

















































































































































































































































































































































































































1 out lacrosse players and people with male names and  
2 systematically dropping out of consideration people  
3 who went to all women's colleges and other folks who  
4 had, you know, sort of clear indicators that they were  
5 female because Amazon, like many tech companies, has a  
6 predominantly male workforce.

7           And, so, yes, it is certainly true that data  
8 can be used to undermine -- to eat away at insidious  
9 biases. It can be used to entrench those biases and  
10 to hide those biases and sort of make them look  
11 natural because, you know, the machine is not biased,  
12 right? The machine just came up with it. We don't  
13 know how it ended up with all of these male lacrosse  
14 players as, like, the people we should hire next, so  
15 it can cut both ways. That's what I want to say.

16           MR. BEALES: There are discrimination  
17 problems out there in the world. There's no doubt  
18 about that, but they are discrimination problems.  
19 They are not privacy problems.

20           MS. MCINNIS: So I just wanted to make the  
21 point that having accuracy in the kind of behavioral  
22 ad delivery, whether or not there's a privacy issue in  
23 that, is not necessarily the framing that I would  
24 suggest. I would say that the privacy issue occurred  
25 in the outset where you collected my data without

1 permission, online and offline, to create a kind of  
2 personalized dossier about me with conclusions that  
3 may or may not be correct in order to serve me with  
4 behavioral ads and also different prices. And so that  
5 is, I think -- the privacy infringement occurred at  
6 the beginning. Also, when you didn't follow my do-  
7 not-track signals, which many companies do not follow,  
8 even though most browsers allow you to signal that.

9 In addition, I just wanted to point out that  
10 most consumers -- some consumers might feel like  
11 they're benefitting from targeted ads, but a lot of  
12 consumers do not and, in fact, many consumers feel  
13 freaked out or concerned about the kind of  
14 advertisements they've been served with. The kind of  
15 conversations around whether or not Facebook or  
16 Instagram is listening to you is the kind of example  
17 here where consumers have no idea how they're getting  
18 such targeted advertisements based on things that they  
19 only said out loud.

20 And, so, that kind of disconnect between  
21 consumer knowledge and the kind of tracking that's  
22 happening is a huge problem that should be addressed  
23 before we talk about the efficiency or the worth of  
24 these advertisements.

25 MR. COOPER: Let me -- Allie, maybe you can

1 answer this or react -- but while we're on the subject  
2 of price discrimination or personalization and  
3 predictions, we have a question from the audience that  
4 I think is a good one, sort of clarifying perhaps.  
5 You know, you mentioned dynamic pricing, but is  
6 dynamic pricing really price discrimination because  
7 dynamic pricing is really just adjusting the price to  
8 supply and demand conditions? So should we think  
9 about that as price discrimination or just kind of  
10 changing the market equilibrium based on shifts in  
11 supply and demand?

12 MS. MCINNIS: So I don't really think it is  
13 about supply and demand, right? It's about my  
14 possible willingness to pay. And by having these  
15 kinds of tailored prices and tailored advertisements  
16 to me, you're also diminishing my share of the  
17 consumer surplus, which is a harm.

18 MS. BOHM: So I want to address two  
19 definitional things. I think there's sort of dynamic  
20 pricing, sort of lowercase D, which is, hey, most of  
21 the tickets on this train are sold out, therefore, for  
22 everyone, all of the tickets are more expensive. And  
23 then there's the kind of dynamic pricing Katie is  
24 talking about, which is, hey, they've realized that I  
25 live in a wealthier area and, you know, I'm a lawyer

1 and whatever and they realize I really desperately  
2 want to go to New York this weekend, and so they're  
3 charging me a higher price. There are two different  
4 things there, and at least to me, one of them raises  
5 more concern than the other.

6 I also want to really quickly address  
7 Howard's point that that's not a privacy concern,  
8 that's a discrimination concern. I think there's a  
9 definitional thing there, too. So there are certainly  
10 folks who are concerned about privacy as a "I want to  
11 be left alone, I am the king of my castle, leave me  
12 alone." And there's nothing wrong with that. That's  
13 really important. You know, privacy does extend from  
14 sort of the Brandeisian property rights idea, but  
15 there's also privacy is a way that we make sure to  
16 protect -- or I should say lack of privacy undermines  
17 some of the other values that are really important to  
18 us. And that includes things like civil rights,  
19 access to opportunities, having fair access to  
20 information online, sort of what does lack of privacy  
21 lead to? Informational disparities, discriminatory  
22 access to opportunities.

23 And, so, when I talk about privacy harms, I  
24 do think about some of the discrimination and more  
25 civil-rightsy harms because I think that, you know, as

1 Katie sort of more artfully explained than I did,  
2 these are sort of when you take the privacy violations  
3 and the personalization as far as they can go or maybe  
4 not as far as they can go but, you know, sort of to  
5 their conclusions, that's where you end up.

6 MR. COOPER: Thanks. So I think both, Katie  
7 and Allie, in your presentations you had talked --  
8 said that, you know, self-regulation doesn't appear to  
9 be working in this market, so I wanted to put that on  
10 the table that, you know, has self-regulation failed  
11 to protect consumer privacy here? And if that's the  
12 case, what's the alternative?

13 So I'll let Garrett kind of take the first  
14 cut at this. And then Leigh may have something to  
15 say. I'm not sure.

16 MR. JOHNSON: Great. Well, I'll start by  
17 saying that I think an opt-out option is highly  
18 desirable in that we have the kind of two facts here.  
19 Online behavioral advertising generates a tremendous  
20 amount of revenue for publishers, and also we have  
21 people that are very concerned about their privacy.  
22 So an opt-out allows these things to coexist.

23 Other policy options have to go down the  
24 ways of hard tradeoffs of ignoring one or the other  
25 considerations. So I think the AdChoices program has

1 some advantages. Because it was rolled out by  
2 industry, it was done relatively rapidly. It had good  
3 coverage. It's kept up with a fast-moving technology  
4 frontier, but there's certainly, you know, lots of  
5 complaints about it. You would hope that the industry  
6 would apply some of the same determination it does to  
7 putting identifiers on consumers' computers as it does  
8 to making sure that the opt-out choice remains  
9 preserved and isn't just deleted by a cookie.

10 They have done some work on this by creating  
11 a ad extension -- an app -- sorry, a browser extension  
12 that preserves these preferences, but that's not very  
13 easy to find on the website. You'd also expect that  
14 if consumers care so much about online behavioral  
15 advertising, you would also expect that they would  
16 have strong preferences against things like database  
17 matches. And, so, this would be something that the  
18 industry might want to consider extending there as  
19 well.

20 Now, the other question was about  
21 alternatives. So this is a really tricky thing,  
22 right, because one alternative is to go down the way  
23 of a browser do-not-track route. And that would have  
24 the advantage of preserving people's privacy  
25 preferences, but it does have the challenge that

1 browsers could set the defaults in ways that don't  
2 fully internalize the externality that that would have  
3 on the advertising industry and on the web.

4           The GDPR, which we'll be talking about  
5 later, is kind of an interesting case because the  
6 language of the GDPR says that you need explicit opt-  
7 in, where consumers need to present to every single  
8 company in every single use of their data. That's  
9 sort of the de jure expectation, but the de facto  
10 thing we've seen so far is an opt-out. And as Anja  
11 says, the experience of being a European consumer on  
12 the web is not super fun. You get to see all sorts of  
13 consent pages every time you visit a webpage, and  
14 about 90 percent of these people are sort of going on  
15 without opting out according to a data release from  
16 Quantcast.

17           A couple of people have brought up this new  
18 bill presented by Senator Ron Wyden, where he  
19 essentially is arguing for a federal do-not-track  
20 page, somewhat like the Do Not Call List. As I read  
21 the legislation, it's wanted to make the Federal  
22 Government a clearinghouse for some of these consent  
23 mechanisms. You know, there may be some arguments  
24 that suggest that the federal Do Not Call List did a  
25 much better job of protecting consumers than the

1 industry version, but I think if you're the FTC, you  
2 should think very, very long and hard about whether  
3 you want to be doing this job, given just how  
4 technologically sophisticated these things are.

5 So I think I'll leave it there. Thanks.

6 MR. COOPER: Leigh, I'll let you --

7 MS. FREUND: Thanks. Yeah, I mean, when I  
8 think about content -- or the question which I'm asked  
9 a lot, which is, is self-regulation failing, has it  
10 failed to protect, especially now that we're talking  
11 about a new privacy legislation or regulation, my  
12 answer is always as compared to what. You know, what  
13 is the alternative? The industry came together in as  
14 early as 2000 and tried to address the issues that  
15 were concerns at the time.

16 It's kind of similar to -- one of my members  
17 gave me this example, so I'll give them credit, but  
18 I'm going to use it. Seatbelts are not failing  
19 because we still have car accident deaths. Seatbelts  
20 are saving lives. A code of conduct that has strong  
21 privacy protections is helping. If there is more we  
22 should be doing, we're happy to engage in  
23 conversations to do it, but I think you can't measure  
24 the way the industry may have developed without a code  
25 of conduct that has strong privacy regulation or self-

1 regulation within it.

2 So many of our members have declined  
3 business model opportunities, declined to do certain  
4 things, declined partnerships with companies because  
5 those things would not comply with our code. So I do  
6 think we have prevented harm from happening in the  
7 marketplace.

8 And, so, I think the opt-out, as Garrett  
9 mentioned, the opt-out regime certainly is something  
10 that we strongly advocate for, but I will note that  
11 our code does contain a requirement for opt-in consent  
12 when the information that we're using is sensitive  
13 enough. So, for example, precise location data or  
14 sensitive health data. Those things cannot be used  
15 without a user's explicit opt-in consent. And, so, if  
16 there are more of those things that we should be  
17 considering, then that is something we are always  
18 talking about and always trying to do, but I resist  
19 strongly the argument that self-regulation has failed.

20 MR. COOPER: Katie, I know you had your hand  
21 up earlier.

22 MS. MCINNIS: Yes, thanks. With all respect  
23 to Leigh and the NAI, the privacy principles they came  
24 out with in the early 2000s, which, by the way, was in  
25 response to avoiding legislation around this issue,

1 were not strong even back then. And then we've seen a  
2 complete abandonment of these principles over the  
3 course of a few years, right? These principles were  
4 only supposed to be followed by coalition members,  
5 then NAI allowed for other associate coalition members  
6 to join, but they don't have to follow it. They just  
7 have to pay dues. And a few years after --

8 MS. FREUND: That is completely 100 percent  
9 untrue, by the way. You must be mixing up trade  
10 associations or self-regulatory organizations.

11 MS. MCINNIS: Okay. But only a few  
12 companies are following the regulations, even just a  
13 few years after they were introduced. And the fact  
14 that consumers don't know a lot about these tools, I  
15 think, would be another example of the failure of  
16 self-regulation and the call for a data policy here at  
17 the federal level, and the number of committee  
18 meetings we've been having around it is another sign  
19 that consumers are not satisfied with the self-  
20 regulatory tools that have been provided to them.

21 MS. BOHM: Well, so to pile on, so first,  
22 let me just say that, you know, self-regulation is an  
23 important tool as far as it goes, and public knowledge  
24 has been willing and interested in working with folks  
25 in the industry to come up with the best self-

1 regulatory tools they can. They only go so far. And  
2 there are a few reasons for this.

3 First of all, I talked about AdChoices,  
4 right? So that was their self-regulatory tool was  
5 this tool that like, eehh, we know what we would be  
6 useful to consumers, so let's do this other thing. Or  
7 I should say, we know what would be more useful to  
8 consumers, let's do this other thing.

9 I think the other piece is even taking  
10 Leigh, you know, at her word, and she's been quite  
11 lovely to sit next to, is not the one Katie is talking  
12 about. Even if all of her companies are really,  
13 really good actors and they're turning down business  
14 opportunities with really bad actors, there are still  
15 the really bad actors out there who aren't going to  
16 voluntarily play in a self-regulatory regime because  
17 they feel that they can get ahead if they don't.

18 Now, you may be saying, but, Allie, those  
19 bad actors aren't going to follow the law anyways, but  
20 if there was a law and, you know, it gave enforcement  
21 authority to an agency or gave folks -- or to state  
22 AGs, or gave folks a private right of action, there  
23 might actually be redress for the folks who don't  
24 follow the law.

25 So I do think that there is an important

1 role for legislation here, and I think we're seeing  
2 that in the conversations that are happening in  
3 Congress now. And I do want to say that, you know, I  
4 don't see that legislation as legislation as pertains  
5 to the advertising industry, right? I see that as  
6 comprehensive privacy legislation that applies to all  
7 of the actors in this space. Some of them are  
8 advertisers. Some of them are ISPs. Some of them are  
9 completely other entities. So it's not a "let's gang  
10 up on the ad industry." It's a "there's a lot of data  
11 out there, there are a lot of risks associated with  
12 that, let's have some rules of the road, let's create  
13 expectations for businesses, and let's create some  
14 protections for consumers."

15 And I think there's an appetite for that,  
16 and I think it will also benefit groups like Leigh's  
17 that want to be doing the right thing because they  
18 won't have that competitor over there doing the wrong  
19 thing.

20 MS. FREUND: Yeah, and just if I could just  
21 add to that, I think, you know, absolutely. I think  
22 federal legislation and comprehensive privacy  
23 legislation is something we are absolutely thrilled to  
24 talk about. We've been trying to advocate, you know,  
25 for the right privacy protective practices for 20

1 years. And, so, I think -- I do think, however, that  
2 self-regulation has a strong role to play in that.  
3 And I think, you know, the FTC is already resource-  
4 constrained, and we can certainly help keep those good  
5 actors in line.

6 And I agree with you about the bad actors.  
7 I tend to not like them either. So, you know,  
8 definitely, but I do think that privacy legislation  
9 has to balance all of the stuff that we've been  
10 talking about today. So it has to balance privacy  
11 concerns with the innovative, open and free internet  
12 that we have today, and it has to find that right  
13 balance.

14 And so, you know, we are happy to engage in  
15 those discussions and looking forward to it.

16 MR. COOPER: I think we have about a minute  
17 left by that clock, but we're right up at 2:30 by that  
18 clock because I think we started a little late. So  
19 rather than getting into my next question, which was  
20 what would privacy legislation look like, and solving  
21 that in a minute and 15 seconds, well, I think we  
22 actually did, I think Leigh and Allie agreed on what  
23 that's going to look like, and they're working on it  
24 right now, up with Capitol Hill.

25 So, anyway, please join me in thanking our

1 panelists for such a vibrant discussion today.

2 (Applause.)

3 (End of Panel 3.)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25



1           We have a very fine panel here. I'm not  
2 going to read everyone's bios. We have them available  
3 in print outside; we have them available on our  
4 website. I do want to just introduce people by name  
5 and affiliation and then leave time for them to do a  
6 brief presentation, six, seven minutes, and then we'll  
7 jump into our discussion.

8           So moving from my left, Jane Bambauer who  
9 teaches at the University of Arizona James E. Rogers  
10 College of Law; then Avi Goldfarb, the University of  
11 Toronto's Rotman School of Management; Anja Lambrecht  
12 of the London Business School; to her left, Amalia  
13 Miller, the University of Virginia, where she's a  
14 Professor in the Department of Economics; one down, I  
15 can't even see over people. Oh, Lior Strahilevitz  
16 from the University of Chicago Law School; and,  
17 finally, Rahul Telang from Carnegie Mellon University.

18           So let me just turn the floor over to  
19 Professor Bambauer.

20           MS. BAMBAUER: Thank you. Thanks so much  
21 for including me. So I'm glad I'm speaking first  
22 because it's some of the gaps in our knowledge of how  
23 privacy and potential privacy regulation is going to  
24 affect innovation that I'm most interested in or at  
25 the sort of highest level of conceptualizing what it

1 is that we're trying to protect when we protect  
2 privacy. And this is -- I think it's important to get  
3 definitions of privacy harms right so that we can then  
4 compare them to potential tradeoffs with innovation.

5           And I thought for today's comments I would  
6 actually use the Cambridge Analytica example to  
7 illustrate that it's actually quite hard to get  
8 concrete and to get agreement about what types of  
9 privacy harms we ought to have the Government  
10 intervening to manage. And the reason that I like  
11 using Cambridge Analytica is that almost everyone  
12 thinks something went wrong and we all kind of use  
13 it as -- well, we all say Cambridge Analytica and we  
14 all nod and we all agree -- you know, we all use it  
15 as sort of a placeholder for "ick." But if we  
16 actually -- if we each individually define what we  
17 think the problem is that the Government needs to  
18 solve, I think we'd start rapidly splintering into  
19 different groups and could not agree on what direction  
20 to go in.

21           So the first thing that might have gone  
22 wrong is that Facebook users didn't realize that when  
23 they were taking this little personality survey that  
24 they were exposing even their own full Facebook  
25 profile, including every "like" that they had ever

1 done on Facebook to this researcher at Cambridge, let  
2 alone the Facebook profiles of all of their friends,  
3 right. So I think descriptively that's accurate, that  
4 Facebook users did not realize how much they were  
5 waiving away when they clicked -- you know, when they  
6 saw the screen warning them about the privacy  
7 implications and it's like yes, yes, yes, just get me  
8 to the survey, I need the survey.

9 So I'm going to treat the transmission of  
10 their data as a decision that Facebook made, and I'll  
11 come back to the consent idea. But even if we think  
12 of this as being ascribable to Facebook, I still think  
13 it's hard to define precisely what should be done. So  
14 is it that the problem is that we're letting anybody,  
15 either Facebook or third parties, study people without  
16 doing IRB-style informed consent?

17 So, you know, inference winds up being at  
18 the heart of much of what we love about internet and  
19 smart devices and smart services. AB testing actually  
20 involves interventions. I mean, they're randomized  
21 controlled experiments that for some reason the  
22 industry call AB testing. And, so, even, you know,  
23 traditional interventions are a normal part of  
24 innovation, and I don't think that we want to prevent  
25 that from happening or put very cumbersome processes

1 in the way.

2 So then maybe what we should do is allow  
3 Facebook to study its users in that way but not  
4 permit third parties to have access to that sort  
5 of -- either the raw data itself or to the sort of  
6 hypercustomization that that raw data would allow  
7 third parties to do. Well, that gets to the heart of  
8 Facebook's and Google's, for that matter, business  
9 model, right? So there's a reason that Mark  
10 Zuckerberg in his Congressional hearing testimony  
11 rejected the idea that Facebook should shift to a pay  
12 service. I think he knows that people -- he knows  
13 what many of the presenters at this conference have  
14 already said, that people won't actually pay for the  
15 services that they get in money, even though they will  
16 pay in data.

17 I don't think that Congress is ready to kill  
18 Facebook. I don't think we should be ready to kill  
19 that sort of business model. And, actually this  
20 relates to the opt-out idea. On the last panel, there  
21 seemed to be at least a little bit of consensus for,  
22 well, when a consumer opts out, that at least should  
23 be honored. And I'm not so sure about that. As long  
24 as opting out continues to happen at a rate of 0.24  
25 percent, sure, let people opt out. It's a small cost

1 that content providers like Facebook can easily  
2 handle.

3 But if John Oliver convinces a bunch of  
4 young people, millions of people to opt out one day,  
5 then that business model is severely compromised, and  
6 so I don't think -- you know, consent itself could, at  
7 least if it's legally enforced, could wind up wiping  
8 out the payment model that we're used to.

9 Okay, so, finally maybe then the problem is  
10 that Facebook can allow traditional advertisers to  
11 have access to this data and to use hypercustomized  
12 content. But there's something wrong with letting,  
13 you know, untraditional content providers like  
14 political actors have access to the same data or have  
15 access to targeting in the same way.

16 And this really gets to the heart of the  
17 externality that I think many people think occurred  
18 with the Cambridge Analytica story. The line  
19 differentiating, though, like sort of standard  
20 advertising and the kind of content that we think is  
21 suspect because it might distort elections, that's  
22 awfully hard to define and, you know, we're  
23 essentially -- what we would be doing is asking either  
24 Facebook or regulators to identify what counts as a  
25 bias or a manipulation versus just content persuasive

1 or maybe nonpersuasive content that people seem to  
2 want to view based on their clicks.

3 So this kind of raises questions that have  
4 been studied for decades now in the advertising  
5 context of created demand, like is there some -- is  
6 there something about firm -- you know, content  
7 providers like InfoWars that's actually creating  
8 biases and demand for certain types of content that  
9 it's bad for people. Or is it that we've kind of all  
10 galvanized around blaming Facebook and Cambridge  
11 Analytica for a problem that really just kind of is at  
12 the heart of American democracy, that basically that  
13 the only problem with democracy is its own voters,  
14 right.

15 So because all of these, so I'm raising a  
16 bunch of questions without offering answers right now,  
17 so I want to share that the way I'm starting to think  
18 about this and I'm sort of in the early phase but that  
19 there is some, you know, evidence-based work with, is  
20 I'm starting to look for early signs of times that  
21 people may be engaged in a short-term techno-panic and  
22 may be sort of psychologically and naturally geared  
23 toward resistance and hesitancy to a technology that  
24 they will in a short or medium amount of time wind up  
25 adopting and even liking versus persistent forms of

1 privacy preferences that seem to be nearly universal,  
2 and that seem to flow and be persistent even when  
3 technologies are changing. So I can say more about  
4 that during the Q&A, but I don't want to take more  
5 time.

6 MR. GOLDFARB: Hi, I'm Avi Goldfarb. So a  
7 lot of these ideas that I'm going to talk about over  
8 the next six minutes were touched on by various people  
9 over the course of the day, but I want to dig into a  
10 few of them -- to the extent that's possible in six  
11 minutes -- to give a high-level introduction to these  
12 ideas.

13 So we think about privacy. What privacy  
14 used to be was either the paparazzi, it was either  
15 there were a handful of people who were declared  
16 public figures and they had essentially different  
17 rights than the rest of us in terms of the  
18 communication of their private life, or we emphasized  
19 security services and the police and there were  
20 restrictions on how they could surveil the public.

21 Privacy's now a business issue. That's why  
22 we're here, that's why it's at the FTC, privacy's a  
23 business issue. It used to be almost purely a legal  
24 issue or a media issue. Now it's more than that. Why  
25 is it a business issue? It's a business issue because

1 of all the data that digitization of media and of all  
2 sorts of other aspects of life have enabled.

3 And, so, what we need to recognize when we  
4 think about this as a business issue is, we do know  
5 already that privacy regulation can restrict  
6 innovation, okay. There is -- the empirical work so  
7 far is that there is a tradeoff. That doesn't mean we  
8 can't theoretically construct a situation where  
9 privacy would enhance innovation, but the dominant  
10 empirical work so far, and you'll hear more of this  
11 later, but this is at least my work with Catherine  
12 Tucker has been that privacy in the online advertising  
13 space, when you restrict information flows, well,  
14 there's a reason that those companies wanted that  
15 information. They could innovate with that  
16 information; they don't do as well without it. And  
17 that's a theme you've heard. You heard it from  
18 Garrett, and you heard a fair bit in the last panel.

19 Another thing to recognize, and this is a  
20 thing about competition, privacy regulation can help  
21 large incumbents. Okay, so what do we mean by that?  
22 To the extent that there is a -- it happens in two  
23 different ways. So one way is you might be much more  
24 likely to trust Google than some new startup that  
25 you've never heard of. And so you might be more

1 likely to give an old, established, large company,  
2 large brand, data about yourself than a startup.

3 In addition to that, what this particular  
4 paper is about is another idea which is that if you  
5 touch a company in lots of different places or, in  
6 particular, a company touches you in a lot of  
7 different places, that means that one opt-out can help  
8 that company in lots of different ways. And, so, if  
9 you're a startup or a smaller company that really is  
10 only doing one particular product, they have to pay  
11 effectively the same regulatory cost to get you to  
12 consent as a very large company. And that can create  
13 an opportunity and essentially benefit incumbents  
14 relative to entrants, benefit large companies at the  
15 expense of small.

16 So if privacy, if the empirical, theoretical  
17 structures that we have suggest privacy is going to  
18 hurt innovation and it might hurt competition, well,  
19 why are we talking about this at all? And the reason  
20 is that consumers actually do care about privacy. So  
21 this was a debate we've heard. Yes, consumers aren't  
22 opting out of these things, but when we fix a  
23 particular context, we see more privacy-protective  
24 behavior today than we used to. So it's much harder  
25 to get people to fill out surveys than it used to be.

1           The Census has to work harder to get people  
2 to fill out the Census or information. Given a  
3 context for communicating data or when we fix that,  
4 we're even more privacy-sensitive than we used to be.  
5 What's changed and the reason why we had the  
6 discussion or at least I think the reason why we had  
7 that discussion in the previous panel on, yeah, but  
8 consumers don't seem to be doing anything about it, is  
9 because along with more privacy concern has come with  
10 huge benefits to data sharing. And so even if the  
11 costs are increasing or the perceived costs of sharing  
12 data are increasing, the perceived benefits, the  
13 ability to have Facebook and Google, et cetera, has  
14 grown as well.

15           And so the point is there's a tradeoff  
16 between privacy and innovation. In lots of cases  
17 there's a tradeoff between privacy and competition.  
18 But that doesn't mean that privacy is bad, it just  
19 means that we need to recognize these as distinct  
20 values, and we need to think about weighing them  
21 against each other.

22           So the policy issue -- the theoretical  
23 policy issue is essentially privacy regulation can't  
24 be too strict because if it's strict it will stifle  
25 data-driven innovation and competition, right? If you

1 don't allow firms to use data, they can't use data.  
2 And if data enables competition, as we heard earlier  
3 today, or as I just described, or if data enables  
4 innovation, it's maybe the core input into a lot of  
5 the most exciting technologies today, artificial  
6 intelligence, ad exchanges, et cetera, then data --  
7 you know, then privacy regulation will be too strict.  
8 Or strict privacy regulation would hurt innovation,  
9 hurt competition.

10 That said, we got to remember, privacy  
11 regulation can't be too lax either. If it's so lax  
12 that consumers don't trust companies, then the  
13 companies won't get the data either. In Europe and  
14 the United States, at least the empirical evidence so  
15 far is we're a long way away from that. It's not  
16 clear if we are worldwide.

17 So getting the balance right is the key  
18 challenge here, and given the importance of data to  
19 innovation, and AI in particular, privacy policy is  
20 one important way the regulatory environment is going  
21 to affect the rate and direction of innovation and the  
22 degree to which competition plays out.

23 With that, Anja.

24 MS. LAMBRECHT: Thank you. So I'm going to  
25 build directly on what Avi just said and start with a

1 particular setting which is financial services. And,  
2 so, you can well imagine that in financial services,  
3 personal finance, consumers, we all worry a lot about  
4 privacy and security and our data in particular  
5 settings. I studied together with my coauthor at the  
6 introduction of a, at the time, quite new  
7 technological service, which in early 2000s, was  
8 online banking. And the question is how do you  
9 actually want to start sharing information with  
10 consumers for the consumer's privacy and security.

11 Now, nowadays, online banking is something  
12 we're used to on an everyday basis. In the early  
13 2000s, it was not very much prevalent. I think there  
14 are lessons that we can learn toward the use of new  
15 technologies in today and in the future.

16 What is the underlying tradeoff? Well, of  
17 course, especially in this type of setting, consumers  
18 care about privacy and security verification hurdles  
19 to prevent others, third parties, to access their  
20 financial information and potentially execute  
21 transactions such as money transfers in these  
22 consumers' names.

23 But the other point is that consumers, and  
24 Avi briefly alluded to that, also care very much about  
25 ease of use or else they may not adopt the new

1 technological service, right? And, so, this is  
2 ultimately the tradeoff we worry about a lot, when we  
3 speak about privacy and technology adoption, and the  
4 question is what are actually the implications.

5 Now, in that particular study, in that  
6 particular empirical setting, what we observed is that  
7 because of privacy and security concerns, the bank  
8 implemented multiple hurdles for a consumer to use the  
9 service, starting with requiring a paper-based signup,  
10 then sending to the consumer login information that  
11 allows the consumer to use the service in terms of  
12 gathering information but not actually executing  
13 transaction to the latter, an additional piece of  
14 information, transaction numbers were required.

15 And, so, if what we have ultimately in  
16 this type of setting and more generally it's a  
17 multistage adoption process where the consumer goes  
18 through the hurdles of signing up, logging in, doing a  
19 transaction and potentially substantive over a time  
20 repeat usage, given these hurdles that were  
21 implemented in order to protect consumer privacy and  
22 security, what we have here is that actually since the  
23 consumer had to go through all these steps, it  
24 introduced substantial delays in the process

25 And what we find is that delays that come

1 here through this problem were exogenous shifters. It  
2 actually reduces at any point in time the probability  
3 a consumer would go to the next stage, say from  
4 logging in, actually doing first transactions.

5           And these effects are significant. So for  
6 example, more than a third of consumers would not log  
7 in in the month of sign-up; about a third of consumers  
8 would not actually do -- initiate a transaction in the  
9 month of their first log-in. And so you can see what  
10 the knock-on effect of those are both for consumers  
11 who now do not use a service that is intended to make  
12 their life easier perhaps or be more efficient in  
13 actually handling and transferring their money,  
14 keeping a certain balance in their banking account,  
15 and on the other hand for firms who still needed to  
16 deal a lot more with paper-based transactions.

17           And, so, to wrap this short summary up, the  
18 key insight here is that, well, complex security  
19 protocols that you might want to set up to ensure  
20 privacy and security are very personal, important  
21 pieces of information that might on the other hand  
22 actually reduce adoption. And to the extent that we  
23 think adoption of new technologies and innovations are  
24 good for consumers and maybe for the economy more  
25 broadly, that raises a question about where the

1 balance would be and what could be done to eliminate  
2 these frustrations by consumers while at the same  
3 point in time encouraging adoptions.

4 And, so, the key point, therefore, is  
5 whether efforts that we have to ensure online data  
6 security and the privacy can, therefore, have and how  
7 they can have unintended consequences for the  
8 diffusion of new anonymitive services. And I think  
9 any discussion of these questions will need to  
10 consider such unintended consequences. Thank you.

11 MS. MILLER: So what I'd like to do with  
12 these remarks is to talk a little bit about some  
13 empirical research that I've done focusing on the area  
14 of health privacy and looking at the effects of  
15 different privacy regulations related to healthcare  
16 data. And I focus on health in my research, health  
17 privacy in particular, because health is an area where  
18 we have sensitive information, the privacy issues can  
19 be really important, the data can be persistent. And  
20 also it's an area where in the United States there's  
21 been the most regulatory activity on the part of  
22 states.

23 So the first paper I want to talk about  
24 looked at the effect of regulation that was targeting  
25 one aspect of data privacy which is data security.

1 It's about controlling information and making sure  
2 it's not being used in ways that are not intended.  
3 And specifically what we did was we looked at what  
4 happens when states passed laws that were encouraging  
5 data security practices and they were trying to  
6 encourage firms to use, to adopt encryption technology  
7 and encrypt their data.

8           What we found is that when states had these  
9 encryption exemptions in their data privacy rules that  
10 basically promoted encryption, we find that more  
11 hospitals adopted encryption and data loss went up.  
12 Why is that? Human error. So what happened was the  
13 technology, the policy was pushing a technology;  
14 people -- firms responded by adopting the technology,  
15 but it didn't achieve the policy goal.

16           And I think that the theme there that I want  
17 to kind of draw out from this research that I'll come  
18 to again is that when we think about designing our  
19 policies, we want to think about the goal and we want  
20 to think about the details of how we get there. And,  
21 so, focusing on a particular technology, especially in  
22 a sphere where technology is evolving, can often lead  
23 to weaker effects than we expect or even reverse or  
24 perverse effects.

25           That theme is going to come up on the second

1 paper I want to tell you about, which was a paper that  
2 looked at the efforts -- some policy efforts that were  
3 made to encourage the adoption of health IT as part of  
4 the HITECH Act. And specifically the goal, one of the  
5 goals, was to try to encourage hospitals to exchange  
6 health information about patients. The policy lever  
7 that was applied in trying to achieve this goal was  
8 promoting a technological capacity on the part of the  
9 hospitals. So they had to show that they had the  
10 technology to be able to share data and to exchange  
11 data, and that it could be interoperable with other  
12 systems.

13 What we find -- so what we find in our  
14 research is that the focus on technology again was not  
15 sufficient. We find in our research that hospitals  
16 that were part of big hospital systems with lots of  
17 hospitals in them were actually more likely to  
18 exchange data with other hospitals. They were more  
19 likely to have the capacity to exchange data, but they  
20 exchanged data internally with other hospitals in  
21 their system.

22 What they didn't do or what they were much  
23 less likely to do was to share data outside of their  
24 system, okay. And, so, the reason for that is that  
25 they didn't necessarily have a business incentive to

1 want to share the data, right? The hospital is  
2 producing this information. They are creating medical  
3 records, they're collecting information, they're  
4 storing it and they are not necessarily going to want  
5 to give it away freely to their competitors, to other  
6 hospitals in their local area, even if there is a  
7 policy benefit or a public benefit for that.

8           And, so, what we have is this creation of  
9 information silos; by focusing on technology we didn't  
10 prevent that. So this echoes, again, the first theme  
11 about thinking about how we design our specific  
12 interventions and how that's important. The second  
13 theme I think is even broader, which is it relates to  
14 this question of how do we think about data, health  
15 data about individuals, but actually consumer data or  
16 individual data more broadly, okay.

17           And this question about ownership, I think,  
18 is a little bit new and special here. The fact is  
19 that companies or businesses or organizations are  
20 creating data. They are collecting data. It's their  
21 data. They might think they own it, but it's data  
22 about people. And, so, people might think that they  
23 have some ownership, and it's actually ambiguous who  
24 should own the data and even who does own the data.

25           And I think this ambiguity about property

1 rights and about even what there should be is an area  
2 of concern and an area that leads, I think, to some  
3 potential inefficiencies. It also means that when we  
4 think about privacy policy there's not a clear binary  
5 on/off of do we protect privacy or not, but there's --  
6 or how much do we protect along a single linear  
7 dimension, but there's questions about what aspect of  
8 privacy are we targeting. Are we talking about the  
9 ability to collect it, to store it, to exchange it, or  
10 to use it. Are we talking about users' rights to  
11 access their own information.

12 So the third paper that I want to tell you  
13 about, this third research paper also in healthcare,  
14 looks at variation in policies, in privacy policies  
15 that actually took different approaches, all to  
16 address the same common issue of genetic privacy. So  
17 different states took different approaches to  
18 protecting genetic information, and what we look at in  
19 our research is how these different approaches affect  
20 the rates at which individuals were willing to get  
21 genetic tests to predict their cancer risks. So this  
22 can be very sensitive information; you think privacy  
23 protection could be important.

24 What we find here is that the type of the  
25 protection actually makes a big difference and that

1 the different forms of protection had completely  
2 different effects. So a policy approach that focused  
3 on informed consent and letting individuals know about  
4 exactly who had the property rights and how that  
5 information was going to be used and about their  
6 privacy concerns actually had a significant effect of  
7 lowering rates of testing. When the privacy laws  
8 instead emphasized or required a, required permission  
9 from consumers for their own data to be redisclosed or  
10 sent to a third party, so it gave the individual more  
11 ownership, that actually promoted adoption.

12 A third approach that's actually the most  
13 common approach used in privacy protection for genetic  
14 information is a focus on how the data can be used.  
15 And, so, rules like that that limit the ability of  
16 employers or insurers to use genetic information in  
17 terms of pricing or market interactions actually had  
18 no effect on adoption. So these antidiscrimination  
19 laws that focus on the use of data were not effective.

20 There are various reasons for these effects,  
21 and maybe we'll have time to talk about it more in the  
22 Q&A, but I'm running out of time, so I want to say  
23 that, right, so that this, again, I think, highlights  
24 this theme earlier about the details of the policy  
25 making a big difference. And even policies that

1 almost sound like they're the same thing, a genetic  
2 privacy law can actually have opposite effects  
3 depending on the particulars of how it's specified.

4           Okay, so to summarize, I want to just relate  
5 this to the two topics of the panel. First of all, as  
6 we relate to competition policy, I think the research  
7 we found with the creation of data silos in big  
8 hospital systems emphasizes the important concerns  
9 that we should have about big data and the potential  
10 to lock in consumers and how this does create  
11 potentially a competitive advantage for bigger firms  
12 and make it harder for incumbents -- sorry, make it  
13 harder for entrants and small firms to compete. And  
14 it relates to the exchange of information.

15           Second point is that when we think about  
16 innovation policy, all of these papers that I've  
17 talked about and some that I haven't had a chance to  
18 talk about but that Avi and Anja have talked about, I  
19 think all show that there is a real connection between  
20 privacy, regulation, and future innovation, and in  
21 many ways, privacy policy is innovation policy in  
22 healthcare and elsewhere.

23           MR. GILMAN Thank you.

24           MR. STRAHILEVITZ: Great. Hi, thanks. So  
25 I've titled this "Confessions of a Convert," and I'll

1 explain that, which is that I've been writing about  
2 policy for 16 years and often find myself at  
3 conferences of privacy law scholars, all of who favor  
4 a much more aggressive privacy regulation, and I've  
5 been one of the few people to say, oh, let's apply the  
6 brakes, let's think about the tradeoffs involved. So  
7 I'll talk you through about a decade's worth of  
8 research and how I got to where I am now. So exactly  
9 a decade ago, I started thinking about ways in which  
10 the proliferation of reputation information about  
11 individuals was providing all kinds of opportunities  
12 for law and legal systems.

13           Yelp and regulation of the medical  
14 profession by the AMA are substitutes for one another,  
15 and in a lot of respects, the kinds of information  
16 that's generated by services like Yelp or TripAdvisor  
17 provides a really nice substitute for government  
18 inspectors and those sorts of mechanisms in making  
19 sure that consumers are getting their money's worth  
20 and that firms are behaving appropriately.

21           About half a decade ago, I started thinking  
22 about the political economy of privacy, why  
23 differences arise, especially between the United  
24 States and Europe, which have only become more  
25 pronounced since then, and tried to emphasize that

1 privacy regulations create winners and losers and that  
2 we can predict who they will be, that sometimes the  
3 impacts of privacy regulations are often regressive.

4           And then just a couple years ago, I started  
5 to think empirically about research. This is actually  
6 a 2016 paper rather than a 2014 one. But in any  
7 event, what we tried to do was make some progress on  
8 one of the chief topics for this panel today, which is  
9 to figure out, well, why aren't markets developing.  
10 We spent a lot of time looking at the use of automated  
11 content analysis with consumers' emails for the  
12 purposes of serving them with personalized  
13 advertisements.

14           We asked consumers -- a nationally  
15 representative sample of them -- how invasive do you  
16 regard these sorts of practices where gmail is looking  
17 at the contents of your emails and giving you  
18 personalized ads, and they said quite invasive -- 7.63  
19 was the mean response on a scale of 1 to 10. And at  
20 the same time, we said, well, would you be willing to  
21 pay any amount of money to avoid it. No was the  
22 response of about two-thirds of the sample. And  
23 that's another example of the privacy paradox that's  
24 been mentioned in some of the other research.

25           Among those who were willing to pay the

1 median willingness to pay stated in surveys, so not a  
2 revealed preference, which was \$15 per year and  
3 looking at how much consumers said this data was worth  
4 to them versus how much we know it's worth to Google  
5 or Facebook or Yahoo. We think that probably those  
6 platforms value it more than the individual consumers  
7 do, at least with respect to personalized ads based on  
8 email contact.

9           So that's sort of what I've been working on  
10 and how I arrived here today, and I do want to stick  
11 by some earlier views that I've articulated, which is  
12 that there's still lots of reasons to think that the  
13 U.S. has done quite well by having a relatively  
14 permissive environment, that we've seen a lot of  
15 innovation, that there are technologies that have  
16 developed in the United States that couldn't have  
17 developed in Europe because people would have needed  
18 permission to do -- to develop the kinds of  
19 applications that have proved to be so successful,  
20 both -- successful both here and there.

21           But at the same time, there seemed to be  
22 real breakdowns in the self-regulatory model in  
23 laissez-faire approach. One of these breakdowns is  
24 that consumers often don't know about all the problems  
25 that can arise, whether it's on a data security side

1 or on a privacy side with robust journalistic efforts,  
2 with robust enforcement by the FTC. Consumers can  
3 find out and make informed decisions. It's not clear  
4 that adequate resources are being developed to  
5 identify privacy snafues or data security snafues by  
6 either of those institutions.

7 And the proof is in the pudding, to some  
8 extent, which is to say that if you ask Americans as  
9 Reuters did a few months ago, whether they trust  
10 Facebook to obey the laws that protect their personal  
11 view -- protect their personal info, the majority will  
12 say, no, we don't trust Facebook, even though Facebook  
13 has a very, very strong financial incentive in getting  
14 people to yes on that question. And some of the other  
15 technology companies with probably better records  
16 generate majority saying that we trust you but not  
17 anywhere near supermajorities.

18 Okay. So as we think about privacy from  
19 where we are in 2018, I think we can talk about some  
20 of the fundamental ways in which the world's looking  
21 worse for privacy and the laissez-faire approach than  
22 it was ten years ago. Jane talked about Cambridge  
23 Analytica. Hopefully we'll be able to talk about that  
24 during the Q&A.

25 I probably think there are things we can all

1 agree about that Cambridge Analytica did wrong. Most  
2 prominently, I should have the right to reveal or not  
3 reveal personal information about myself. And I  
4 didn't choose to delegate that to the 800 friends I  
5 have on Facebook. And when Facebook organized their  
6 API such that any of 800 people could choose to reveal  
7 a lot of information about me that was potentially  
8 sensitive, that strikes me as a technological  
9 breakdown, one that potentially lends itself to  
10 regulation.

11 We're seeing especially in the last election  
12 cycle, in the last couple of years, doxing, instances  
13 of online harassment, online trolling that's really  
14 off the charts. And I think it's scaring off the  
15 sensible center from a lot of political discourse,  
16 scaring off women, scaring off people of color, really  
17 compromising fundamental values that are bedrocks of  
18 American and democratic societies.

19 More generally, think about how often you  
20 answer your cell phone now versus how often if it's an  
21 unrecognized number you just let it ring and go to  
22 voicemail. Lots and lots of people as a result of  
23 breakdowns in do not call and flagrant violations of  
24 do not call, lots of people have stopped answering  
25 phones. Think about the cost of that. Those costs

1 are real, and they're felt by consumers, they're felt  
2 by people trying to make phone calls.

3 And we can look overseas and see some of the  
4 things that's happening with social credit scoring in  
5 China and be really worried about some of the  
6 potential for abuses with these kinds of technologies.

7 So just in the minute I've got left, let me  
8 identify a couple of issues. The first, which I think  
9 we'll talk about on the next panel, is there's lots of  
10 inconsistencies between GDPR and the American  
11 approach. The world is going with the European  
12 approach, not with the American approach. That makes  
13 -- that causes real problems for American companies  
14 and for the free flow data across the Atlantic or  
15 across the Pacific, between North America and Latin  
16 America.

17 So one idea that harkens back to work by  
18 Victor Mayer-Schonberger in his 2009 book Delete,  
19 which formed the basis for the European right to be  
20 forgotten, turns out, I think, to have some modern  
21 adaptations, which is here's a proposal for deletion  
22 by default, okay. The main problem with the right to  
23 be forgotten is currently implemented by the European  
24 Union is that it's unconstitutional under their First  
25 Amendment law.

1           There are ways to accomplish the same kinds  
2 of objectives without running aground of any  
3 constitutional problems, and deletion by default,  
4 which is certain data should automatically be deleted  
5 by let's say ten years after it's collected, purchase  
6 history information, Facebook posts, et cetera, and  
7 people could always choose to opt out of that, which  
8 is, I think, both constitutionally permissible under  
9 the U.S. regime, and also probably better.

10           So Google puts out really useful data about  
11 how often people are actually exercising the right to  
12 be forgotten, and it turns out that the rate of  
13 utilization is about 0.15 percent of European  
14 residents have exercised their rights under the right  
15 to be forgotten under a generous interpretation of  
16 data from the Google transparency report.

17           So as we think about, well, what are the  
18 kinds of purposes that are vindicated by the right to  
19 be forgotten, the right to be forgotten, as employed,  
20 which puts the onus on the consumer to delete  
21 information, isn't working. Something like deletion  
22 by default would work much better and it's an approach  
23 worth considering. Thanks.

24           MR. COOPER: Mr. Telang.

25           MR. TELANG: I'll try to be quick so that we

1 have opportunities for others to chime in as well. My  
2 name is Rahul Telang. I'm a Professor at Carnegie  
3 Mellon University. I'll pick up from where Lior left.  
4 I'm not as pessimistic, I think, as maybe he is about  
5 the power of markets and competition in solving some  
6 other problems, but let me just highlight and maybe we  
7 all agree with this. But in an ideal world really  
8 what we want to know is where exactly is the friction.  
9 Rather than thinking about what regulations will work,  
10 we want to probably sit back and ask, well, what  
11 exactly is the friction that people face when they're  
12 dealing with the customer data, or of our own data and  
13 firms that are utilizing that information.

14 You know, think of that as essentially an  
15 externality problem, that firm has my data, they are  
16 somehow misusing it, or extracting too much rent out  
17 of it than I would like them to do it, and that's the  
18 externality they're imposing on me. And the question  
19 is that how can we push that externality back onto the  
20 firms.

21 Maybe I'm misquoting, but, you know,  
22 generally the FTC has looked at this as a problem of  
23 can we make information available to consumers so that  
24 they can make better informed decisions, more or less  
25 without imposing too much regulation, and I think

1 that's what Lior also sort of mentioned. And I'll  
2 come back and talk a little bit about where we stand,  
3 but then the idea is that, well, this should lead to  
4 across-the-board innovation, both on the demand side  
5 and actually at the supply side, right? I mean, if  
6 you want a whole lot of privacy, then there should be  
7 some firms available who are willing to provide that  
8 privacy, maybe not at the firm level but maybe at the  
9 intermediate level.

10           Maybe you will use a certain browser with  
11 certain features in it that'll make sure that Facebook  
12 might or might not be able to collect your data.  
13 Maybe you're not able to do it, but at some level, the  
14 idea is that -- both that there is going to be a  
15 demand for privacy security, whatever you want to name  
16 it, but then also there is a potential possibility of  
17 supply for privacy security.

18           And, you know, I guess the question maybe  
19 some of us believe that this model can never work,  
20 maybe some of us might believe that at least partially  
21 this model can work. I mean, fundamentally, this  
22 problem maybe just comes down to whether security and  
23 privacy can be a feature that the firm can advertise,  
24 and it doesn't have to be that whether we are willing  
25 to pay for it monetarily. There are some other ways

1 people are willing to pay, including market share,  
2 transactions, how long we want to have a relationship  
3 with the firm, so on and so forth, or whether it is  
4 just a bug that we are worried about and then  
5 everybody's trying to figure out a way to undermine  
6 that.

7 In some aspect, the evidence is not  
8 completely negative. And, in fact, if you think about  
9 it, you know, maybe the data breach notification law  
10 would be a good example where, you know, it forced a  
11 fair amount of disclosure, at least on the parts of  
12 the firm. And if you look at it, we are holding a lot  
13 of firms actually accountable, even if not the firms  
14 directly, we do punish the executives.

15 I mean, Equifax CEO had to resign because  
16 there was a data breach. Mark Zuckerberg did have to  
17 come in front of the Congress and actually provide  
18 some details and, you know, at least some  
19 embarrassment, Wall Street Journal reporting and the  
20 New York Times press, which probably none of them they  
21 would like. So there is a little bit of externality  
22 that we are pushing back on the firm without any, you  
23 know, serious regulation on what you can do with my  
24 data or what you cannot do with the data. But at  
25 least in terms of making it clear to people that,

1 look, these people might or might not be abusing of  
2 our data.

3 And there is really no impact, no way for us  
4 to empirically measure whether things have gotten  
5 worse or better, but there is at least some evidence  
6 that maybe firms are being elastic to some of those  
7 changes in terms of how they are storing of our data,  
8 how they are sharing of our data, so on and so forth.

9 I think, you know, one other point is that  
10 sometimes we talk about, you know, when we're  
11 designing policy, can you share the data, should we  
12 stop the data, sharing between firms or data abuse. I  
13 think at some level you will also think of maybe there  
14 is certain part of the data that is off limits and  
15 maybe there is some other part of the data that it  
16 perfectly might satisfy the firm.

17 So, I mean, think about online  
18 advertisement. Sure, some targeting is very  
19 effective. We need some data for the targeting to be  
20 very effective, but maybe there is a whole lot of  
21 information that the firm uses that's really not that  
22 effective, or they can find proxy for that and be able  
23 to be reasonably effective without knowing my Social  
24 Security number or name or what have you, and some  
25 other proxies might work, too. So it doesn't have to

1 be always a zero sum game.

2 One more point. One more point I want to  
3 highlight is that it's also we have to remember  
4 sometimes that sometimes it's the uncertainty in  
5 regulation that actually can hurt innovation more than  
6 the regulation itself sometimes. Again, if you go  
7 back, when the data breach notification laws came,  
8 everybody complained about it, so much compliance is  
9 happening, so much compliance costs are happening. I  
10 don't think anybody complains about it. In fact, a  
11 firm says, you know, instead of 50 different states, I  
12 would rather have one national law so that, you know,  
13 I can kind of get over with some of the -- or lower my  
14 compliance cost. Nobody is saying that we shouldn't  
15 be having those laws.

16 And, in fact, if you think about it, there  
17 are second-order and third-order benefits to sometimes  
18 these regulations. For example, if you talk to cyber  
19 insurance policymaker, they will -- everybody would  
20 agree that actually the data breach notification laws  
21 led to so much cyber policy being written to provide  
22 insurance against data breaches because some of those  
23 regulations actually provided some certainty about  
24 what the cost would be, what the floor would be, what  
25 the ceiling would be. And that led to, you know, some

1 of the significant growth in cyber insurance, which  
2 also then creates good practices and what have you.  
3 So there are these secondary and tertiary benefits  
4 sometimes with regulations, you know, lack of  
5 uncertainty can help, but it is a lot of work, not  
6 just in the privacy space, but automobile space,  
7 health space, environment protection space, which  
8 seems to argue that if you reduce the uncertainty and  
9 stop sending unclear signals to the industry actually  
10 it can be very helpful.

11 Again go back, the automobile industry  
12 bitterly opposed the seatbelt and the air bag. And  
13 once those regulations actually came in, they figured  
14 out a way to actually live with it, not only live with  
15 that, actually innovate where all of us benefitted,  
16 the consumers and the safety, but they also were able  
17 to sell it as a feature where they were able to  
18 actually price them out.

19 Something to think about where we think  
20 about regulation that sometimes having some certainty  
21 can be actually much more useful than sometimes just  
22 arguing about what the regulation and the content of  
23 the regulation should be. So I'll stop here.

24 MR. COOPER: Okay, terrific. I guess I'd  
25 like to start really with a question for the entire

1 panel. We've had -- I'm sort of reminded, we've had  
2 some really excellent research-based panels. We are a  
3 research-based agency. We do research-based law  
4 enforcement on both the competition and the consumer  
5 protection side. We do research-based policy work,  
6 but I'm thinking of various threads that have come up  
7 over the two days that have reminded me of an outdated  
8 and terribly unfair label for economics as the dismal  
9 science.

10 So what do I have in mind here? There's  
11 quite a bit of research on certainly market  
12 imperfections, whether or not they're durable market  
13 failures, people might debate, so very high  
14 information costs, very high maybe information  
15 asymmetries when it comes to privacy issues, both  
16 between firms and consumers, folks like we're sitting  
17 up here, and indeed between firms as vendors and firms  
18 as consumers.

19 Certainly, there's evidence of people  
20 suffering these kinds of information privacy-related  
21 harms, ranging from identity theft to any manner of  
22 other things. We've had some very interesting and I  
23 think useful and important research on some of the  
24 limits of intervention in this space, right.

25 So first competition issues surrounding

1 privacy interventions, which may not always but may  
2 tend to favor large firms and incumbent firms at the  
3 expense of smaller firms or entrants. Certainly,  
4 unanticipated effects from privacy regulations, which  
5 sometimes I'm thinking of some of Professor Miller's  
6 research, say with Catherine Tucker, just health  
7 effects that weren't anticipated with IT regulations.  
8 One thing, or even, you know, you get -- you flip the  
9 sign of your anticipated effect as with some of the  
10 data security regulations. It doesn't mean that all  
11 data security regulations will have these effects, but  
12 it's certainly not a positive result.

13           And, so, I guess one thing is sort of just a  
14 question going down the line. It seems that there is  
15 maybe some pertinent research, but quite a bit less  
16 that answers the policy question, what do consumers  
17 win with one or another privacy or data regulation  
18 intervention.

19           Plainly, consumers have concerns in this  
20 space. I don't think anybody would deny that, but one  
21 question is, do we have an adequate research basis for  
22 saying, first of all, that these interventions will  
23 actually be effective, whether in one silo or another  
24 or across large sectors of the economy; and, second,  
25 you know, an adequate way of assessing consumer

1 benefits, right?

2 So we have costs when we fail to intervene;  
3 we have costs when we intervene. Have we developed a  
4 good science of assessing and then actually achieving  
5 concrete benefits. Anyone? We'll go down this way  
6 unless someone wants to pass.

7 MS. BAMBAUER: So I agree that we have very  
8 good research on some narrow questions. I continue,  
9 though, to -- and I'm basically restating what my  
10 opening comments were, that I continue to be concerned  
11 that we haven't even really defined the harms well  
12 enough to then know how to measure them. And that's  
13 really sort of more of a philosophical question than  
14 even an empirical one.

15 And so without it, though, the foundation  
16 for doing the empirical research that we would need to  
17 do is lacking. So, yes, I'm concerned that we don't  
18 have enough of an evidence base quite yet.

19 MR. GOLDFARB: So if we're weren't the  
20 dismal -- we're looking for some kind of Pareto-  
21 optimal solution where everyone -- there's a market  
22 failure where everyone would be better off because we  
23 have a regulation. And that -- it doesn't happen  
24 enough. Maybe credit scoring and the Fair Credit  
25 Reporting Act was a privacy regulation that was

1 Pareto-improving but -- and in some sense we've been  
2 looking for that in the privacy space for 20 years.

3 It's not obvious that such a thing happens.  
4 It seems pretty clear that the empirical work says  
5 there's a tradeoff. There's a tradeoff between, you  
6 know, more privacy might mean less innovation; it  
7 might mean less competition. I have some other work  
8 that suggests it might mean more inequality but that  
9 doesn't mean that it's a bad thing. We've also heard  
10 a whole bunch of reasons why privacy is good.

11 And, so -- you know, and you said, you  
12 know, this regulation's not effective. In some sense,  
13 a lot of the regulations have been extraordinary  
14 effective. If the goal was to restrict data flows,  
15 the regulations restrict data flows. They do exactly  
16 what they were supposed to do. That just means that  
17 ads become less effective or healthcare doesn't work  
18 as well. But they are effective in terms of their  
19 explicit goals on restricting data flows.

20 So I just think it's important to realize  
21 there's tradeoffs here. These are hard decisions.  
22 And in some sense the empirical work -- like, as an  
23 economist, I don't -- certainly I don't feel like I  
24 have the skills to tell you about those tradeoffs.  
25 What I can say is what those -- you know, I can really

1 lay out well is what those tradeoffs are.

2 MS. LAMBRECHT: Okay, so two points on that.  
3 I think one interesting point is that the perception  
4 of privacy changes. You know, what we regard today as  
5 privacy-relevant or what was regarded 20 or 50 years  
6 ago as privacy-relevant or sensitive information may  
7 not be regarded as such anymore today. at least not  
8 all of it. And if I look at my younger students, they  
9 might still have a different perception of which data  
10 are, you know, privacy-sensitive than I have.

11 So I think one aspect is that  
12 desensitivities and they're of the trade -- therefore,  
13 the tradeoffs also change over time. And I think this  
14 is just one point to keep in the back of our mind as  
15 we are trying to think about policies.

16 The second point is that I do believe that  
17 these tradeoffs are highly context-dependent, and the  
18 harms and the benefits are very context-dependent.  
19 And I know similar to what Avi said, I think it's very  
20 hard to lay out the overall, overarching framework for  
21 how these tradeoffs should be sold.

22 So think, for example, a retailer that holds  
23 information about your browsing behavior. We had the  
24 example of Target earlier, but think about this  
25 happening online, and using it in a way that one

1 consumer feels as privacy-invading. On the other  
2 hand, the retailer might also use that information to  
3 structure information displayed on -- in response to  
4 product searches on their website, which may have --  
5 for consequences of the consumer gets better selection  
6 of product, a better choice, makes a better choice and  
7 may spend less time on making those choices.

8 And, so, this is what I mean with context-  
9 dependent. There are settings where the harms may  
10 more obviously -- or that the benefits may more  
11 obviously outweigh the harms, and maybe other settings  
12 where the harms may play out in very different ways,  
13 way outside the specific context, for example, in  
14 online advertising.

15 MS. MILLER: So I think these are the tough  
16 questions. A few thoughts. One thing in thinking  
17 about the costs and benefits of privacy protection, I  
18 think it's always helpful for me to step back and  
19 think about the costs and benefits of privacy itself  
20 and then think about the privacy regulation.

21 I think that, you know, some of the results  
22 that we find of privacy regulation leading to less  
23 adoption of technology could actually reflect an  
24 underlying latent benefit or need for that regulation.  
25 So to the extent that informing consumers about

1 privacy risks makes them less likely to do something  
2 that entails a privacy risk, it's not obvious that  
3 that's inefficient. It could be that they were  
4 inefficiently unaware of privacy risks or that it  
5 wasn't salient to them.

6 And so I think that there's sort of a  
7 question of how much are we -- there's a question --  
8 there's tradeoffs involved in the privacy policy, and  
9 I think also the point Avi made earlier is important  
10 that no privacy protection is also going to be a  
11 problem. So when we think about the costs and  
12 benefits of privacy protection policy, one of the big  
13 costs we want to think about from not protecting  
14 privacy is all of the privacy-protecting activities  
15 that individuals will engage in in the absence of  
16 regulation that protects them.

17 So if they don't feel that their data are  
18 safe, they may not download apps on their phone. They  
19 may not do different kinds of things. They may shut  
20 off Facebook or never post their child online because  
21 they don't feel that that privacy is protected. And,  
22 so, we think about those potential benefits from  
23 privacy protection. We want to take those into  
24 account.

25 At the same time, you know, my own research

1 and research by others does show that sometimes  
2 regulation, well intended, can have real harms in  
3 terms of slowing the diffusion of technologies. I  
4 didn't talk about this paper, but this other research  
5 I did with Catherine Tucker looked at privacy laws  
6 protecting health privacy led to less adoption of  
7 electronic medical records in U.S. hospitals. And  
8 then we show in another paper that this actually --  
9 this slower adoption led to greater mortality, greater  
10 infant mortality because this technology itself was  
11 saving infants' lives.

12 And, so, there are, you know, real  
13 substantial costs to not protecting privacy but also  
14 to not having these technological innovations in  
15 healthcare and other spheres.

16 I just kind of want to give some, another  
17 point about just the very pessimistic results that I  
18 have about I think the tradeoffs are real and I think  
19 they're important to consider, but I don't want the  
20 message to be -- so I think the message should be that  
21 we should be cautious and the details matter and there  
22 are a lot of ways we can go wrong. But I don't want  
23 the message to be that that's an excuse for inaction  
24 or for just throwing our hands up and not trying.

25 I think what it means is that we should have

1 modest expectations. We should put in some effort  
2 before we make rules and to try to look at the  
3 research, try to experiment, try things on a smaller  
4 scale, maybe where the impact is not going to be so  
5 bad if we get it wrong. And try things. And then,  
6 you know, be flexible.

7           If we have a policy, let's monitor and let's  
8 see if it's working or if it's not working, and if it  
9 isn't, let's change it. So I don't think that it's  
10 something that we sit down and, you know, in a room  
11 devise the optimal solutions, you know, QED X star,  
12 and we go with that. I think we just want to be aware  
13 of the issues and then actively, continuously try to  
14 work on that.

15           MR. STRAHILEVITZ: I think I agree with  
16 what's been said. It's hard to do cost-benefit  
17 analysis for privacy because privacy harms are and  
18 always have been hard to quantify. Okay, so let's  
19 start with that, but that doesn't mean that when we're  
20 trying to do something like cost-benefit analysis we  
21 have to throw our hands up in the air.

22           So one thing that you can try and do is look  
23 around you and think about whether the ways in which  
24 the legal system deals with privacy are typical or  
25 exceptional. And, so, I want to provide two lenses

1 from doing that. One way you can do that is by  
2 looking at how privacy gets treated versus how other  
3 kinds of big goofs get treated. All right, so one  
4 thing that's really unusual about the way that privacy  
5 is regulated by the Federal Trade Commission is that  
6 the Federal Trade Commission does not start out with  
7 fining authority for big privacy goofs. And, so, when  
8 I explain to laypeople that it's only because Facebook  
9 had previously entered into a consent decree with the  
10 FTC that the FTC has the ability to impose monetary  
11 fines as a result of Cambridge Analytica. They're  
12 very surprised by that. You're probably not surprised  
13 by that, but people you talk to who are not lawyers,  
14 regulators, policy people are probably extremely  
15 surprised.

16 And, indeed, that makes the United States  
17 exceptional when compared to the way that other  
18 countries deal with privacy and also other parts of  
19 the U.S. regulatory system deal with big goofs, right?  
20 So when Ford Pintos started exploding, right, because  
21 of faulty gas tanks, we didn't say, okay, Ford, you  
22 know, if you make another car that starts exploding,  
23 we will fine you for that but, you know, you get one  
24 free goof. This was a badly designed car, you're off  
25 the hook, right?

1           We kind of have that response with respect  
2 to privacy, at least from a federal regulatory  
3 perspective. There's other things that will happen,  
4 like class action lawsuits that Facebook will be  
5 dealing with. They'll lose some consumers. I'm not  
6 suggesting that they face no repercussions, but it is  
7 a little bit unusual how we treat privacy vis-a-vis  
8 other kinds of products or other kinds of interests  
9 and how the U.S. treats privacy versus the way the  
10 rest of the developed world treats privacy. And I  
11 think that can be informative in terms of how we  
12 should think about what the right approach is.

13           MR. TELANG: The generic takeaway is it's  
14 hard to say anything simply because -- is there a  
15 generic takeaway that we can take, you know, from all  
16 the research and the meta research? It's hard because  
17 it's a very heterogenous problem. I think one thing  
18 that I feel we can take away is that, you know,  
19 consumers are really good at compartmentalizing, that  
20 they -- for us, the transaction costs are very high.

21           Even reading one line every time we transact  
22 with a website is just too costly for us. However,  
23 you know, there's some research that I'm working on  
24 and one of the challenges of privacy research at some  
25 level is that if you go survey-based then you're

1 always, you know, overestimating everything, because  
2 if you ask people, and I think people already in the  
3 last panel talked about the variance between survey  
4 and behavior is so large that you wonder what you can  
5 glean. Plus there is a long-term issue, too, but,  
6 anyway, we are actually working with the actual  
7 transaction. We're working with a very large bank  
8 which has very detailed information on how people  
9 transact. And one of the things that we clearly  
10 notice that people care if something goes wrong with  
11 their financial -- that is, if something goes wrong  
12 with the credit card, with the bank, with something  
13 that has direct money involved, they are a lot more  
14 careful. They're a lot more willing to punish the  
15 firm if it's going to have -- if a fraud is going to  
16 happen on your bank or your credit card account, and  
17 we can see that in the data.

18 On the other hand, if Home Depot loses your  
19 data or if Target loses your data, we are a lot less  
20 willing to punish them. Our transaction behavior  
21 doesn't change a whole lot maybe because we think  
22 that, well, Lowe's isn't going to be any better.  
23 Maybe we think that the financial cost is really not  
24 very high, the credit card is going to pick it up,  
25 I'll get a new credit card, I really don't want to

1 kind of go through all the hassle.

2 So I feel like it's very context-dependent.

3 If I feel that I'm going to incur a significant

4 financial harm, I think people really take action.

5 And if they feel that, well, the financial harm is

6 secondary, tertiary, might harm happen sometimes in

7 the future, might not happen at all? I think they

8 tend to kind of ignore many of the privacy red lights,

9 if you would, in that regard.

10 MS. BAMBAUER: So I just wanted to add one

11 thing. I think it might be useful to distinguish the

12 intrinsic value of privacy that people might want

13 control over the access to their data and the ultimate

14 use of their data from the downstream harms that

15 privacy might protect. And I find that if we identify

16 the downstream harms then we can try to measure them,

17 and that gives us a lot better of a chance, I think,

18 to do this tradeoff.

19 But with the intrinsic value of privacy, you

20 know, like I don't quite know what a privacy goof, for

21 example, is. I know that when a Pinto explodes,

22 nobody wants to be in that Pinto, but -- and everyone

23 basically ascribes roughly the same value to, you

24 know, to their health and life and also their money,

25 but the intrinsic value of privacy is not clear to me,

1 and I think Ginger Jin mentioned yesterday that a  
2 problem in this area is that preferences -- to the  
3 extent they can be measured at all -- are widely  
4 varying. They are time-dependent. They are dependent  
5 on so many things that I don't even know if it's  
6 useful to think about intrinsic values, and maybe we  
7 should be looking at the downstream.

8 MR. COOPER: So thank you. Interesting  
9 conditions under which someone does want to be in a  
10 Pinto, but so, you know, we've heard a lot, I think,  
11 here about context, and maybe it's not surprising that  
12 people have done very fruitful research in specific  
13 contexts, specific industries, specific technologies,  
14 right, whether we're talking finance, consumer credit,  
15 healthcare, different research on healthcare systems'  
16 adoption versus other issues in healthcare.

17 I mean, maybe in some ways, I mean, to pick  
18 up on something that was mentioned about FTC, this is  
19 convenient for the FTC's approach to privacy, both on  
20 the competition side and the consumer protection side,  
21 right? We look at transactions, at mergers that may  
22 unduly burden competition and do harm to consumers.  
23 We have a framework for doing that, whether in the  
24 information economy or elsewhere.

25 On the consumer protection side with privacy

1 and data security enforcement we look for harms,  
2 right, specific harms, cognizable under the FTC Act or  
3 under special statutes and evidence for concrete harms  
4 and concrete context. And under unfairness harms that  
5 aren't offset, say by countervailing efficiencies.  
6 But I'm also wondering a little bit first it was  
7 mentioned, I think by Professor Strahilevitz -- maybe  
8 I just got it wrong -- but about our authority. Well,  
9 maybe two of you, conditions under which we can levy  
10 fines or pursue different remedies.

11 So one question I would ask is simply what  
12 adjustments might be recommended to our authority or  
13 not to improve our ability to address context-specific  
14 harms, whether on the competition side or on the  
15 consumer protection side. And then I guess second,  
16 sort of what's left out we don't do everything. Are  
17 we optimistic or pessimistic about extending some of  
18 this learning to calls for much more general,  
19 overarching privacy regulation, whether we're talking  
20 about, you know, compare and contrast, say, HIPAA with  
21 the GDPR approach or, you know, Fair Credit Reporting  
22 Act with the GDPR approach, federal, state, industry  
23 or overarching.

24 I guess both -- so two hard questions if we  
25 could just go down the panel and I guess -- I think

1 we've actually got eight minutes, but thank you, by  
2 the clock. We're scheduled to go until 4:00. No?  
3 That's what it says here. Okay. Well, sorry, if we  
4 could go briefly.

5 What was the question now?

6 MR. GILMAN: So FTC authority is one. Would  
7 you alter it based on any findings? Maybe that's  
8 enough.

9 MR. STRAHILEVITZ: I'll take a stab at it.  
10 So I think one thing that would be really useful for  
11 the FTC to think about are what are the kinds of  
12 problems that the courts have a hard time remedying  
13 and so, you know, a classic example is the data  
14 breach, okay? So courts really struggle with data  
15 breaches for the following reason. Let's suppose a  
16 whole bunch of data is breached. Let's suppose that  
17 every American faces a baseline risk every year of 2  
18 percent -- 2 percent chance they'll be victimized by  
19 identity theft, okay?

20 Now, let's suppose that the people whose  
21 data was breached face a 3 percent chance of identity  
22 theft. And let's say we're talking about tens of  
23 thousands or hundreds of thousands of people. We know  
24 that the breach was costly, very costly. We know that  
25 it elevated the risk for people in the relevant pool

1 by 50 percent, but courts are going to be looking for  
2 proof that a particular individual suffered identity  
3 theft, the classic harm in a data breach, as a result  
4 of this particular breach, okay?

5           You'll want to -- at least there's a circuit  
6 split in terms of dealing with these issues -- but  
7 you'll want -- in order to have an airtight ability to  
8 get first standing and then establish the causal  
9 nexus, you're growing to need to show a court that  
10 it's more probable than not that particular  
11 individuals suffered particular out-of-pocket harms,  
12 pecuniary harms, as a result of a beach. And I think  
13 courts have a hard time with those kind of cases.

14           That's not the standard model of how a court  
15 proceeds. The standard model of how a court proceeds  
16 is show me in a civil suit that it's more probable  
17 than not that your injury resulted from their mistake.  
18 So that's an area where we know statistically a lot of  
19 people are harmed, but we also know courts, Article  
20 III courts, are going to really struggle with it,  
21 where I think there's a lot of room for the FTC to do  
22 really good work because the FTC can litigate and  
23 enforce on behalf of the aggregate.

24           And it doesn't so much matter whether any  
25 individual happens to have been victimized because of

1 the baseline risk of identity theft or because of the  
2 elevated risk resulting from a particular breach.  
3 And, so, I think that when the FTC thinks about its  
4 authority it should think about, okay, what are class  
5 action lawyers doing and is any of that accomplishing  
6 any good. What is self-regulation doing and is any of  
7 that accomplishing any good? What are state attorneys  
8 general doing, and is any of that accomplishing any  
9 good? Okay, what are the thing they're bad at? Odds  
10 are good that those are things that the FTC can add  
11 the most value through.

12 MR. COOPER: Thank you. Apparently, we're  
13 also bad at time management, so I apologize for  
14 cutting this short. Thanks very much to our panelists  
15 for their contributions and thanks for your attention.  
16 We do not have a break here. We're going to shift  
17 right to -- sorry?

18 We have a five-minute break, so I'm wrong  
19 about that, too. Five-minute break, but please come  
20 back promptly. We've got a panel discussing GDPR.  
21 Thanks to our panelists.

22 (Applause.)

23 (End of Panel 4.)

24

25

1           PANEL 5: THE POTENTIAL IMPACT OF GDPR ON  
2                            COMPETITION AND INNOVATION

3           MR. STEVENSON: Hi, everybody. It's 4:00.  
4 That means it's time for the last panel of the day,  
5 and this is the panel on the potential impact of GDPR  
6 on competition and innovation. My name is Hugh  
7 Stevenson from the Federal Trade Commission.

8           We just heard a general discussion about the  
9 effects of privacy regulation on competition and  
10 innovation. And in a sense, this panel is now a kind  
11 of case study to look in more depth at that general  
12 question. And here it's the effect of the GDPR, the  
13 General Data Protection Regulation that we've heard  
14 referred to a number of times throughout the  
15 conference.

16           This regulation, which entered into force in  
17 May of this year in the European Union, it's obviously  
18 still early days for GDPR, but we have a distinguished  
19 panel here lined up to talk about its potential  
20 effects and the effects more generally, I would say,  
21 of the privacy approach reflected in the EU. When we  
22 talk about the effects of GDPR, it's not just the  
23 effects of the new regulation that came into effect  
24 that added some new features to what existed in Europe  
25 before, but also the European approach, which as we've

1 heard, varies in some significant ways from the  
2 American approach dating back at least to the '95 data  
3 protection directive.

4 We have lots of panelists here and little  
5 time, so I've asked each speaker to give a few initial  
6 thoughts before we proceed to questions. And we'll  
7 start with Renato Nazzini, who's a competition expert  
8 and a Professor at King's College London, and I turn  
9 the floor to him.

10 MR. NAZZINI: Thank you very much, Hugh, and  
11 thank you very much for the invitation to be here. So  
12 in the five minutes that I have, I would like to cover  
13 three points on the impact of European privacy  
14 regulation, which is just recently the GDPR but  
15 previously the privacy directive, on competition. And  
16 I start with one first point. We heard a lot today  
17 about the impact of privacy regulation on competition.

18 And I think there is no doubt in terms of  
19 the theoretical work that has been done and also the  
20 empirical work is there, in my view, that privacy  
21 regulation may have a negative impact on competition,  
22 maybe start the competitive process by favoring or  
23 disproportionately certain players versus the others.  
24 And there is also no doubt that there may be an impact  
25 on innovation and productivity and so on.

1           Now, the point I'd like to make that  
2 European approach is not really a choice between data  
3 protection regulation or no data protection  
4 regulation. Data protection, the right to privacy and  
5 data protection is a constitutional right, the right  
6 of a constitutional standing in European Union and a  
7 fundamental right. So the point is which data  
8 protection regulation to achieve the desired outcome  
9 should we have.

10           And I think that's really the important  
11 policy debate, we haven't had enough of it, we went  
12 straight into the GDPR, the privacy directive, and  
13 then the GDPR type, kind of process-based, heavy  
14 prescriptive regulation, which we can still have this  
15 debate now. You know, it is never too late to change  
16 something that doesn't quite work as well, assuming  
17 that it doesn't.

18           The second point that I'd like to make is  
19 that, of course there, is also a lot of talk, and  
20 there has been a lot of talk about the GDPR, about the  
21 role of privacy regulation as an enabler of  
22 competition. And I'll give you the most important  
23 example, which is the right to portability in the  
24 GDPR, the right of the individual who provided the  
25 data to obtain this data transfer then or have been

1 transferred to another supplier.

2 Now, the point I'd like to make here is that  
3 this portability right, which is -- or may be there  
4 also to address issues such as consumer switching in  
5 certain markets where data are important and there is  
6 a significant switching cost in the loss of data,  
7 financial services, messaging apps, social networks,  
8 and so on and so forth. It's not really a competition  
9 remedy, and it's not, therefore, going to be very  
10 effective, in my view, at addressing any competition  
11 concerns that we may have on these markets.

12 And the key reason for that is that actually  
13 together with switching costs and data, the other  
14 problem you have in this market is consumer inertia.  
15 There is quite a lot of research and certainly even  
16 case law in commission practice in Europe on this  
17 point. Therefore, the right to portability which  
18 depends entirely on the choice and the initiative of  
19 the consumer is not really going to be very effective  
20 if we do not have a very well informed and active  
21 consumer.

22 I'd like to contrast it for just a moment  
23 with the open banking remedies in the U.K. Open  
24 banking in the U.K. is a set of remedies which is  
25 there to address competition concerns in the retail

1 banking sector. And one concern was very low levels  
2 of switching of consumers and actually small  
3 businesses as well. And the remedy there imposed on  
4 certain U.K. banks is -- it relates to actually the  
5 obligation of these banks to make transaction data  
6 available to other financial service providers, such  
7 as anonymitive fintech companies.

8           And this comes together with a very  
9 significant package of remedies really tailored to  
10 give consumers and small businesses the information  
11 they need to make an informed choice and prompting  
12 them almost to make the choice overcoming, therefore,  
13 their inertia. So that is a proper competition  
14 remedy, may work well or not, it's too early to say,  
15 but that is a competition remedy as opposed to the  
16 right to portability.

17           And so my second point was actually using  
18 privacy regulation to enhance competition, remedy  
19 perceived competition problems. It's not likely to  
20 work very well.

21           And the third point I'd like to make in  
22 really a very, very short time is that one more thing  
23 to bear in mind is this idea of privacy regulation and  
24 privacy standards as a parameter of competition and  
25 whether a breach of privacy regulation can be an

1 element of a case of anticompetitive abuse or  
2 anticompetitive practice against a company, for  
3 example, a dominant company. And there is an ongoing  
4 investigation against Facebook in Germany precisely on  
5 this theory.

6 Now, for example, the Italian competition  
7 authority has addressed that very problem, the use by  
8 Facebook of data from third-party websites, you know,  
9 when the consumer is on third-party websites rather  
10 than on Facebook itself and their consumer protection  
11 legislation.

12 And, therefore, my third and final point is  
13 that actually while business and markets and perhaps  
14 life becomes more complex and privacy and data do  
15 become an element of competition analysis, in so many  
16 ways, I think there is a point in going back, perhaps  
17 sticking to basics in keeping these different tools  
18 that we have privacy enforcement, whatever it might  
19 be, private enforcement or regulation, competition  
20 enforcement or in consumer enforcement clearly  
21 distinct to avoid costly mistakes. Thank you.

22 MR. STEVENSON: Thank you very much for  
23 that.

24 We turn next to Garrett Johnson who we heard  
25 -- from Boston University, we heard from earlier

1 today, and we actually got an audience question about  
2 what is the impact of GDPR on innovation and  
3 competition and how can this measured. And I think  
4 Garrett can say a little bit on that subject from his  
5 perspective.

6 MR. JOHNSON: Thank you. So yesterday,  
7 several of you heard research from Jia, Gin, and  
8 Wagman on the short-run effects of GDPR on technology  
9 venture investment. They found an 18 percent  
10 reduction in the number of weekly venture deals and a  
11 40 percent reduction in the amount raised in an  
12 average deal following the rollout of the GDPR.  
13 That's obviously not great news.

14 Today, I want to tell you about some joint  
15 work that I have with Sam Goldberg at Kellogg, who is  
16 in the audience, and Scott Shriver at Colorado where  
17 we're looking at what happened online in Europe. The  
18 first way we're going to look at this is we're going  
19 to look at site visit and conversion outcomes on a  
20 panel of 2,300 websites. The second thing we're going  
21 to look at is third-party interactions and tracking on  
22 a panel of 28,000 websites. And the final thing we're  
23 going to look at is competition by looking at the  
24 number of sellers that publishers in Europe used  
25 looking at a panel of over 100,000 websites.

1           So I want to stress at the outset that this  
2    is not so much research that's hot off the presses as  
3    much as research that hasn't even made it to the  
4    presses, so take things with a grain of salt. This is  
5    a case of, I think, supply rising to meet demand.

6           So, first, I want to talk about the results  
7    for the panel of websites and site visits and  
8    conversions. For 2,300 websites, we see something  
9    like a 10 percent reduction in site visits and  
10   something like a 10 percent reduction in sales or  
11   conversions after the GDPR. And this is of the 900  
12   websites that are in our data that have that  
13   information.

14           Now, these findings are very provocative and  
15   very alarming, so I want to give you three big  
16   caveats. The first is that we're still trying to  
17   determine to what extent this is a real decrease and  
18   not an artificial decrease of reduced ability to  
19   collect data in Europe.

20           The second thing is that when you're looking  
21   at the effects of policy that impacts an entire  
22   continent at a certain period in time, it's pretty  
23   hard to find a good control that can give you a  
24   benchmark to evaluate that with. We're using the 2017  
25   data in Europe as a benchmark.

1           And, finally, this data, by nature, is  
2 extremely noisy and, so, we need to be careful in  
3 drawing strong conclusions for that. Now, the second  
4 thing that we looked at is compliance by EU websites  
5 in terms of the amount of third-party interactions or  
6 tracking that happens on those websites. The way that  
7 I went about this is I collected data from the top  
8 2,000 websites in every European country, EU country,  
9 as well as Canada, the U.S., and globally for an  
10 overlap of 28,000 websites.

11           And what I did is I represented myself as  
12 being a French user via VPN and collected, using  
13 software, every single third party that interacted  
14 with my browser, whether it be through cookies or HTTP  
15 requests or JavaScript. And what I saw there is in  
16 the week after the GDPR, there is a 12 percent  
17 reduction in third-party interactions relative to the  
18 days leading up to the GDPR. And because everyone is  
19 sort of scrambling to get in accordance with the GDPR,  
20 you might expect that that number would continue to go  
21 down, and, in fact, that is what happened in Denmark,  
22 that is what happened in the Netherlands.

23           But if you look at Bulgaria and Poland and  
24 other countries, you actually see that it goes down  
25 and then it bounces right back up again. So you look

1 at an average of all my data, these third-party  
2 interactions by now are essentially where they were  
3 pre-GDPR levels. So one thing that I want to do is  
4 try to see what explains whether or not these  
5 increases happened or not because we think it has  
6 something to do with basically how afraid these  
7 companies are of regulators in their local area, even  
8 though the GDPR was supposed to be uniformly applied,  
9 and so we used a survey metric of data providers that  
10 tried to quantify just how lenient they think their  
11 regulator is.

12 And that turns out to be a really great  
13 predictor of whether or not tracking third-party  
14 interactions went back up post-GDPR. And that's after  
15 accounting for wealth and for accounting for ad  
16 blocking and characteristics of the website, like the  
17 amount of content and ads that they have on the  
18 website.

19 Another finding that we found is that the  
20 place where you saw the most reduction in third-party  
21 tracking was actually where there were the least  
22 European users, so the websites that had 10 percent or  
23 less European users had the largest reduction, and we  
24 think that that's probably a result of a set of  
25 incentives that says that you will receive a fine of 4

1 percent of your global revenue if you violate the  
2 rules.

3 Now, the last thing when it comes to  
4 competition on this point, the evidence is pretty  
5 mixed if you split by top ten tracking firms versus  
6 below. The top ten were affected -- or reduced less  
7 than the bottom ten or the firms below the top ten  
8 trackers. But if you split it by top 50 versus  
9 outside that top 50, that pattern reverses.

10 And, so, we have a third piece of evidence  
11 that speaks to the competition issue that I'll go  
12 through briefly, and that is that we thought that when  
13 you tell firms that they're going to be liable for  
14 sharing data with others and that they need to get  
15 consent that firms would be less likely to interact  
16 with more firms. And, so, we looked at a self-  
17 reported measure of the number of ad sellers that  
18 European web publishers use called the Ads.Text  
19 initiative, and there we basically found nothing,  
20 which we were quite surprised by. So there's a small  
21 increase in the number of sellers that these websites  
22 are using, but, you know, there's a small increase in  
23 Canada, too, and so there was really not -- there was  
24 no sort of massive decrease as we might expect.

25 So with that, I'll pass things on.

1           MR. STEVENSON: Thank you for giving us this  
2 preview of this very interesting research, and you all  
3 heard it here first.

4           So next we turn to Jim Halpert to get a  
5 practitioner's perspective. Jim is a well-known  
6 privacy lawyer at DLA Piper and has been involved in  
7 some of these issues for quite some time. Jim?

8           MR. HALPERT: Thank you, Hugh, and thanks  
9 for the opportunity to speak. I'm actually here today  
10 with the head of our Polish IPT practice, Ewa  
11 Kurowska-Tober, who can speak further about Poland and  
12 the enforcement environment, which I think is a little  
13 bit different than the assumption behind the survey  
14 data, but it's nonetheless a very interesting survey.

15           I'd make a few points that are more from a  
16 practitioner's sort of practical perspective. I've  
17 seen it for non-EU entities that are -- that have some  
18 presence in Europe but do not have a lot of users, GDP  
19 -- the decision about whether to comply with GDPR if  
20 they were a website operator was a fairly clear  
21 decision for those who were not among the largest.  
22 And you can see data that the top third of the 100 --  
23 or a third of the top 100 websites responded to GDPR  
24 by blocking EU visitors, and there are a number of  
25 articles about this.

1           The same thing is true of nearly 100 public-  
2 facing websites that a survey by Data.VerifyJoseph.com  
3 came up with as well. So you see a parade of entities  
4 that just were not making that much money in Europe  
5 who said it's not worth it. So from a competition  
6 perspective, you know, probably the crafters of GDPR  
7 smiled at that because they don't really want  
8 competition necessarily coming from the United States  
9 in the internet market, but nonetheless, there clearly  
10 was, at least when this regulation went into effect, a  
11 drop-off effect on public-facing websites that just  
12 didn't want to deal with the GDPR compliance through  
13 their ecosystem.

14           Another thing to think about is that  
15 requirements for granular consent necessarily  
16 disadvantage entities that have fewer customers and  
17 need to rely on the notice and consent being floated  
18 by the website operator and put them at a  
19 comparatively weaker position to craft a consent that  
20 will fit their business models.

21           We see this also in terms that -- and this  
22 is not something that's public, but the term -- the  
23 processing term, processor terms or subprocessor or  
24 co-controller terms that were passed down to smaller  
25 entities by bigger entities under GDPR. The fact was

1 that smaller entities took an awful lot of  
2 obligations, contractually, and an awful lot of  
3 liability that they probably were not able to handle,  
4 but nonetheless, the formality of the processing  
5 agreement led to bigger entities exercising their  
6 greater bargaining power to drive through obligations  
7 to be able to absolve themselves of compliance.

8 Another thing to look at in the ecosystem  
9 environment like the advertising ecosystem -- and  
10 Chuck Kerr who represents Better Ads is in the back  
11 and does a lot of work; I know that Leigh Freund was  
12 here as well -- is that the GDPR did create at least  
13 temporary disruptions with a sort of whipsaw effect  
14 where the entities, there were several of them that  
15 are very big in the internet advertising environment  
16 and were under a lot of scrutiny by regulators. So  
17 they needed to, you know, break it -- to make an  
18 omelet, you need to break a few eggs, and they needed  
19 to come up with a compliance structure that was  
20 auditable, and ecosystem providers needed to conform  
21 to that.

22 I would suggest that a less granular set of  
23 obligations on downstream entities that was more  
24 outcome-spaced, would be a better way to avoid drop-  
25 off and disruption in the ecosystem, and I'm not here

1 to praise the CCPA, the California privacy law, in all  
2 aspects. There are ways in which it's very poorly  
3 drafted, but its processor obligations, its service  
4 provider obligations are very outcome-based.

5 Really, the question for the service  
6 provider, they need to sign an agreement saying to be  
7 a service provider then be outside of the disclosure  
8 obligations under the CCPA, they need to promise only  
9 to process the data, store it, use it for the duration  
10 of the service contract that they have with the entity  
11 that is the business that's giving them the data, and  
12 not to sell it or use it or disclose it for any other  
13 purpose.

14 And that may be a more neutral way to get to  
15 an outcome where the core interest, which is in  
16 preventing further pollution, if you will, of the data  
17 -- personal data ecosystem out there is achieved  
18 without being so granular for obligations that need to  
19 be passed along to smaller entities that really can't  
20 say no. Thank you.

21 MR. STEVENSON: Thank you, Jim.

22 So we've heard a little bit about the role  
23 of the regulator in the EU system under GDPR, and  
24 there's a data protection authority, or DPA, in every  
25 country, so it's only fitting we include a DPA

1 perspective on the panel, so we turn next to Simon  
2 McDougall from the U.K.'s DPA, which is called the  
3 Information Commissioner's Office. And Simon even has  
4 innovation in his title, so he seems perfect for this  
5 panel. So we'll give him a couple of minutes to  
6 describe their perspective.

7 MR. MCDUGALL: Thank you. I've had this  
8 title, Executive Director of Technology Policy and  
9 Innovation for a whole five weeks now. Before that, I  
10 ran a privacy consulting practice for Promontory,  
11 which is now part of IBM, and spent most of the last  
12 few years helping large corporations with their GDPR  
13 implementation. So my comments now are informed as  
14 much by what I saw in my time in the private sector as  
15 now.

16 I want to just first talk to a couple of  
17 points that have already arisen. First of all, you  
18 could get the impression that Europe was some kind of  
19 blazing wasteland on May 26th and nobody got any ads,  
20 and that was all terrible. It really was not like  
21 that, and I don't think anybody noticed any particular  
22 difference in their experience on a day-to-day basis.

23 I also think that to quote Chairman Lai in  
24 his conversation with Henry Kissinger about the French  
25 Revolution, it's too early to tell what the impact of

1 the GDPR will be. And I think Rahul made a great  
2 point on the last panel that uncertainty is as  
3 damaging as prescriptive regulation. And what we  
4 definitely saw leading up to the GDPR and then  
5 afterwards was a lot of uncertainty. So it will be  
6 really interesting to see how this data pans out over  
7 the next few months and indeed next couple of years  
8 because right now the GDPR seems to be going okay, to  
9 be honest. And in terms of the market in Europe, you  
10 know, again, I'm not hearing anything terrible from my  
11 old private sector clients.

12 I want to mention one thing in relation to  
13 competition and then a couple of points around  
14 innovation as well. The points I'll raise on  
15 competition is just to note in passing that the GDPR  
16 has some interesting mechanisms in it, which I think  
17 have the possibility of really enhancing competition  
18 in the medium term. And that's codes of conduct and  
19 certifications.

20 And the difference there is that a code of  
21 conduct in GDPR-speak is where a body such as a trade  
22 association creates some rules specific to its  
23 vertical, and then a data protection authority will  
24 sign them off. Certification involves certification  
25 bodies and a more complicated scheme.

1           We're seeing a lot of interest right now in  
2 codes of conduct, less so in certifications because I  
3 think they'll take longer to implement. I think if  
4 for certain markets we get simple, practical codes of  
5 conduct, then that could be very helpful to new  
6 entrants because it will reduce this uncertainty and  
7 add clarity.

8           Conversely, if we end up endorsing -- as  
9 European data protection authorities, we end up  
10 endorsing very complicated codes of conduct, obviously  
11 that could provide a barrier to entry by just creating  
12 more rules around particular environments that are  
13 deterring to smaller firms. So that's something we  
14 need to look at, but I think good, clear codes of  
15 conduct can be very helpful in these circumstances to  
16 reduce this uncertainty.

17           But I want to spend a couple of minutes also  
18 talking about the innovation side of my job because I  
19 think often today competition and innovation have been  
20 conflated in different ways. So let's talk about  
21 innovation in terms of its classical competition,  
22 whereby we're talking about the process where we go  
23 from somebody having a really bright idea, some people  
24 in the garage, an innovation hub of a large firm, an  
25 academic, all the way through to realization, i.e., a

1 retail product goes out or a government does something  
2 for its systems which is cool and wasn't done before.  
3 So let's talk about innovation there.

4 My role is new at the ICO, and I'm building  
5 an innovation department which we're still staffing  
6 with some amazing people, but we're very focused on  
7 innovation as innovation, and we're doing a whole  
8 range of different things to promote it. Three areas  
9 quickly in the time I have.

10 Firstly, we're engaging with thought leaders  
11 around key areas, such as artificial intelligence,  
12 digital ethics where a lot of this innovation is  
13 happening. So we've been very active in helping set  
14 up the Center for Data Ethics and Innovation in the  
15 U.K., which is a government-backed center which is  
16 just being founded now as we speak. And we're working  
17 with the Alan Turing Institute around explainable  
18 artificial intelligence and how we can help ensure  
19 this trust in AI.

20 I think there's a huge risk here that AI  
21 goes the same way as GM, where, hey, you guys have got  
22 it, we haven't got GM, genetic modified foods, in  
23 Europe because everyone lost trust in that particular  
24 technology. AI could easily go the same way unless  
25 the industry explains to people what on earth is going

1 on. So explaining AI is a big thing.

2 Secondly, we are building a regulatory  
3 innovation hub whereby we're accepting that we're a  
4 horizontal regulator in a world of vertical  
5 regulators. And when a firm comes with innovative  
6 ideas to our financial services regulators or our  
7 telecoms regulators and they have questions, we then  
8 can help make sure it's a one-stop-shop for that  
9 regulatory question by being in the room with that  
10 regulator or being at the end of the phone to help  
11 them.

12 Thirdly and finally, we are setting up a  
13 regulatory sandbox, leveraging the success of  
14 financial services regulatory sandboxes with  
15 innovative firms whereby firms can apply to be in the  
16 sandbox. And if we say yes, they develop a close,  
17 continuous, collaborative relationship with, in this  
18 case, us, the ICO, where they can take their project,  
19 they can pilot it, and they can work with us so that  
20 they end up doing something exciting and innovative  
21 but in a privacy-respectful way.

22 So my key message here is that as a privacy  
23 regulator and I think it's applicable to privacy  
24 regulators around the world, we do not have to be  
25 passive here. We can be on the front foot and we can

1 do interesting things to promote both competition and  
2 innovation. And there I'll stop, thanks.

3 MR. STEVENSON: Thank you very much. We  
4 appreciate that particular description of the many  
5 interesting projects that the ICO has underway.

6 We have next Rainer Wesley, a friend and  
7 colleague from the EU Mission, and before that,  
8 formerly of DG Comp, and we give the floor to him.

9 MR. WESSELY: Thank you very much for  
10 inviting me to this panel. It will not surprise you  
11 that we in Brussels at the European Commission are  
12 following these hearings with big interest because  
13 most of, if not all of the topics discussed here, are  
14 equally of high relevance also for our internal  
15 discussions.

16 Originally, my intention was actually to  
17 start off to give you a very brief overview of how we  
18 deal at DG Competition at the European Commission with  
19 big data, data, and data protection in our Commission  
20 -- press the microphone, it is on, it tells me -- with  
21 data protection for specific markets. But taking that  
22 this was part of an earlier session this morning  
23 already and taking our time constraints, I will limit  
24 myself to one key observation. We have gathered over  
25 the years a lot of experience, in particular in merger

1 cases, of how to assess data and big data markets, but  
2 what we see recently is that the assessment of data  
3 protection in our competition and merger analysis is  
4 getting ever more important. And the reason for this  
5 is certainly that consumers give always more  
6 importance to their protection of the data, and we can  
7 see that, and this is reflected in our decisions.

8 And, actually, it also mirrors my own  
9 experience. Five or ten years ago I think I would not  
10 have cared so much about what happens to my personal  
11 data, but nowadays I think if I have an option where I  
12 can go for safer and more protective measures then I  
13 would always try to opt for that.

14 As our competition commissioner, Margrethe  
15 Vestager, put it already in 2016, we would not use our  
16 competition enforcement to fix privacy problems, but  
17 that does not mean that we will ignore genuine  
18 competition problems just because they have a link to  
19 data, which takes me now to the topic of today's panel  
20 and the question of the actual or potential effect on  
21 innovation and competition of the GDPR.

22 And I would like to structure it in three  
23 points, basically where we are coming from. As Renato  
24 already said before, data protection in Europe is  
25 nothing new. We have had rules for many, many years,

1 over two decades. And, intuitively, I think that  
2 would speak for questioning whether they should be a  
3 negative impact on competition and innovation in the  
4 first place.

5 Then I would look at where we are now. We  
6 have created a very strong, level playing field across  
7 Europe, which reduces compliance cost and reduces  
8 burden for companies. And looking forward, I think I  
9 will add some words on the entry barriers which  
10 allowed -- through GDPR, as also Renato mentioned  
11 already, we have built in innovation incentives,  
12 thanks to privacy by default and by design. So I  
13 think in the end and eventually the GDPR should  
14 actually stimulate innovation and competition.

15 So if I look at where we're coming from in  
16 the past, we had a directive and a patchwork of many  
17 national laws. Since the beginning of the data  
18 protection reform and the discussion of the reform, we  
19 saw that competition and innovation were at the heart  
20 of these discussions. The aim was to create a level  
21 playing field addressing the consumer trust deficit  
22 and simplifying and harmonizing the data protection  
23 leading framework as a key element of the digital  
24 single market, which is, as many of you will know, one  
25 of the key priorities of the current European

1 Commission.

2 In other words, the patchwork that existed  
3 in the past has been replaced by one single pan-  
4 European law. Instead of having to deal with 28  
5 different data protection laws and 28 ways of  
6 interpretation, since May last year -- this year  
7 operators doing business in Europe can rely on one set  
8 of uniform rules.

9 This brings me to where we are now. The  
10 GDPR has put these rules into a new shape, making them  
11 more coherent and directly applicable. Of course, we  
12 had heard many concerns, and I heard them yesterday  
13 and today again, that certain economic experts say  
14 that their business models will actually not work with  
15 the GDPR and that they are competitively disadvantaged  
16 with big and foreign operators.

17 As already also mentioned, it is probably  
18 too early to make a long-term assessment at this point  
19 in time to see whether these claims are actually true.  
20 We have seen fear of some companies because of  
21 compliance, because of risk of fines, and there has  
22 been lot of uncertainty, but I think generally first  
23 evidence that we see points in a different direction.

24 For many companies, compliance with GDPR has  
25 actually brought along opportunity to bring their data

1 house into order. They could look at what kind of  
2 data they actually collect, they could see what they  
3 use it for, how they assess it, and how they process  
4 it. For some of them, this brought actually new  
5 opportunities because they could find out what data  
6 they possess and use it in new more innovative forms.

7 In doing these checks, and there was also  
8 already mentioned some of them have also eliminated  
9 unnecessary risks, which we see in the recent past  
10 that risks of data breaches can lead to high financial  
11 interpretation of costs. I think there was a study  
12 last week which tried to put a price tag on the loss  
13 of revenues due to reputational risk which was a  
14 multi-billion sum.

15 Without consumers' trust in the way that  
16 data is handled, there can be no sustainable growth in  
17 the way of our data-driven economy. So the GDPR has  
18 harmonized and simplified data protection and this in  
19 return has led to a significant reduction of  
20 compliance cost and administrative burden. I think  
21 these are very tangible direct results and benefits  
22 for, in particular, small and foreign companies which  
23 want to be active in the European market and which do  
24 not have the resources to make studies of legal  
25 requirements of different national systems.

1           Now, looking forward, the GDPR has, as  
2 already mentioned, introduced mechanisms to lower  
3 entry barriers. We look at Article 20 of the GDPR,  
4 which stimulates and facilitates the entrance of new  
5 players. The right to data portability has a clear  
6 competition rationale, and there I would slightly  
7 contradict Renato because I think you can draw a  
8 comparison to the right of number portability in the  
9 telecommunication sector, and we saw that this was a  
10 very stimulating effect, and we hope to replicate this  
11 effect also for data portability.

12           MR. STEVENSON: Thank you.

13           We turn now to our final panelist, who is  
14 Orla Lynskey, a Law Professor and Data Protection  
15 Expert at the London School of Economics, who I see  
16 way down there. And we'll hear her perspectives now.

17           MS. LYNSKEY: Thank you, and many thanks for  
18 the opportunity to provide some remarks for this  
19 hearing today. I think before I start I just want to  
20 highlight again the very different constitutional  
21 context in which this discussion has occurred in  
22 Europe because of the presence and the EU charter of  
23 fundamental rights of both a right to privacy but also  
24 a separate right to data protection.

25           And as a result, there is a legal obligation

1 to have data protection rules in place to protect the  
2 data of European individuals. And I think that's an  
3 important differentiating factor between this  
4 discussion in the EU and this discussion in the U.S

5 I'd like to think about two interrelated  
6 claims about how EU data protection rules can impact  
7 on competition and on innovation. And the first is a  
8 very obvious one, which is that the GDPR and its  
9 predecessor, the 1995 data protection directive,  
10 formed part of the legal and regulatory landscape that  
11 competition authorities needed to take into account  
12 when undertaking competitive assessments and thinking  
13 about the application of competition policy.

14 Now, this sometimes led to the incorrect  
15 assumption that the mere existence of data protection  
16 regulation meant that these markets, data markets,  
17 were functioning effectively for consumers. And I  
18 think you can see this, for instance, in some of the  
19 European Commission's decisions. So if you look at  
20 merger decisions like Google-Snelfie or Microsoft-  
21 LinkedIn, you see before the GDPR had even been signed  
22 off that the Commission is saying that the mere  
23 potential for the right to data portability to be  
24 exercised meant that consumers couldn't be locked in.

25 And I think that's an erroneous assumption

1 to work from because we have clear empirical evidence  
2 that there are many impediments to individual control  
3 over personal data. So my own research has focused on  
4 the role and the limits of information self-  
5 determination in European data protection law. But  
6 also I think we have a documented cycle of what  
7 Farrell, a former Director of the Bureau of Economics  
8 here, described as a dysfunctional equilibrium. And  
9 that is the fact that firms who do wish to  
10 differentiate their offerings on the basis of more  
11 privacy-protective products find that there is little  
12 incentive to do so because consumers have already  
13 resigned themselves to the fact that there is no  
14 better offering out there, and this creates a vicious  
15 cycle.

16 And I think we have -- that idea was  
17 proposed in 2012. And if you fast forward to this  
18 year, the consumer organization which in the U.K.  
19 documented similar phenomenon when they say that we  
20 have a situation of rational disengagement from data-  
21 protection policies. And that is that, in fact, the  
22 rational thing for a consumer to do might be to  
23 simply not engage with those policies in certain  
24 circumstances because they are so complex and the  
25 ability to control data is so limited.

1           So, then, the second point I want to make  
2   is, or a query I want to ask is, what might GDPR do in  
3   order to improve this situation. And, here, I think  
4   that although the core system of checks and balances  
5   in EU data protection law has remained unchanged from  
6   the 1995 rules, the GDPR introduces some small but  
7   significant substantive changes that have the  
8   potential to really clean up the European data  
9   ecosystem and, in particular, online.

10           And, so, I just want to highlight one that  
11   has currently become the focus of complaints to  
12   European data protection regulators. And, so, if we  
13   consider how data is processed or the legal basis for  
14   data processing, one of the most commonly used ones  
15   online is consent. It's not the sole legal basis for  
16   processing but it is one of the most frequently used.  
17   And consent has to be freely given, specific, and  
18   informed. So far so similar to the 1995 rules.

19           However, what the GDPR does do is specify  
20   that freely given consent -- in considering whether  
21   consent is freely given, you need to take utmost  
22   account of whether or not the performance of the  
23   contract is made conditional on the processing of data  
24   that is not necessary. And, so, here the idea is that  
25   you will use or acknowledge that consent is not freely

1 given if it leads to unnecessary data processing and  
2 if, therefore, consumers can't access services or  
3 goods that they wish to access as a result.

4           So this conditionality requirement is, in  
5 fact, a presumption, so there's a presumption that if  
6 access is conditional on unnecessary data processing,  
7 that consent is unlawful, that, therefore, it has the  
8 potential to seriously alter the way in which data-  
9 driven -- and in particular data-driven advertising  
10 models, and in particular programmatic advertising, is  
11 operated in Europe. Because if the European data  
12 protection boards, the new agency for data protection  
13 in Europe, takes a hard line or a strict  
14 interpretation of this provision, it could say that  
15 data as counterperformance for the offering of a  
16 particular goods or service is not necessary for the  
17 performance of the service. And we have several  
18 opinions of its predecessor, the Article 29 working  
19 party, to indicate that that's the way in which it is  
20 thinking.

21           And this, I think, would then push us  
22 towards a model of advertising in Europe that is no  
23 longer behavioral and programmatic but rather  
24 contextual as was highlighted in the previous panel.

25           And just to say finally because I need to

1 wrap up that these small but significant substantive  
2 changes are coupled with very significant enforcement  
3 changes. And the fines -- the 4 percent of annual  
4 global turnover have received all of the attention,  
5 but, in fact, in my opinion, what's likely to be far  
6 more significant is the creation of a new agency, the  
7 European Data Protection Board, in order to ensure  
8 consistency across Europe of decision-making, but also  
9 the potential to mandate a representative organization  
10 to take actions on your behalf, which is provided for,  
11 for instance, under Article 80 of the GDPR.

12 And, so, we have the potential also here for  
13 private litigation in order to really render  
14 individuals' data protection rights more effective.  
15 And then I think we'll be in a different data-driven  
16 environment.

17 MR. STEVENSON: Thank you very much for  
18 those comments. And I think that these and some of  
19 the earlier comments remind us that here we are  
20 dealing both with some different constitutional  
21 contexts, as Renato and Orla mentioned, some different  
22 administrative context, the kind of commentology of  
23 the system in Europe for deciding sort of the rules  
24 and also different enforcement context. There was a  
25 reference to the fines and what has been added from

1 GDPR on that subject.

2 I'd like to take up first the issue that you  
3 just raised about the European Data Protection Board  
4 and the other sort of related aspects of this system  
5 that deal with interpreting the law and how that  
6 looks. This is a '99 article, sort of document, it's  
7 a long thing, the GDPR, but it has a number of  
8 provisions that deal with interpretation. How  
9 important is interpretation to the effect of GDPR on  
10 competition and innovation and how fit for purpose is  
11 the mechanism that's been set up, the European Data  
12 Protection Board and the DPAs within that?

13 Maybe I'll start with Simon and then Jim  
14 then others who might want to comment.

15 MR. MCDOUGALL: I think having the  
16 consistency mechanisms in place is critical. And to  
17 echo some of the other speakers, we shouldn't forget  
18 about this regulation and also the preceding '95  
19 directive, you know, work specifically around having  
20 the free movement of data around Europe, as well as  
21 with the regulation and introducing privacy as a  
22 fundamental right as well.

23 So it has always been around both those  
24 mechanisms and having a level playing field across  
25 Europe. We had a really practical problem in the

1     buildup to GDPR where, quite rightly, many local data  
2     protection authorities were issuing lots and lots of  
3     guidance to help their national organizations, all the  
4     firms they regulated get up to speed with GDPR.

5             For international organizations, that meant  
6     there was an awful lot of different guidance to keep  
7     track of, and with the best will in the world,  
8     sometimes there was variation. We've just had the  
9     EDPB provide guidance on one particular area, which is  
10    around rationalizing the shopping list of conditions  
11    that might mean a firm has to undertake a DPIA, a data  
12    protection impact assessment, where there were  
13    differing lists across different countries.

14            That's really practical, helpful stuff, so  
15    we do need these mechanisms, and over time hopefully  
16    we'll see a lot of these wrinkles be smoothed out.

17            MR. HALPERT: This is a great example --  
18    sorry. Simon offered a great example of the work that  
19    the EDPB needs to do, but the fact remains that the  
20    much ballyhooed one-stop shop and harmonized set of  
21    rules that Rainer described did not exist as to key  
22    elements of ambiguity prior to adoption or GDPR going  
23    into effect. And the cost of GDPR implementation  
24    exceeded \$10 million for most firms that were  
25    multinational and had more than \$500 million in sales.

1           So the result was significant uncertainty  
2 with -- our firm developed a DPI assessment tool and  
3 had to customize it before this guidance came down to  
4 different requirements in different states. And this  
5 is a very common process. With regard to personal  
6 data breach, Ewa and I were speaking this morning and,  
7 you know, one assumes that risk to fundamental rights  
8 and freedoms of the data subject would be a uniform  
9 breach notice requirement across Europe.

10           Well, in Poland, the regulator, when given  
11 the advance notice, will not say in any circumstance,  
12 even a trivial one, that there isn't a risk to the  
13 fundamental rights and freedoms of individuals, which  
14 is a different standard than in other EU member  
15 states. So really the EDPB needs to be very active to  
16 counter the centripetal forces that are at work among  
17 autonomous DPAs.

18           I'd also add that there is no uniformity  
19 with regard to issues like children's consent, labor  
20 laws. The German implementation of GDPR contained a  
21 whole separate labor code, labor privacy code that was  
22 enacted. So while I don't think that actually GDPR  
23 offers a good model of uniformity at this point for  
24 the United States to look to in its eventual privacy  
25 regulation, and while I'm very sympathetic to data

1 portability and many of the other points that Rainer  
2 mentioned, I think it's really worth looking at the  
3 EDPB as a work in progress to try to fulfill the idea  
4 of a uniform set of rules across Europe.

5 MR. STEVENSON: Thank you. I think Rainer  
6 wanted to comment, and then Garrett.

7 MR. WESSELY: Well, yes, I think I can  
8 confirm that obviously the current definition and way  
9 of interpretation of the GDPR is extremely important  
10 but we have seen also from the EDPB that throughout  
11 last months there has been guidance. There have been,  
12 I think, in total 18 guidance papers in the meantime  
13 published, which builds on top of the guidance which  
14 was given previously already by the Article 29 working  
15 party.

16 So that is obviously a first challenge also  
17 to see where the guidance is most important in the  
18 first place. And to the uncertainty which is and was  
19 in the market, I think that is probably normal with a  
20 big new regulation like the one that we saw. But on  
21 the other hand, what we can see is that there have  
22 been certain companies which have decided to play safe  
23 in the first place, said that they would suspend for a  
24 certain time the activity, vis-a-vis Europe would  
25 block European customers, but what we see now is

1 actually already a trend that most of these pages are  
2 in the meantime accessible. Again, which shows that  
3 we have to clearly distinguish between the very short-  
4 term effects, the midterm, and the longer term  
5 effects, and that is exactly also where we then have  
6 to focus our guidance, I think.

7 MR. HALPERT: Absolutely. Totally agree.

8 MR. STEVENSON: Thank you. Garrett and then  
9 Renato.

10 MR. JOHNSON: So I think the question of  
11 interpretation is a really important one because, you  
12 know, we're here talking about this because the U.S.  
13 and certainly many business leaders or some business  
14 leaders are calling for a GDPR-style regulation in the  
15 United States. So the reason interpretation is  
16 difficult is that, as someone said, I think Simon  
17 said, you know, on May 6th, Europe didn't burn down.

18 Now, it would be hard to conclude from that  
19 that there were no impacts of GDPR. Certainly the  
20 research that was presented yesterday, and some of my  
21 research suggests that there are some impacts of the  
22 GDPR and some of those are troublesome. But a larger  
23 issue is that, you know, what we have yet to see is an  
24 enforcement action in Europe that clarifies some of  
25 these issues.

1           So I think Orla brings up a really good  
2 point about the state of programmatic advertising in  
3 Europe. Currently, the sort of de facto way that most  
4 websites have handled this is an opt-out notice that  
5 shows up when you arrive on their website, and  
6 basically 90 percent of people are consenting or not  
7 going through the process of opting out.

8           Now, the laws, as you say, if the regulators  
9 want to take a hard take on this, the laws pretty  
10 clearly say that they want opt-in consent, that's  
11 specific to purposes, so imagine as you're a consumer,  
12 you need to check, you know, 50 different companies  
13 that get to know your website -- get to know that you  
14 visited a website and eight different purposes, you're  
15 going to be checking a lot of boxes. And, of course,  
16 that's going to mean that basically no one's going to  
17 be checking these boxes.

18           And then you'd see a very different effect  
19 of the GDPR on the web. So I think the truth will  
20 continue to evolve here.

21           MR. STEVENSON: Thank you.

22           Renato.

23           MR. NAZZINI: Yes, very briefly on this  
24 point, and coming to that from a competition  
25 perspective, I think even the regulatory setup in

1 Europe, what is very important and is happening to an  
2 extent is that competition authorities and data  
3 protection regulators talk to each other. Of course,  
4 interagency cooperation always comes at a cost in  
5 terms of resources and time, but I think it is very  
6 important, especially if, as Rainer was saying,  
7 certain of the provisions of the data protection of  
8 the GDPR ought to be interpreted in a way that fosters  
9 competition.

10 I'm very happy that the right to portability  
11 is there, obviously. I'm just saying that it is not a  
12 panacea for competition problems in these markets, in  
13 which it's law. Data are a little bit more complex  
14 than just a six or seven or eight-digit number to  
15 port. And, for example, where interpretation will be  
16 important, and we have seen already good evidence that  
17 we are going towards that direction, you know, let's  
18 interpret, for example, the right to data portability  
19 in a way which is more conducive to competition.

20 The regulation says, data provided by the  
21 individual, well, clearly a broader interpretation  
22 that provided by which includes as much as the data  
23 which is necessary for others to compete as possible,  
24 that would be a good thing for competition. So I  
25 think this point is quite important.

1           MR. STEVENSON: Thank you.

2           Let me turn to another subject that often  
3 comes up in connection with GDPR, and that is the up  
4 to 4 percent of total worldwide annual turnover as  
5 potential sanctions, which has already been mentioned  
6 in the conference several times, even outside this  
7 panel. What effect do those provisions have  
8 potentially on innovation and competition? Are there  
9 certain effects, either pro or con, of having these --  
10 I think anyone would describe them as, indeed I think  
11 even one of the authors of GDPR describe them as heavy  
12 sanctions. Orla?

13           MS. LYNSKEY: Well, I think the fines were  
14 initially modeled, in fact, on antitrust fines with  
15 the antitrust and the competition provisions as the  
16 source of inspiration for that. However, I do think  
17 regulators, including the ICO, for instance, in the  
18 U.K., have been very quick to point out that they will  
19 continue to work with those data controllers and data  
20 processors that are endeavoring to comply with the  
21 regulation and that fines are kind of a backstop here.

22           But as I said, I think there are other  
23 mechanisms, such as the potential for strategic  
24 litigation that is provided by regulation, that will  
25 lead to, as we were just discussing, more interpretive

1 clarity.

2           If I can come back to the point that Garrett  
3 made about the problematic impact of GDPR, well, if  
4 that is fewer third-party trackers, well, again,  
5 that's a question of whether or not you think that is  
6 problematic because, in fact, at the moment there is a  
7 complaint pending before the ICO in the U.K. and Irish  
8 data protection commissioner that the entire realtime  
9 bidding system is inconsistent with many core  
10 principles of GDPR, including data minimization,  
11 fairness, transparency, and many others. And that is  
12 a question, then, of looking at the entire system that  
13 is in place and seeing whether or not that's data-  
14 protection-compliant.

15           And then on the issue of less investment,  
16 which the Wagman paper mentioned yesterday, I think  
17 this comes back to what Simon said, which is it  
18 depends on whether or not we can encourage investment  
19 in privacy-protective technologies and privacy-  
20 enhancing technologies. For instance, that paper  
21 doesn't consider at all the jobs that will be created  
22 for data protection officers and others.

23           So I think a narrow focus on simply the  
24 fines and the sanctions ignores all of these other  
25 potential mechanisms for interpretation and

1 innovation.

2 MR. STEVENSON: Jim.

3 MR. HALPERT: Actually, I'd like to make one  
4 quick point with regard to the group actions point. I  
5 think that group actions can make sense, but they only  
6 make sense if the legal requirements are relatively  
7 clear. And it's a little bit troubling to think of  
8 group actions as the battering ram to get clarity,  
9 where in a system, the question of what's a legitimate  
10 interest of the data controller, for example, that  
11 overrides the data protection subject.

12 That's something that the regulators really  
13 should provide guidance on. I totally agree with you  
14 that the question about how realtime exchanges work in  
15 relation to data protection, some guidance would be  
16 helpful on that, but a regulator really should be  
17 doing that sort of work.

18 I'd also point out that there are very  
19 different sorts of incentives in class action  
20 litigation in the United States, and one shouldn't  
21 assume, as some do, that while GDPR has class action  
22 risk that should be, for example, the mechanism for  
23 enforcement of the California Consumer Privacy Act or  
24 some federal law that was based on GDPR.

25 There's no e-discovery regime in Europe, so

1 the asymmetrical costs, which are about a million  
2 dollars anytime a lawsuit is filed, that are only  
3 borne by the defendant, are very, very different.  
4 There are also -- are typically not the ability to  
5 obtain attorneys' fees; and, in fact, there are no  
6 damages available under GDPR group actions. So this  
7 is really an apples-to-oranges comparison, and I just  
8 wanted to give that frame and then give back the time.

9 MR. STEVENSON: I just wanted to put one  
10 more question out. We only have a few minutes left.  
11 And that is, and I know one of our Commissioners has  
12 sort of raised the issue of one thing that U.S. law  
13 does in some ways is to tailor the regulation that  
14 exists to the risk, to tailor regulation to the risk.  
15 Is that important to do here, and does the GDPR do a  
16 good job of tailoring the regulation to the risks that  
17 exist?

18 Renata.

19 MR. NAZZINI: I think I can have the first  
20 go at that. I mean, it seems the GDPR is actually a  
21 set of rules that in principle, there are other  
22 exceptions and modulations, but apply to all firms and  
23 all data with the higher threshold for certain  
24 particularly sensitive data, such as health data,  
25 political opinions, et cetera.

1           In principle, it's not the kind of risk-  
2 based, outcome-based regulation, but it's a process-  
3 based regulation which applies across the board. So  
4 it doesn't really do so, but I think it is fair to say  
5 that the objective of the regulation was actually to  
6 set out that level playing field across the board.  
7 And that's where some of the problems that Garrett and  
8 others actually have highlighted come from.

9           MR. HALPERT: In fairness, though, fines are  
10 geared to risk of harm, too, so there is some -- if  
11 one looks at the eye-popping sanctions, they do depend  
12 on high risk, for example.

13           MR. STEVENSON: Okay. Simon?

14           MR. MCDUGALL: Well, to echo what Jim was  
15 saying, yeah, there's definitely elements to the GDPR  
16 which do talk directly to considering risks. The  
17 accountability regime is also a new entrant, and I  
18 think it's critical to understanding how the GDPR can  
19 reward good behavior in firms large and small.

20           But I also want to say one word on just how  
21 this wraps into the other risks that large  
22 organizations and small organizations deal with and  
23 reputational risk. And what I think we're seeing on  
24 both sides of the Atlantic right now is an ongoing  
25 breakdown in trust. And that's an ongoing breakdown

1 in trust in many ways, but one of the ways is in how  
2 people -- whether people trust organizations in  
3 handling their data. And that has a massive  
4 competitive impact, and sometimes it's dragging all  
5 organizations down, so it's not a relative thing, but  
6 I think in many cases it favors the incumbent because  
7 people aren't going to make the leap into a new  
8 venture or a new technology if they don't really trust  
9 the environment they're in. And that's a critical  
10 part of the GDPR that it can help rebuild trust and  
11 give you confidence in using new services because they  
12 believe their data will be handled responsibly.

13 MR. STEVENSON: Orla, did you have a  
14 comment?

15 Oh, I'm sorry, Rainer.

16 MR. WESSELY: I would strongly agree to  
17 that. I mean, certainly it is process-based, and what  
18 we think that the challenge is that the GDPR has to be  
19 sufficiently flexible actually to adapt itself to new  
20 risks which we could not even predict at the time that  
21 the GDPR was planned.

22 Just let me make one additional point. We  
23 try, as from the first day of the GDPR, to be as  
24 constructive as possible in the dialogue with the  
25 economic operators on the market. I think by now it

1 is clear that GDPR is not used as a fining sword and  
2 so as a very smooth phasing-in, which is also  
3 underlined by -- I don't know whether you followed  
4 that, but Commissioner Joureva just said that in June  
5 next year, 2019, people have one day -- we will have a  
6 stock-taking exercise in order not to wait until 2020,  
7 which would be the set time for when we have to report  
8 back to the European Parliament. So next year, we  
9 should be able to address actually many of these  
10 questions and look into the effects on innovation and  
11 competition.

12 MR. STEVENSON: Any other last words on  
13 this? Yes, Renato.

14 MR. NAZZINI: Just one point about fines,  
15 actually. I think one positive aspect to the 4  
16 percent worldwide turnover fine is it actually -- an  
17 argument that obviously not too explicitly but it has  
18 been made and I've heard in Europe that, you know, you  
19 have to use competition enforcement to in effect  
20 bolster privacy regulation because fines were too low  
21 and ineffective cannot be made any longer.

22 So really, now, you have effective  
23 sanctions, so in mergers, in abuse-of-dominance cases,  
24 et cetera, we shouldn't use competition policy to  
25 punish and deter privacy breaches.

1           MR. HALPERT: I'd add one point with regard  
2 to big data and data protection. If we're taking  
3 about an incumbent that has a lot of personal data, it  
4 is difficult to open up that data in personally  
5 identifiable format to other competitors without  
6 having some data-protection measures in place. So  
7 there is some inherent tension here that's worth  
8 considering as we move into the pure antitrust  
9 analysis of this sort of problem, and I just wanted to  
10 raise that as something to think about.

11           MR. STEVENSON: Thank you very much. Three,  
12 two, one, we're out of time. So please join me in  
13 thanking our panelists.

14           (Applause.)

15           (End of Panel 5.)

16           (Hearing concluded at 4:59 p.m.)

17

18

19

20

21

22

23

24

25

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

CERTIFICATE OF REPORTER

I, Linda Metcalf, do hereby certify that the foregoing proceedings were digitally recorded by me and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, not financially or otherwise interested in the outcome in the action.

s/Linda Metcalf  
LINDA METCALF, CER  
Court Reporter