about privacy self-management, which is this idea that people manage their own privacy by reading these policies and making choices. I think this is a flawed approach, not just because people don't read privacy policies-- and also I think the point that there's this tension, privacy policies are useful to regulators and advocates and academics and others who can read them carefully and you're going to give a lot of information, but the average consumer really can't get all that. So there's a tension. You almost need two different things, which is what Paul Schwartz and I have proposed in our ALI project, which is a transparency statement for the regulators and then something simpler for the consumers.

But as a consumer, reading the privacy policies is relative meaningless. I don't read them because it's too many, the amount of entities I do business with and sites I visit, hundreds, thousands, I don't have time.

And then the choices, do I share this piece of information on Facebook? I don't know. The implications for privacy depend on how that information is combined and aggregated with other information over time and how that information might line up and what someone might do with something and what algorithm someone might create five years from now and a whole litany of things that I can't even figure out. So I really can't make the judgment as a privacy expert on exactly what the implications and costs and benefits to me, especially the costs over time, are going to be for me to release a certain piece of data.

So it's very, very difficult. And now multiply that by 1,000. And I have to make that decision all the time. Just really, really hard to do for the consumer.

So I'm just not sure that that approach-- it's great if there's like one company that you actually do business with. I'm only on Facebook. But it's not. I'm on all the sites.

Like the professors-- I give an amount of homework every night. And I think it's reasonable for my students to read 30 pages in a night. But what if they have 10 professors and each assign 30 pages. And that's what the companies are doing. Every company thinks, hey, they can pay attention. We click this great mechanism.

Yeah, multiply it. It doesn't scale. That's the problem.

And the consumer, if you say, hey, we protect your data with reasonable data security. What's that? As a consumer, I how do assess your security? How do I know how prepared your employees are to not be phished? How do I know what kind of encryption you're going to use and all these other things?

I can't really make an informed assessment, which is why we need an agency like the FTC to be looking out for people, just like when I would travel abroad and the taxi fares, they didn't have a meter. And I didn't know what the right fare was. And they would just say like it's x whatever. And I had to trust them or make some-- I didn't know.

It's nice to know that someone's looking out for me. And there's a meter. And someone's thought of what the right fare is going to be. And I don't have to worry about someone cheating me. Or I can pick up a jug of milk and know that I can drink it and I'm not going to be poisoned. I don't have to do research. Imagine if you didn't have the food safety and you actually had to go online and research the safety conditions at each farm to figure out do you buy food from there. I'd just like to know like I pick up a product at the supermarket and I think we want the same thing for privacy.

DAVID VLADECK: It's amazing how when you use the phrase privacy policy, everybody launches into a diatribe. So I'm going to take a minute and launch into my own. One is they're privacy policies. The original sin was calling them something that they're not. None of them

really deal with privacy. They deal with data use. And part of the problem is they've been misnamed.

The other problem, of course-- and this gets back to the question that James started with-- the difference between ex ante regulation and something else. If you have a regulatory regime that is clear so you know that everything you do on the internet is safe or at least you have that promise, even if it's not enforceable, then the privacy policy or the data use statement becomes less important.

And part of the problem that we have-- and the FTC has done a lot of work on simplified notice, and Dan and the ALI have done a lot of work on trying to figure out a better system for this. But these are really notice systems. And they need to be simplified. Many of them are written by lawyers. So they're bound to be incomprehensible. And they're often designed to be incomprehensible.

So this is an issue that plagues us. And I just don't think we've collectively figured out a way to escape it.

HOWARD BEALES: I think actually Mick Jagger had the answer to what's going to happen here in 1964. The technology was a little different, but he said, a man comes on the radio-- like I said the technology is a little different-- telling me more and more about some useless information, supposed to fire my imagination. What happens? I can't get no satisfaction.

DAVID VLADECK: There we go.

JAMES COOPER: All right, so David, with that segue-- thank you, Howard-- we've kind of set the stage for where we are in the US. What do you see is any of the problems-- you know, because again the headline of this panel is supposed to think about rethinking the current privacy and data security regime, what are some of the problems, if any, of the current status quo? Are there any harms that you don't think are being addressed? Are there inefficient enforcement? Either over deterrents, under deterrents? So what do you think, David?

DAVID VLADECK: So let me just use a few examples, because time does not permit me to go through all the concerns that I have. But one is I don't think we have effective tools to really understand what's going on with big data, let alone to regulate it sensibly. So we all know that data collection is now ubiquitous. We bring it into our own homes through always on devices, or sensors, and the Internet of Things. We know that this data is being collected.

But our laws really don't have any restraint on the sale or renting of this data. We know it moves. We know it has a substantial economic value. But we don't have any real information on the velocity of volume of this kind of data aggregation. So that presents risks.

Paul, one of my colleagues, both at the FTC and here, wrote an article 10 years ago in which he sort of cast in dystopian light what he called the database of ruin. Well, we don't know yet whether there are these kinds of enormous databases. But there's nothing in US law that really restrains that development.

And these kinds of databases pose risk to consumers. There's the risk of data breach. After all, these would be honeypots. They'd be a magnet for identity thieves. And we know identity theft is still rampant.

So one question that the FTC, I think is going to have to grapple with is, where is this data? What's it being used for? How is it being transmitted? To whom? And for what purpose? So that's one issue that I think the Commission is going to have to grapple with going forward.

Second, the rapid initiation of algorithm decision making in the marketplace. Now, I said this morning, I'm no fan of human decision making. We generally don't do such a great job. And machines may help.

But for regulators, these kinds of decisions are very difficult to oversee. They're not transparent. Machine learning algorithms are impossible to interrogate. You can't put them under oath. It's hard to root out disparate treatment based on factors that are impermissible-- age, gender, race, things like that. Nor is there necessarily due process at the end of the decision making chain.

And so I know the agency has already done a fair amount of work on this. But this is an issue that I think demands greater attention, because I do think it poses enormous risks to those who come out on the bottom in terms of these kinds of decision making.

In terms of enforcement, my concerns are not really with over enforcement, because the agency resources are too scarce for that. Indeed, when I was there the Director of the Bureau of Consumer Protection-- and I don't know whether Howard had the same concern-- but I spent a lot of my time doing triage, deciding which cases to bring and which cases not to bring, even though many of those cases in the latter category were meritorious, and we should have brought them if we could have. So I don't think that's the problem.

I do think there are enforcement challenges. So one is, how do you enforce against an industry like the mobile app industry, which is highly diffuse, diverse industry, thousands and thousands of that developers? Many of whom either don't really know what the law requires or just don't really care.

So The New York Times did a story yesterday about COPPA violations, violations of the Child Online Privacy Protection Act by app developers that were tracking kids 12 and under without explicit parental permission. Sure, the FTC could bring 20 or 30 enforcement actions against this kind of industry. But it's not at all clear to me that you get any kind of deterrent value that you really need.

So one question is with respect to these kind of diffuse industries, how do you make them comply with the law? That's one problem. Another is we have to figure out to what extent machine learning decision making tools are staying within the statutory guidelines. That is an enforcement problem.

And last, we have a lot of companies under order. And order violations are hard for the agency to detect and to deal with, simply because the high volume of companies under order. That's a

serious enforcement matter. I mean, for a company to violate an FTC order undermines the ability of the agency to do its work. It undermines the deterrent value of consent decrees or enforcement cases. And I think that sort of the new management at the FTC is going to have to grapple with that. There are many others, but I'll stop there.

JAMES COOPER: Would anyone else look to the weigh in?

MAUREEN OHLHAUSEN: One thing, building on what David said, I agree that one of the challenges for the approach that we have-- and when I talked about privacy policies it's not certainly to say privacy policies are it and take care of everything. It's just that I don't think they're as totally useless as some other people seem to think they are.

But the other problem is these kinds of harms that we may have a lot of little bits of data that weren't sensitive, that weren't even personally identifiable when they were collected. But through these new tools that can be assembled into a more complete mosaic and identify to a certain person. And then I think the question there is, is there harm? Is there a risk here? And that is where I think we need to start thinking, how do we address that?

Because a lot of those uses may be great. They may be very beneficial. We don't want to stop those.

But for the harmful ones-- and if we look at something like that going back to the pre-internet days and the Fair Credit Reporting Act, it was trying to get at those kinds of issues, to allow some kind of balancing and use of this data, but to allow consumers to know if it was being used in a way that disadvantaged them in connection with an important decision, like employment or insurance or some other ones, lending, and then gave them insight into what it was and the right of correction.

So I think that is where we need to start thinking about kind of a risk-based approach, because I don't think we can necessarily foresee all the uses. I'm a little concerned about the data use specification requirement, because as Howard said, there may be great uses down the road that consumers would like. But they still need to be protected from some of these new abilities to use these little bits of data in a new way.

HOWARD BEALES: I don't know why the more complete mosaic is itself a problem. I mean the one part of that clearly is a problem is if the government can get that. But there's another tool to control that problem. And it's the one we ought to use and not worry about the possibility that this might be put together.

I want to say two things about-- you know, I think big data is a really interesting question. And there are certainly potential costs there. But there's also been big benefits. I mean, that's where our fraud control tools come from is data aggregations, often data that was collected for a different purpose that's put together in an algorithm that predicts the likelihood that a particular person is really who they say they are. And if it weren't for those tools, there'd be a whole lot more identity theft than there is, which is way too much.

But that's a big data effect. You can't do that with little pieces of data one at the time. You got to aggregate the data in order to get a more comprehensive picture.

The other thing I wanted to say is about algorithms, which raise some potentially interesting questions. But I think the algorithms that ought to be of concern are the ones where the user of the algorithm doesn't face the costs of mistakes, because an algorithm is just basically a way to classify. You're a good risk. You're a bad risk. You're a good prospect. You're a bad prospect.

There was a really interesting example of Reuters, which wants to get scoops on international news. And it does that in part by following tweets. But there's a lot of bogus tweets. And so they built an algorithm to figure out whether this was likely a real story that they should follow up on or a bunch of fake tweets that they should ignore.

They face the costs of both mistakes. They're going to miss this story if they misclassify these tweets as false tweets and ignore it. They're going to waste resources if they misclassify these tweets as true and pursue it and their false.

So they know what the trade-off is. They know what the costs are of both kinds of mistakes. There's no reason to think they make the wrong trade-off.

And I think that's true of a lot of marketing applications, where if I screen out, quote unquote, "bad" prospects, I'm turning away business. I don't want to do that by mistake. I want to turn to it away if it's bad business. But I don't want to turn it away if it really is good business. So there's some fairly strong incentives within the system to make sure the algorithm works well. Where you don't have those incentives is where somebody using the algorithm only pays part of the costs and the rest of the costs are shifted to somebody else.

DANIEL SOLOVE: With the algorithms I think there there's a lot of concerns, because suppose especially a predictive algorithm, suppose the hotel chains get together or create an algorithm for determining when a particular hotel guest is going to damage the hotel room or treat the hotel room badly or do misconduct in a hotel room. And they basically come up with the algorithm, and it comes up and says that you're one of those people and starts--

DAVID VLADECK: Quotes Mick Jagger

DANIEL SOLOVE: Along with Mick Jagger too. And you start to not be able to rent hotel rooms or suddenly you're charged more. And what are your rights there? Because when you're targeted in a predictive sense, it's like, hey, I never did any damage? Well, we're not saying you did, the algorithm is just saying that we think there's a high probability that you might.

So there's something wrong with the algorithm. It's just taking into account factors. And, hey, it might actually be true. But you haven't done it. Should people have rights to say just because it says I'm likely to, how do I disprove that?

DAVID VLADECK: How do even know it?

DANIEL SOLOVE: Exactly. How do you know it? How do you disprove it? How do you argue with a prediction?

So if the FBI says our government says you're going to commit terrorism, we won't let you on the plane. You say, well, how do I prove it? It's like, well, live your life and die. And then if you die and you haven't committed terrorism, then we'll take you off the list, because we know you didn't do it. The algorithm was wrong.

But there has to be something to say like who regulates-- what are the concerns with the incorrect thing? How much transparency do we have? How can it be used? What about people's rights to challenge it and say, hey, the prediction is wrong and either inaccurate?

I mean, to just kind of leave it to the industry to do whatever they want without looking to the harms that consumers might suffer from this, I think, is something that we definitely don't want to do. That's why I think it's very important that we look into this and have good regulation on it.

DAVID VLADECK: Let me push back a little on Howard's point. It may be that Reuters bears the risks on both sides of this. But in consumer finance or credit worthiness or anything else, the consumer who is misclassified by the algorithm bears the risk, may not be enough, and there are no shortage of stories that have been publicly discussed where people have been disadvantaged based on correlations not on their actual-- So American Express had a serious problem, because it was reducing the credit limits for black customers who went to certain kinds of box stores that were deemed to be indicative of a credit risk.

And when that became public, their answer was we screwed up, but we relied essentially on an algorithm. And so again, I'm not trying to suggest that machine learning can't help us make better decisions. But there needs to be both some transparency and some due process here, particularly where it's not the company that bears both sides of the risks.

HOWARD BEALES: Well, I mean, I think in the financial transaction, it often is a company that bears both sides of the risk, because they're turning away business that would be profitable business. And there is an incentive to not do that. I mean, we can argue whether it's the perfect incentive or not.

I think the other thing we have to recognize is human decision makers have all those same biases. They're every bit as hard to tease out. They are probably less transparent than algorithms.

And I know when I was at the FTC in the 1980s, the early 1980s, and we were bringing a lot of equal credit opportunity cases, every time we looked at a judgment creditor-- a guy who sits down and looks at the applicant across the table and say, you look honest, I'll loan you money-- there was discrimination. It varied whether it was women or a race or what kind of discrimination, but there was discrimination.

Credit scoring guys didn't have that problem. Credit scoring reduced the discrimination problems that were inherent in judgemental creditors. And that's the potential gain from algorithmic

decisions. More data is usually better because it can challenge your preconceptions about what's going on and what's the right answer here.

DANIEL SOLOVE: Sometimes. I mean I think that that's true sometimes. But sometimes algorithms are no better than the humans that designed them. And there are hidden biases that can crop up in algorithms, not just the people who design them, in fact the data being input into them. If you input data that is infected with human biases into algorithms, the algorithm spits out data that also is infected as well. So there's a lot of concerns all around.

Absolutely, algorithms can improve human judgment. Absolutely, human judgment can be problematic. But I do think that the cost of, let's say for a business just saying, hey, I don't want this business, I'm going to turn a consumer away is not enough. It's not the same level of harm to the consumer. Because a business can say on the aggregate, we just think certain types of consumers are just not very profitable for us, so who cares if we lose a little bit of business, we ultimately gain. For those consumers who can't have access to credit, who can't get a loan, it's a much, much bigger deal and a much, much bigger cost.

So I actually don't think the market would always work itself out because I think that businesses might be make a good economic decision. Hey, if we do this, yet we lose a little business, but we also lose some risk. But that doesn't always look the same way on the consumer side.

JAMES COOPER: Maureen, you wanted to comment.

MAUREEN OHLHAUSEN: Yeah, I wanted to weigh in on this. I do think that there is the mechanism of the market where if one company has a poorly designed algorithm and it is leaving good business on the table, someone else has an incentive to try to capture that. And that's one of the things I think we are seeing in the lending area. They are finer distinctions being made with better targeting tools that allow lending to occur at better rates than really going by the rough calculation of a credit score that you know you kind off fall on this side of the line or that credit line. So I went at certainly take into account the fact that there are competitive pressures to having a better algorithm to expand your business.

JAMES COOPER: Just to kind of follow-- it seems a lot of this discussion is about the classifications obviously that come out of algorithms. Is Section 5 the right way to address that? I mean, we think about Section 5, would it be-- at least three out of four of you on the table have been in the position of an enforcer-- leaving aside whatever statutory or regulatory authority Congress has given the FTC to enforce discriminatory, is section 5, should it address an algorithm unfairly classify someone as getting sub-prime loans, for instance? Is that stretching Section 5 beyond where you think it should go? Or is that the right place for Section 5 to be? Or instead should it be Congress making cuts of what is unfair discrimination?

HOWARD BEALES: It's beyond where I think Section 5 should go. Obviously, the FTC has a role in places where Congress has given it a role like equal credit opportunity, where it enforces. And it's reasonable and appropriate for it to do that. That's what it should do.

But to look for discrimination, even of the same sort, in other places is a whole different set of considerations than what the commission knows about. And has expertise in. I mean, one of the proposals that was kicking around at the time of the unfairness policy statement was, well, maybe we should use Section 5 to say boards of directors should be more representative? Elizabeth Warren, call your office.

And that was the kind of thing that the Commission and Congress were trying to get away from. And that's why those subjective kinds of values I think is something that the unfairness statement says in general we can't do that. And even if it's something we might do, it's probably more appropriate for a different agency to do it.

DAVID VLADECK: I have a seemingly different answer. I agree with Howard that this kind of issue would arise mostly ECOA or FICRA or some of the other statutes the agency enforces. But I think to the extent that there is some intentionality here, then it would fit under the Unfairness Doctrine. That is if there was reason for the designers or the users of the algorithm to know that it is somehow either inadvertently or because of the training data systematically excluded x people based on gender or one of the suspect classes, I think the agency would have an unfairness case. But I think the burden on the agency in a case like that would be very high.

JAMES COOPER: I imagine you probably don't want to weigh in on that.

MAUREEN OHLHAUSEN: It's been covered.

JAMES COOPER: Yes, it has been covered adequately. Just while on this about-- and you raised something, David-- I think it's interesting about early on in your earlier response thinking about some of the problems, do you think-- and both really both David and Howard's people enforced, sat there and looked at the complaint recommendations and thought about what relief you should get. Do you think the FTC in its 13(b) equitable powers-- I mean, do you think it's hamstrung at all in its ability to get adequate relief in privacy cases?

I realize the commission I think on a bipartisan basis has been on record as saying that in data security cases, civil penalties authority would be good. And I could be wrong, but I think that's right.

MAUREEN OHLHAUSEN: That's correct.

JAMES COOPER: But leaving aside that, in privacy enforcement, do you think there needs to be a bigger stick than what we have now? Which it seems in many cases, when these are apps that are free and collect data, it may be very difficult to get equitable relief under 13(b).

DAVID VLADECK: In my own view-- and I don't think this is the Commission's view-- is that there ought to be original finding authority under 13(b). And take Ashley Madison, there's no way to do meaningful redress there. Injunctive relief is not going to give much solace to people whose marriages ended or whose spouse committed suicide. So I do wonder about the ability of the Agency to forge any kind of effective remedy in those cases.

I also think that if you look back at some of the cases that we brought early on during the Liebowitz era, I think the simple penalty, for example, against Google or Facebook, initially would have had a deterrent value. Facebook is currently under investigation again. Google, it took only two years before it violated the consent decree. I do think there ought to be initial finding authority under 13(b).

I think the Agency, the Commission would have to use it carefully, particularly where other remedies were just simply inadequate. But I do think 13(b) cases ought to be-- I think civil penalties ought to be available in those cases.

JAMES COOPER: Howard, I don't know you want to weigh in on that.

BILAL SAYYAD: Sure. Yeah, no, I don't like the idea of civil penalties and especially in an area like privacy. I like the original scheme of the FTC Act that's essentially the one bite at the apple, because the precise meaning of unfair and deceptive is not that clear. And the way the Act was set up, the Commission could get an order. And if you violated the order, you were subject to civil penalties for that.

But civil penalties sort of presume a really clear standard I think what's a violation and what's not. And that's not so clear in a lot of the privacy areas. I think it is a lot clearer in data security. I do think civil penalties there make a lot more sense. But in a lot of privacy and some other areas, I think monetary relief is not appropriate.

JAMES COOPER: All right. So, Howard, while I have you, we're now turning to kind of how we are seeing a shift, we look at the GDPR-- or some changes in the landscape of privacy regulation around the world and throughout the United States. We see GDPR, California, the FCC privacy rule that's now in a funk. They all seem to be taking a lot more of a FIPS-based approach, a notice and consent, deletion rights, correction rights. We see in the GDPR and California.

On the other hand, we have the FTC, which has been really based on demonstrating likely consumer harms or deception. And this tees off a little bit-- we've discussed a little this in the ex ante versus ex post discussion, but do you have any thoughts on why you think we've seen a trend toward this, at least in recent evolution of the these newer privacy schemes, away from a harms-base and more toward a consent-based?

HOWARD BEALES: Well, I think I think two things. One is-- and I think this remains true-- there's a remarkable unwillingness to articulate what are the harms we're worried about or inability to articulate what are the harms we're worried about. And if you can't do that, then it's hard to do a harm-based approach, especially as an across the board regulation that applies to absolutely everything. You've got to think through the harms that you're trying to prevent first. And there's been to me a remarkable unwillingness to do that.

Second, I think the FTC in the last few years has-- it certainly hasn't abandoned worrying about consequences. But it's also moved towards more what I would call of FIPS plus in its enforcement actions. I mean the Vizio case is a really good example.

There's just no way to tell the story about that case that doesn't come down to notice and choice. People were surprised to learn-- did it violate their expectations to learn that their internet connected TV was connected to the internet? Really? And did they think that it was making recommendations for the next thing they should watch without knowing what they had been watching in the past? Really?

MAUREEN OHLHAUSEN: It didn't make recommendations, Howard. It said that's what it was collecting the data for.

HOWARD BEALES: But it didn't make recommendations. Well, the complaint doesn't charge the failure to make recommendations.

MAUREEN OHLHAUSEN: But it charges that it is collecting the data and sharing it--

HOWARD BEALES: For ratings purposes. This was a completely innocuous use. There's no harm there at all. No harm there at all. Other than people didn't know. It violated their expectations. But why is that bad?

MAUREEN OHLHAUSEN: But it was also collecting data, like even if you weren't watching something streaming, you were watching a DVD or something, it was collecting and reporting that this television watched this DVD. So that's not a ratings purpose.

HOWARD BEALES: Well, and again, what's the-- I mean, it is a ratings purpose, because how are people spending their time with the set, which is what the television rating services are busy measuring is how much time is this is set on. That's what box top is recording.

MAUREEN OHLHAUSEN: But that's not what was being collected.

HOWARD BEALES: But this is complementary to that data.

DAVID VLADECK: In addition to that data.

HOWARD BEALES: Well, this is competition for Nielsen. It's got a box that measures what the TV is on and what channel is it tuned to and that's about it. It's additional information about whether people are actually watching a TV show on the channel that it's tuned to or watching something else. I mean, you can say it was unexpected, but I don't know why it's bad?

DANIEL SOLOVE: Well, I guess there's a lot of dispute about harm. This is one of the problems when it comes to harm is that you say, well, that harm's never articulated. Well, maybe the harms that you would think is what harm is not articulated. I mean, there are harms in some of these cases that don't necessarily mean that someone's out financially or their reputation is ruined. And part of it is consumer trust, that you know you buy a product, you think something is going to be used in a certain way, and suddenly discover, well, whoa, all this other stuff is going on.

And that doesn't just hurt the consumers. It also hurts other industry. People start to not trust it, well, gee, I don't want to buy you know the Nest things, because they're going to do something

with my data. I don't want to buy a Google Home. I don't want to go and use these new technologies, because I can't trust what they're going to do. Nothing they say-- and it could be a different company.

But if consumers start losing faith that what's told to them, what they expect is not what they expect, all these products, they're going to start to say, why do I want to start bringing this stuff into my home, when you know it seems like to everybody the common story is they're doing something else with it that I didn't expect. And that hurts other companies. And it undermines the companies that are doing the right thing and are saying what they're doing with it and then doing that. And then if they want to use it for something else, tell people. Try to get their consent.

DAVID VLADECK: The is the Bob Bork problem. This is why we have the Video Privacy Protection Act because someone went to-- they used to have stores where you could rent videos. And everyone was outraged because who knows whether he was sitting there at night watching Disney shows or porn.

HOWARD BEALES: But Vizio says, to me the Vizio case seems to say the store can't keep the record. Now that seems that seems crazy. They're not publishing this.

DAVID VLADECK: It's a TV set. It's not your content provider. It's not your content provider. It's a TV set. It's like a radio. It's not a content provider. And what Vizio is doing is keeping an account of what you watch and selling it with no restraint on selling it.

HOWARD BEALES: They're selling it anonymized.

DAVID VLADECK: Well, OK, but that's why have a Video Privacy Protection Act, because Congress--

HOWARD BEALES: There's nothing in the Video Privacy Protection Act that would keep the store from reporting the aggregate rentals by title. That's true. And that's what Vizio wanted to do with this data was stuff by title.

But I just wanted to say that if we think about the problem the way Daniel just characterized it, then I think it's a problem that has no solution. I mean, there are going to be-- there's an interesting article in The Wall Street Journal today that I didn't read closely about 5G and why it's important to be first, predicted among other things we're going to have internet connected tennis shoes.

Now imagine having to read the privacy policy for your shoes and your light bulb and everything else. There are going to be things that happen in this new world that consumers will not know about. All right, their cars will do things now that they don't understand how it happens or that it happens.

If the goal is for consumers to understand at a technical level what's going on and how all the information is being used, we're not going to get there, guys. Let's think about what's second best.

DANIEL SOLOVE: Well, I think the consumer-- I totally agree with that point. Consumers really aren't going to understand the technical thing. That's why I think the FTC plays a great role here as a backstop to say, look, someone's got your back. If the uses are going to start to get so far afield, so unexpected we're going to stop that. We're going to keep that in check.

And I think it shouldn't be like, OK, wow, you're going to be totally ruined. That shouldn't be the standard. I think it should just be-- obviously, if there's a small variation in use and it's very innocuous, it's not a big deal, I don't think we should go after trivial things. But I think significant variances in use are aren't totally trivial. And it's not like it's impossible.

And you can also look at circumstances. How hard would it have been just to try to shape expectations a bit better about what this product is going to do? Companies should have some kind of an obligation not to just hide the ball and secretly do things. I'm not saying it has to be a fine print of a privacy policy.

But the more people understand a little bit about like, OK, what are these new products doing and what are the consequences, there's an education that needs to happen as we make the these changes. And it's not happening because there's no incentive to do it. It's like, great, I can get away with just doing it on the fly. And no one's going to come after me.

HOWARD BEALES: I think the important backstop, though, is not that I know there's nothing surprising happening with my data because, I'm sorry, whatever your data is there something that would surprise you that's happening with it almost for sure. And even if you're quite sophisticated about what's being done with information and how it's being used, that's probably true.

The question should be, is there something that's being done with that data that's creating a problem? But the mere fact that I didn't know it was there is not the problem.

JAMES COOPER: Well, now, that Daniel and Howard agree on the role of consumer expectations in privacy. Great. We solved that problem I want to make sure we have time for some of the questions we got. But I want to turn back to David. In my introductory remarks, I kind of posited that we're at an inflection point, that there's something out there seems to be to be at least have a lot of people talking or suggesting that we need to rethink privacy here in the US, maybe moving us closer to the EU. We see this in California.

So to David, do you think that the pressure for national and international conformity is going to drive federal privacy law closer to these other models, whether we like it or not?

DAVID VLADECK: I think that the enactment of the California statute and sort of the smart implementation of it, deliberately slow implementation, has created an interest in many other states to see if they could replicate what California has done. And so I don't think that Congress is going to immediately race to enact federal privacy legislation. But many of the most important statutes that we have, the environmental protection laws, the occupational safety and health laws, these were all enacted basically in response to an emergement of state law.

And so my guess is that unless the business interests that are unhappy with the California law succeed in either scuttling it back in the California legislature or attacking it successfully in court, you'll see other states moving to adopt a regime based on the California statute, which is to some extent based on the GDPR.

And so the other force that is very much at work and the privacy lawyers either here or watching this on the web, they know this because they've spent the last six months advising clients nonstop on compliance with the GDPR. So I do think it's going to have an influence on the United States. I think that that's problematic in and of itself. I think there are many laudable goals in the GDPR.

I think for the United States to adopt that kind of approach would be very difficult. I mean we are not based on a code system of laws. And the GDPR reads a little like the Napoleonic codes updated a little. So I think there's some friction in the joints. But I do think that particularly California's got 37 million people. It's the fifth largest economy in the world. It is the locus for much of the development, the tech community. And I think it's going to be highly influential.

And I think I think the FTC has to be very conscious about what's going to take place as a result. And I do think that Congress has basically made itself relevant in this debate. And that may be a good.

JAMES COOPER: Howard or Daniel.

HOWARD BEALES: I agree with that. I would point to a slightly different example of what I actually think is probably the most likely outcome. California is big enough to sort of drive things substantively. But it turns out so is Vermont.

Vermont passed a law requiring labeling of anything that had genetically modified organisms. That provoked industry support for a preemptive federal law that says you got a label if it's got genetically modified ingredients, but you can label by a QR code that people can scan and go to a website to figure out whether it's genetically modified or not. There will be pressure for a preemptive federal legislation. What that federal legislation will look like is not so clear. But I think there will be that pressure.

DANIEL SOLOVE: In the early days of a breach notification, I remember I testified before Congress right after the Choice Point breach. This is 2005. And there was interest, very strong interest in Congress, look at all these states are starting to pass breach notification. And industry was all behind it. We have to comply with all these different standards. And this is going to be very complicated and expensive. And we really need some federal preemptive law. There was even a couple of bills kicking around. Nothing happened.

So I have very little faith that this Congress really can pass a law, let alone tie its shoes. So I'm not expecting, even though I think that some of these laws could benefit consumers and benefit industry to have some in these areas. I just don't think it's likely. And so I think Congress just will not have the roles unless it somehow gets its act together. It really won't.

I mean, the most significant privacy legal change that was passed was passed as part of Obamacare. It was that was the HITECH Acts updating of HIPAA and passing the notification rule. And that's really the big accomplishment for Congress since 2000 really. Not much has gone on.

So I don't hold out much hope. And so I think it's going to be what it is. And I think there's some problems with that approach, when we're going to have a lot of varying state legislation on privacy. Breach notification is at least something that's more focused on one thing. And you variances, all sorts of different laws, like California's with different variations is really going to be a big nightmare for industry to comply with. And I don't necessarily think that's a good thing.

HOWARD BEALES: I will say when I started at the FTC in 2001, everybody said internet legislation and privacy legislation is going to pass right away and you guys better get behind it.

DAVID VLADECK: Well, we said that at the beginning of the Obama administration as well.

JAMES COOPER: Maureen.

MAUREEN OHLHAUSEN: I was just going to point out that Congress and the FTC aren't the only actors in this drama, or the states. So NTIA and NIST and Department of Commerce and the White House are considering pass forward. Do we look at some sort of approach that would allow more of a uniform privacy framework to add to be put in place? So I would encourage people to pay attention to that process as well.

JAMES COOPER: I just got a card-- I was going to wait for the audience, but this says, point of fact, HR 6743 Federal Data Breach is going to the full House. And it was just voted out of committee today. So breaking news here. I'm guessing it was prompted by this panel. So think immediate action. Immediate action.

So we're talking here about the pressure, the external pressure on the US. One thing that we have here in the US is the First Amendment though that seems to push back against privacy regulation. So I wanted to, Daniel, turn to you. And I know you've written and thought about this the sort of international or at least the comparative privacy law, do you see any problems with extraterritorial application of elements of the GDPR? For instance, we see that the European Court of Justice is now considering the extraterritorial application of the right to be forgotten. We saw a Canadian court deal with some of that early this year with Google. So do you see that as a potential pushback?

DANIEL SOLOVE: I mean, there's definitely certain problems with that. I mean a lot of laws, including US laws, have extraterritorial application as well, including the California law. And I think that to some extent every country and every region has a right to regulate those who do business in its borders. I guess one thing is good luck enforcing that over in the US. If a company is not in Europe, the GDPR says it applies, but I don't see what they are going to do to really enforce it.

So it's there on paper. It looks scary on paper. But in practice, it's kind of a joke. They really can't enforce it.

There are certain aspects of GDPR that wouldn't fly under the First Amendment. But there are a lot of aspects under it that are fine under the First Amendment, that are embodied in various US laws. I can look to a lot of different provisions of GDPR and find analogs and similarities in US laws, including even right to be forgotten. There are already rights to be-- COPPA has one, for example.

So a lot of these aren't like foreign radical concepts. There are certain things about GDPR that just will not fly in the US for First Amendment reasons, as well as just general US approaches. So the idea that you need to have a lawful basis to process data, that you have to be somehow authorized to do it and there's only certain justifications that allow you to even use or collect data, I don't think that would really work in the United States. It's just so contrary to the US approach, which is generally a permissive approach, like you can use it unless there is a problem that's caused by it. And that's generally the US approach is not to just say you know you need authorization to do something unless what you're doing starts creating an issue.

So I don't see that being carried over. But I think a lot of the things that GDPR does and a lot of things these laws do are not so radical and foreign and different to the US. You look at HIPAA, you look at GDPR, there's a lot of similarities. Actually much more than the California law. HIPAA has a lot of similarities.

A lot of GDPR is just having a privacy program, doing basic risk assessments and other things, all of which HIPAA requires. And the GDPR often doesn't say a lot about what those things should entail. It says, hey, do privacy by design and do it early. But it doesn't say what you're supposed to do for that. It's largely empty. It says do a private impact analysis. But it doesn't have a lot of specificity on these things. It's sort of how HIPAA is in a lot of ways too.

So in a way, I don't think things are so radically at odds with each other and that the GDPR approach is radically incompatible with the United States. I think there are certain things that won't transfer over. But I think the things that transfer over, the commonalities and the things that could work are more than the things that can't.

JAMES COOPER: Anyone else want to jump in on that? All right, so in our little bit of time left, I've gotten lots of great questions. Unfortunately, I won't time to ask all of them. But I want to direct one to Maureen because it's right in your bailiwick. It has to do with the FTC taking advantage of its dual role as both having consumer protection and competition side and using that to examine the impact of data, not just in the consumer protection dimension, but on the impact on small business competition and entry. I know you've written about that and thought a lot about the mixing privacy and competition.

MAUREEN OHLHAUSEN: Certainly, in a competition analysis, data could be considered, if it is an asset that is being combined in a merger, in a way that is going to reduce competition in some way. I mean much like combining two distribution systems or combining two factories.

I think one of the questions, though, is really a lot of times concerns about privacy are really what are driving concerns about trying to use privacy in a competition analysis. So it's not really about hurting competition. It's about hurting privacy.

So I think there are certainly are examples one could think of. So say there were two very privacy protective handset manufacturers, and they sort of had that big part of the market. And so you could say that was a separate part of market than other handsets. And they were going to merge. And then they were going to have a high market share of the handsets that compete on privacy attributes.

That could be an antitrust case, just like you could have two manufacturers of super premium ice cream who want to merge.

JAMES COOPER: Just hypothetically.

MAUREEN OHLHAUSEN: Just hypothetically, super premium ice cream, that was the case. And anyway, so I think it's not that data cannot be a part of it. The concern has to be about competition.

Now, on the other hand, we have had situations where one company is buying another company and they're going to be combining data sets. They're not horizontal competitors. It's not that it's taking the competitor out of the marketplace. But the data that is going to be transferred over to the merged company was collected with a certain set of promises.

And so what we've said through the head of Bureau of Consumer Protection the promises travel with the data. So if you collected this data and said, we're not going to use it for marketing, and then they're going to combine it and then use it for marketing, they would have to get a new set-- well, basically a new consent from the consumers. So if the consumer says, well, no, no, that's not what I wanted, then they would have to take them out of that data set.

So that I think that's the way it has been handled. I mean, there are merger cases where you are combining two very unique datasets. Like we had a case about mapping used for insurance. And we had a competition remedy because it was going to reduce competition. And so we actually had a remedy that required sort of replication and sharing of this dataset.

But often these types of mergers that involve a lot of data, they're being combined to create what we would consider in antitrust like a new product, like a new efficiency, as long as it's not harming consumers as a consumer protection matter. And that wouldn't be considered a negative kind of thing.

I actually have an article about this called "Competition, Consumer Protection, and the Right Approach to Privacy"--

JAMES COOPER: She will be outside signing it on the way out.

MAUREEN OHLHAUSEN: It's in the Antitrust Law Journal on 2014. But it's not to say these values aren't important. It's to say what tools you use that's an important consideration. If you are concerned just about someone is going to use data in a way that harms consumers, that's a core consumer protection issue. And you should use those tools if you are concerned that this transaction that involves data sets is going to reduce competition, either competition on privacy or competition in some other form, then antitrust is the right tool.

JAMES COOPER: Anyone else?

HOWARD BEALES: Yeah, I just think there's a different perspective on it that is also important. As we look at it as states and Congress look at additional regulatory requirements, those often have differential effects on competitors. And in particular in the privacy world, it is a whole lot easier for a consumer-facing company like Google or Facebook to get consent than it is for the behind the scenes somebody that does exactly the same thing using exactly the same information, but they collect it via cookies planted by a host of different publishers participating in an advertising network.

But that is the competitive fringe in the online advertising market. And regulations that make it harder for them help to entrench Google and Facebook. And that's not necessarily a good thing. But it is very much a competitive concern.

JAMES COOPER: So here is a question or 2 minutes and 21 seconds left about the-- it didn't come up surprisingly, but we kind of touched around it-- the privacy paradigm. Maybe Dan, I lean this one first at you first, but the audience member says, how do you reconcile the fact that consumers right away value privacy highly when asked, but they tend to do things that contradict these stated values? And I think we all know that is a privacy paradox. That stated preference seems to diverge from revealed preference in the privacy space.

DANIEL SOLOVE: Alessandro Acquisti, an economist at Carnegie Mellon, has done some really great work on this and studied this very effect of people what they say and what they do are at variance. And that's often the case. And part of it is that the choices that people have and the way that they make those choices are shaped by how those choices are presented to them and a bunch of other factors that could lead them to make choices that are not always consistent with their stated attitudes.

And so we might say, well, what is true? Do we say the behavior is the truth about what they really value? Or is it what they say?

I actually think it's neither. I don't think what they say is actually reflective of how they actually value something. But I don't think behavior is always a good metric either, because there's a lot of things skewing the behavior. And Acquisti does a great job of pointing out all the different skewing things on the behavior.

So in a way, it is very difficult to measure what consumers actually value, because I think both metrics are problematic for doing that, because a lot of it's how informed the consumer is and

what information they're given and so on. And you get very odd effects. One of his studies is very interesting.

He had two groups. In one group he told like we are going to collect very sensitive data. In one group he said, we're going to protect it. We're going to give all sorts of privacy protections and security protections on it. And the other group he said nothing. And guess which group disclosed more? The group he said nothing to.

And so it's almost like punishing you for actually doing the right thing. And that's because when you told people all the privacy and security protections, people's minds suddenly woke up. Oh, my gosh, maybe there are these risks that I didn't think about. And that made them more cautious.

So a lot of interesting effect. And I just urge you to read his work. It's very illuminating and he did a much better job than I did at tackling this issue.

JAMES COOPER: Oh, I'm sorry, David.

DAVID VLADECK: I make one other-- people are generally presented with take it or leave it offers. I mean either you are on Facebook or you're not, or you use Google search or not. And we did some research when I was at the FTC about these issues. And part of it just-- and this just sort of echoes with what Dan says, how the choice is present.

JAMES COOPER: Howard.

HOWARD BEALES: I think how you frame it clearly matters. But consumers have all sorts of preferences where it's a perfectly valid preference and a perfectly real preference. But when they confront the cost of satisfying that preference, they make a different choice. And there are issues of how you pose the question and how you define it and what consumers know. But there's also these choices have costs. And consumers may make them differently.

Example I like is organic foods. Something like 48% of consumers say, yep, I prefer organic. Organics markets is about 5%.

JAMES COOPER: All right, well, I wish we could go on forever. I'm sure the rest of you all do. But we are out of time by the six 0s on the clock up here. So join me in thanking this great group today. I will await my instructions from below.

BILAL SAYYAD: We have one more little end note, if Howard Shelanski, professor here, will give closing remarks. And here he comes now, the Price Is Right style.

HOWARD SHELANSKI: All right, great. Thanks very much, Bilal. And thanks to all of you for being here. I'm used to at academic conferences saying I'm standing between the audience and cocktail hour. There's no cocktails here. So you guys are stuck. I will nonetheless keep things brief.

I want to start by just reiterating what Dean Treanor said this morning. It's a real honor for us here at Georgetown to be able to host these first days of this series of hearings that the FTC is hosting. We have a deep connection to the FTC, as Dean Treanor explained. And it's really just wonderful to have such a vibrant debate and so many of you here today. And special props for my antitrust students who showed up. I really appreciate that. Former students, so they're not getting any benefit from this, since I'm not teaching it this semester.

One of the things that I think is particularly heartening about today's discussion is we really see the full integration of the Agency's consumer protection and competition missions. I think both of those are front and center. Certainly the last panel makes it very clear in the issues that these hearings are tackling.

And you heard Bilal say earlier that the Bureau of Competition and the Bureau of Consumer Protection are really complementary. I might add, Bilal left one thing out of his formulation, which was the Bureau of Economics. And it's my view that with a small handful of FTEs, the Bureau of Economic could actually be completely substituting of both of those other bureaus. But that's perhaps a chauvinist stick view from someone who spent some time at that agency and in that bureau.

The importance of these hearings really can't be understated. I think one of the great things of the American regulatory system writ large and one sort of a distinguishing set of characteristics that one sees when one goes around the world and sees how regulation and law enforcement is done in many other very sophisticated jurisdictions is a level of transparency and accountability that characterizes the way our federal agencies act.

And to be sure, one could be cynical about certain actions that those agencies take. But when one takes a broad view, it really is quite impressive. Agencies have to justify their decisions. Agencies have to have a coherent framework. And they have to have evidence.

And those agencies don't get to make those decisions on their own because they're subject to accountability through the courts. And you just have to open up the paper today to see an example of a court overruling a federal agency that did not meet those standards. So the agencies have a real obligation.

These hearings fall into that framework of transparency and accountability. An agency that fails to justify its actions in a particular case to a court loses a case. An agency that fails to justify its program and its approaches and framework loses its relevance before the public. And that is I think a very damaging and harmful thing to have happen.

So for an agency periodically to hold sustained public hearings where it examines both the sets of problems on which it is focusing and the analytical framework with which it's approaching those problems is really a very important aspect of maintaining that relevance, maintaining that legitimacy with the public. And that is exactly how I see these hearings and what I see the FTC is doing.

The FTC has always been an agency that cannot stand still and rest too comfortably with the problems it's focusing on or with the tools with which it's analyzing its approaches to those problems. Indeed, that was the spirit in which Chairman Pitofsky launched the hearings nearly a quarter century ago. We were in a time of very interesting economic turmoil with the rise of high technology industries, economics and other tools for assessing where there were competitive harms, where there were harms to consumers were changing and developing. And it was his judgment as chair that the agency needed to go out and make sure that it was well understanding what problems the public was focused on, that it was understanding the industrial changes that were before it, and that it was understanding the state of the art of the knowledge with which you would assess those problems.

Well I think all of those forces are even stronger today. And when Chairman Simons came into office, he came into office at a moment that most of us in the antitrust field and many of us in the consumer protection field recognized as sort of a historic moment. I think there was sort of unprecedented debate-- I don't want to say unprecedented, but certainly unprecedented for the last 40 years-- debate over some of the fundamental framework and conventional understandings of how antitrust should be enforced.

There is a recognition that we have much sharper tools out there for understanding how consumers behave and process information. It's time for the agency to step forward and make sure that it is fully taking account of and understanding that public debate, because if it doesn't, it will keep looking over here and the public will be thinking about problems over there.

So if you open up, again, the paper over the past week, you'll read that there is a lot of public debate, a lot of debate in academia, a lot of debate in think tanks about whether the consumer welfare standard as conventionally conceived in antitrust enforcement is adequate to address some of the concerns about market structure changes or wealth distribution changes, things that the first panel this morning talked about.

I had people come up to me and say, can you believe the FTC invited so-and-so? Those are flaky ideas. They shouldn't be giving airtime to those.

And the FTC and I firmly disagree. These are things that people are thinking about. And they are motivated by the problems that every day consumers are perceiving. And if the agency turns its back on those voices in the debate and doesn't take into account what might be legitimate in those arguments, the agency will lose its transparency. And it will fail the test of accountability before the public.

So recognizing that, we see on all of the panels today and on the panels that we will see in the other 19 days of hearings that I think are scheduled are a real diversity of views that explore the outer boundaries of what would traditionally be thought of as competition enforcement or consumer protection enforcement. And only by taking into account that thinking at the outer boundaries, of hearing about the problems that might be novel or different in form from the way we've seen them before given the rise of large digital industries and AI and new kinds of technology, only by fully exploring them and doing what Chairman Simons said we should do and that he would do in his opening remarks, follow the evidence. Follow the evidence to

identify where there was really a problem. Follow the evidence for where we have a good understanding of tools that can resolve those problems.

In that way, the agency will do two things. The agency will modernize its thinking. It will better be able to explain its actions. Even where the action is inaction, it will better be able to say action is not warranted, or we don't know enough to have action. And we're making that decision having taken into account the state of the art thinking and having really heard from the public, from stakeholders of all kinds, about what the problems are that they are feeling and that they are sensing out there in the marketplace.

By doing that, the agency will become more effective. It will modify its framework as it needs to be more effective. But it will also be more effective and transparent in justifying what framework eventually arrives at after these hearings.

So these are more important as events than the one-off kinds of conferences that very often characterize a field. They are a sustained and iterative process over 20 days, where some of the same issues will come up again and again. Everything is documented. Everything is public. And at the end, there will be reports very transparently explaining what evidence the agency is crediting, what arguments its crediting, what arguments it doesn't feel it can credit, and the technology, if you will, of consumer protection and competition enforcement under Section 5 at the Agency will be all the better for it.

So this is an important enterprise. Its an important enterprise not just for the people on the different panels. But its an important enterprise for all of you to participate in-- commenting, sending your comments to the Agency. The Agency has got an open window for those comments right now-- because it is a unique moment that we might not get again for another 20 or 25 years, or else it will occur incrementally through the case by case kinds of transparency and accountability.

So this is a critically important moment. I think this is a really auspicious start today to that moment. I look forward to following and participating in some of at least the remaining 20 days. I would encourage all of you to do so as well. Thank you.

[APPLAUSE]

BILAL SAYYAD: So I'm just here to say thank you. And say 5% down. And then our next session, September 21, Constitution Center, so not very far from here. And that will get us, I don't know, 10% down. Thank you. Thank you. Thank you to the panelists. Thank you to everybody.