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-- tMc 0ATj (t

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,

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

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 expen hTo bee.

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

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

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

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

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

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.

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.

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

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 inad

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

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 BEALE0.002 Tw -9.25 -2.Td [(A poroi)-22 (-22 (-t4 ()-1 z)9 (Ei.9 (w it t(in)2 w)22t)-9.9 ,2 (u)2.9

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 diff (i)-2 (ua1 Td [(p)2 (rs)-1 (2 (e)4 J 0 Tc -0 Tw 0i)-2 (i

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 poisla6 (S)-4ubC /P <o FT(a)-6 (r)3 (e)4 (s)-0 (s)-1 oidt the

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 prem(i)-2,e1(us)9igS6 (ttr)5

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.

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

identify where there was really a problem. Follow the evidence for where we have a good