FEDERAL TRADE COMMISSION

COMPETITION AND CONSUMER PROTECTION
IN THE 21ST CENTURY

Thursday, November 6, 2018
9:00 a.m.

American University
Washington College of Law
4300 Nebraska Avenue, N.W.
Washington, D.C.
FEDERAL TRADE COMMISSION

INDEX

PAGE:

1 Welcome and Introductory Remarks 3

2 Perspectives on Data Policy 5

8 Former Enforcers Perspective: Where Do We Go From Here? What is Right, Wrong or Indeterminate about Data Policy? 72
PROCEEDINGS

WELCOME AND INTRODUCTORY REMARKS

MS. AMBROGI: Good morning, everyone, and welcome back to the third and final day of the FTC’s hearing here at American University Washington College of Law. We want to extend our thanks to AU for being such gracious hosts over the last few days and also thank you to our participants in today’s hearing and to those who have joined us in person or on the webcast.

So the first day of the hearing really laid the groundwork for how to think about the economics and business of big data. Yesterday, we delved into the specific factors to consider when conducting an antitrust analysis of markets involving data, including a focus on online advertising, as well as the impact on privacy regulations on competition and innovation.

Today, we are going to take a step back and with a couple of great panels ask some broader questions about where antitrust enforcers, policymakers, and other stakeholders should go from here.

I will conclude with our final disclaimer that this event is being photographed and webcast with
huge thanks to our tech team, and by participating in this event, you are agreeing that your image or what you say may be posted at ftc.gov or one of the FTC’s social media sites. We have given this disclaimer every day. It is a privacy disclaimer, so it is also relevant to what we have been discussing.

Thanks, and let’s go to our first panel, Perspective on Data Policy, moderated by Peggy Bayer Femenella, of the FTC’s Bureau of Competition.

MS. FEMENELLA: Thank you, Katie.
PERSPECTIVES ON DATA POLICY

MS. FEMENELLA: Good morning. Our first session today will offer various perspectives on data policy. We continue to navigate a challenging topic and strive to develop appropriate policy. Hearing from multiple viewpoints provides an important framework. To lead this valuable discussion, we are privileged to have representatives from a variety of uniquely relevant organizations.

Our panelists will share their views regarding the intersection of big data, privacy, and competition, and will offer potential legal, regulatory, and policy next steps to address important data policy needs. The panelists will each start with a prepared statement and then I will pose some questions for discussion.

Also, for anyone in the audience that would like to ask a question, there will be someone from the FTC walking around with comment cards. So please just go ahead and write your question on the comment card and it will be collected for the panel.

Now, before we begin, I want to briefly introduce our panelists. First, we have Allie Bohm, who is Policy Counsel at Public Knowledge. Public Knowledge is a public interest advocacy organization...
that promotes freedom of expression and open internet
and access to affordable communication tools and
creative works.

Next, we have Ramsi Woodcock. Ramsi is an
Assistant Professor of Law at the University of
Kentucky College of Law whose research focuses on
consequences of the information age for the antitrust
treatment of personalized pricing, dynamic pricing,
and advertising. He also has a secondary appointment
as Assistant Professor of Management at the Gatton
College of Business and Economics.

Katie McInnis is our third panelist. Katie
serves as policy counsel on privacy and technology
issues for Consumers Union, the advocacy division of
Consumer Reports. Her work focuses on technology and
the consumer rights to privacy, security, control, and
transparency.

Next we have Eric Null. Eric is Senior
Policy Counsel at New America’s Open Technology
Institute. He has worked on consumer privacy issues,
such as children’s privacy and broadband privacy, as
well as telecom issues, like net neutrality and
universal service fund.

And, finally, we have Tom Lenard, who is
Senior Fellow and President Emeritus at the Technology
Policy Institute where he works on privacy and competition issues.

So we will go ahead and get started. Allie, you can go ahead and begin our discussion, please.

MS. BOHM: Thank you. Thanks for having me today.

It has become virtually impossible to participate in society without revealing our personal information. Most essential entertaining and useful services demand personal data that are then used to build detailed profiles of us and to deliver targeted advertising.

Service providers follow us around the internet scooping up -- and across devices, scooping up more and more data to come up with more precise ways to sell us products. Consumers are dissatisfied with this state of affairs. Some find it abusive that privacy is the price to pay to participate in modern society. Some find it frustrating to be paying twice, once with their data and once with their dollars. And nearly all are outraged by data breaches, hacks, revelations of corporate and state surveillance, and other social and political scandals.

Consumers in the United States want more control over our personal information and we demand
privacy protection. It is clear that the status quo is not working and I think that is likely part of why the FTC is having these hearings today.

So what are some solutions? Some advocates have argued for stronger and more creative antitrust enforcement. In fact, some have said that is the solution. It is Public Knowledge’s view that while antitrust has a role to play in protecting competition and consumers’ privacy in the digital age, it alone is woefully insufficient.

Here is why. First, competition could incentivize companies to differentiate by innovating in privacy protections. However, it could just as easily promote more aggressive data collection in order to give companies more competitive edge.

Second, any settlement after an investigation or any consent decree as part of a merger approval can only be a primary tool for protecting privacy so long as it is enforced on an ongoing basis which would require substantial FTC resources. I probably do not need to tell the people in this room that the FTC often prefers structural remedies, such as asset divestiture, rather than remedies that make it have to monitor companies on an ongoing basis.
Third, antitrust may just turn one privacy offender monopolist into several smaller privacy offenders offending competitors, none of whom have sufficient market power to be considered dominant and to fall under antitrust enforcement going forward.

Fourth, the consequences and impacts of many privacy violations are the same regardless of the size of the company involved, and in most cases, antitrust simply cannot get involved if it is a nondominant player.

It is also not clear that the FTC can step in when it comes to traditional backward-looking antitrust enforcement. As this audience likely knows, single firm conduct is typically only a violation of antitrust law to the extent that it unreasonably restrains competition. Despite antitrust’s focus on consumer welfare, it will not typically address negligent or risky behavior by dominant firms even when that behavior harms consumers.

So what can the FTC do? Narrowly, in antitrust land, the FTC should use antitrust enforcement to encourage nonprice competition, including competition based on different levels of privacy protection. Antitrust should recognize that one of the harms of market dominance may be the
ability to coerce consumers to provide more personal information in return for essential or unavoidable services. In addition, the possession of data could be considered as a potential barrier to entry during merger review, even when the merger would not otherwise have significant vertical or horizontal competitive effects.

The FTC could also use its UDAP authority through case-by-case adjudication to figure out whether third-party trackers on -- or I should say trackers on third-party websites are deceptive when they track folks all around the internet without those individuals' knowledge or consent.

The FTC could also conduct a 6(b) study of how platforms are using data and how their data affects competition. The advantage of a 6(b) study is that it results in a published report. So if it turns out, as Public Knowledge postulates, that antitrust is not entirely the solution to the problems of competition and privacy and big data, there will actually be a record to help build other solutions.

Finally, the FTC should advocate with Congress for passage of a comprehensive privacy law that imbues the agency with much-needed resources and with rulemaking authority. This is not a novel idea.
Even during the golden age of antitrust enforcement in the 20th century, antitrust was never seen as enough on its own. The same period that saw robust antitrust enforcement also saw the first wave of consumer protection laws.

I am happy to go into detail about what Public Knowledge would like to see in any comprehensive privacy legislation during the Q&A.

As a final thought, my organization strongly supports competition, but competition is not always a per se good. So for example, there is not enough competition in the pharmaceutical industry and prices are way too high. But that does not mean that we want Joe Schmoe on the street selling fake drugs. He might be able to sell them more cheaply than you sell real drugs and it might drive down prices, but the costs to society of having fake drugs on the market are not costs that, we as a country, want to bear. And that is -- and the role of regulation is to keep bad actors, like Joe Schmoe, off of the market.

I think the same thing can be said in privacy land and in data and big data land. We do not want nefarious actors doing things that we, as a society, would not want with our data, and the role of regulators is to keep that from happening.
So I appreciate the opportunity to be here and I look forward to discussing more during the Q&A.

MS. FEMENELLA: Thank you, Allie.

Ramsi, if you would like to go ahead and give your prepared statement?

MR. WOODCOCK: Thank you. It is great to be here.

We need to focus more in antitrust on issues surrounding the exploitation of data than we have so far and perhaps shift the focus away a little bit from antitrust issues surrounding the extraction of data, because that may well give us a sense of the way forward here that is very different from what has been put on the table so far.

So data allows firms to know more about their customers and thereby to extract more value from them. It allows them to tailor prices to their customers through personalized pricing. It allows them to raise prices when market demand surges as part of dynamic pricing, which is spread over the last 10 to 15 years from one side of the economy to the other, from Disney World now dynamically pricing access to its parks, to Broadway shows dynamically pricing tickets, to Amazon dynamically pricing hundreds of thousands of products and changing those prices...
hundreds of times per day.

Through targeted advertising, it also allows firms to increase the willingness of consumers to pay for products that, absent the advertising, they would not, in fact, prefer. So this exploitative effect of data should be the key focus for antitrust going forward.

The reason why it has not been the key focus for antitrust is because the exploitation of data is not in itself anticompetitive, and it is a long-standing rule in antitrust that a firm’s decision to raise prices in and of itself is not an antitrust violation. So on a superficial level, it looks like there is no way for antitrust to respond to this vastly increased bargaining power that firms now have, vis-a-vis, consumers as a result of the fact that they now know so much more about them.

It turns out, however, if you look a little bit more closely, that there is a very important role for antitrust to play in this story. Because while data allows firms to increase the amount of value that they extract from consumers, competition places a ceiling on that level of value that firms can extract from consumers.

If you think about -- take any market
whether it is concentrated or not, competitive or monopolized, if you think about what data does, it allows firms to figure out how much they can raise prices without alienating their consumers. So it allows them to extract more value from consumers for any given level of competition in the market.

However, the more competitive a market is, the less the firm can raise prices and so the less value it can extract. What that means is that the data revolution gives antitrust enforcers a mandate to deconcentrate markets, to expand competition across the board, because only by doing that can we place a ceiling on the amount of value that firms can extract from consumers through data and lower that ceiling to offset the increase in value that data is allowing firms to take from consumers.

What that means is while antitrust cannot attack individual exploitive practices as anticompetitive because they are not in themselves anticompetitive, the raising of price is not in itself anticompetitive, by ramping up enforcement against genuinely anticompetitive practices, practices that result in markets being more concentrated than they need to be, antitrust enforcers can create the competitive environment that makes it harder for firms
to successfully exploit the data advantage that they have gained over the past few years.

So what this means, in other words, is that data gives us a reason to go back to the enforcement levels of the ‘60s and ‘70s. It gives us a reason to challenge every horizontal merger. It gives us a reason to challenge every vertical merger. It gives us a reason to pursue firms based purely on their size as was done quite commonly in the ‘60s and ‘70s in everything but name.

And once we do that, that lessens the need for sort of the complex considerations regarding limiting data extraction and privacy that so far have preoccupied us. Because if the data is no longer useful for exploitation purposes, maybe we can be less concerned about its extraction to begin with.

Thank you.

MS. FEMENELLA: Thank you, Ramsi.

Katie will now give her statement.

MS. MCINNIS: Thanks, Peggy. And thank you to the FTC for hosting these hearings and giving us the opportunity to speak to you here today.

So there is an obvious power imbalance between consumers and companies and there has been for years. But, unfortunately, the amount of data that
companies can now mine, collect, and use on consumers has exacerbated this imbalance. We, at Consumer Reports, are working hard to make sure that that imbalance is ameliorated to the extent that we can help, but consumers really do need a federal data privacy law that will give them the protections that they need and really deserve.

This data protection law would have reasonable data minimization that is tied to context and consumer preferences. We would also like permission for extraneous data collection, along with detailed information about data security practices, strong data security practices, ways for consumers to get access to their information, and robust enforcement. And, of course, any federal data privacy law should include increased resources and rulemaking authority for the FTC.

In addition, we think that a data privacy law would not preempt stronger state laws. It should create a floor and not a ceiling. Our states are laboratories of democracy and we do not think that we should prevent innovation on the state level to further protect their consumers in the ways that they see fit. Consumer Reports is trying to help consumers evaluate the privacy and security choices that are
presented to them, but, unfortunately, privacy policies are way too long, full of legalese and often buried on websites and not easy for consumers to evaluate one against another.

For this reason, Consumer Reports introduced the digital standard in March of 2017. This is our understanding of what is best as far as data security and privacy practices for products and services for consumers. We started evaluating products under this standard this year. We have seen a huge response both from companies and from consumers.

However, this effort depends on transparency, which is one reason why we are pushing for any kind of privacy law to include requirement of SEC-type disclosures from companies as far as their data practices and privacy policies. That way these policies could be read by those who are already reading them and they would have more information. Regulators, policymakers, reporters, and groups like Consumer Reports would be able to fully understand what companies are doing with consumer information.

We also support any effort to get to this endpoint, but we understand that, at some point, consumers just also need in-the-moment disclosures as well, which is why we appreciate this layered
approach. However, we will get into more of the
nuances of what we think about the data privacy law
today in this panel.

Thank you.

MS. FEMENELLA: Thank you, Katie.

Now, Eric will give his statement.

MR. NULL: Good morning, everyone. Thank you to the FTC and thank you to Peggy for putting this together.

Since I am a third consumer group to speak, I will try to not repeat things and perhaps can keep this relatively short.

But, you know, OTI, Open Technology Institute, my organization, has been thinking a lot recently, particularly about the level of competition,particularly amongst social media platforms, but also just among big tech platforms in general and thinking about ways that we can sort of chip away at that a little bit without necessarily doing something like breaking up a company, for instance.

But essentially we are seeing this growth of a couple large social media tech companies, who are able to more and more collect data and be able to, for lack of better word, exploit that data. And what ends up happening or what has happened is basically they
end up crowding out smaller companies that could
sprout up or, you know, companies start with the idea
that they would get bought up by one of the bigger
players.
And so you end up having fewer and fewer
companies with more and more data and then you end up creating this system, particularly for businesses and minority -- communities of color, low-income businesses that feel forced to use these platforms to reach their customers and they cannot necessarily expand beyond those because there are not really many other options.
So obviously, there are a lot of ways we can go forward with this, antitrust is one of those ways. I am not an antitrust expert, so my understanding of competition is probably a little less nuanced than some of my other panelists and some of the people in this room. So, you know, obviously, one of the more extreme ones is to break up companies, which as I have said, you know, we do not necessarily support, certainly not at this time, particularly because how would that work, how would you break it up. It is not like AT&T where you can break it up into long distance and local. So there are a lot of questions there that may end up making things -- there are lot of things
there that might end up making things worse than better.

Another option is to make behavioral advertising less appealing and less profitable. That way smaller companies that have less data and have access to less data could compete on more a level playing field with contextual advertising or subscription models or something like that. That is also not necessarily something we would like to do, at least in the immediate term. The option that my organization prefers, which my director spoke about yesterday on the revenues panel, is emphasizing data portability which allows users to port their data between services to allow a competitive service to take advantage of the data that someone has already put into the world on another platform and just move it to that platform and be able to target advertising based on that information. But then also platform interoperability, which is not to be confused with data interoperability, which is about making sure that data can be -- you know, there is like a standard for the data to be ported.

Platform interoperability is more about being able to use any platform and communicate with anyone else on any other platform. We have an example
of this right now in the fediverse, which has services like Mastodon and PeerTube, where they basically just -- they all interact with each other and then you can communicate across the platforms. We obviously do not see that today because companies are trending toward locking down their services and their data rather than opening them up.

I will just say a couple things about privacy, substantive privacy rights. You know, obviously, a lot of us are thinking about and talking about comprehensive privacy legislation, but also what the FTC can do without any new legislation.

The three things I just want to emphasize right now is data minimization, which Katie covered, the right to control and access and delete and modify data; and then enforcement of -- you know, strong enforcement of whatever privacy regime we end up coming up with. And I will leave it at that.

MS. FEMENELLA: Thank you, Eric.

And, now, Tom will go ahead and give his statement.

MR. LENARD: Thank you, Peggy, and thanks to the FTC for inviting me to speak. I think this has been -- I have watched some of the hearings in the last couple of days and I think they have really been
very good.

I want to make two related points. The first one may seem obvious, but probably needs to be said fairly often, is that policymakers need to do the necessary analysis to make sure that privacy policies actually do produce positive net benefits. And as part of that -- and this is particularly important for the FTC given its mission -- is assessing the competitive implications of privacy policies.

The competition policies generally have a strong economic underpinning and while there is now more debate on the subject, I think there is still a fairly widespread consensus that antitrust should deter activities that are harmful to consumers. But privacy is behind antitrust in terms of incorporating economics and evaluating the relevant tradeoffs and doing the analysis necessary to show that the proposed policies have benefits greater than costs and therefore actually do improve consumer welfare.

So for example, we know that collecting and analyzing large amounts of data is the basis of much of the innovation that has occurred on the internet over the past 20 years. Many of the benefits of data are realized when data are reused, combined with other data sets, used to answer new questions that were not
anticipated at the time the data were collected. But
many privacy policies target those practices and
restrict the collection use and sharing and retention
of data. We need to more rigorously assess the cost
and benefits of those policies to know whether they
actually make consumers better off.

If markets are operating properly, if there
is no significant market failure, there is no reason
for the Government to intervene in the first place.
We know that consumers willingly exchange personal
information for the resulting benefits despite what
they say in surveys. And we also know that firms
suffer quite significant financial repercussions when
they experience data breaches, which gives them an
incentive to put the necessary resources or certainly
a lot of resources into avoiding them.

So are these factors consistent with the
notion that the market for privacy is subject to
serious market failure? That is a question that needs
to be analyzed in more detail.

We know the consumers routinely exchange
their information without reading and understanding
privacy notices suggesting that most consumers do not
find it rational to spend the time and effort to do
so. Is this consistent with various transparency
notice and choice proposals?

Perhaps, most importantly, I think this needs to be the starting point really of most analyses, we need to define more clearly the privacy harms that are being targeted and that we want to avoid. The recent informational injury workshop that the FTC held and the summary memo that the BE and BCP staff wrote, I think were a good step in that direction. And this is critically important because benefits, by definition, consist of a reduction in harms. If there are no harms there can be no benefits, only costs. And while we all know that identifying harms is difficult, it is not enough to simply assert that collecting information or sharing information with third parties is harmful, per se.

Now, on the competition front, I think more economic analysis would help illuminate the tension that exists between privacy regulation and competition. Some of these issues were discussed in the last two days. There is quite a bit of theory and evidence that many privacy regulations favor large incumbents and make entry by new firms more difficult. I think this is borne out by the early experience with the GDPR, which imposes large up-front compliance costs and appears to benefit the large tech platforms,
and we see smaller companies pulling out of the EU in reaction to the costs of complying. And on the consumer side it was referred to yesterday as well -- there is a paper by Campbell, Goldfarb and Tucker, which is a different argument, but it kind of reinforces the other argument, focusing on transactions costs shows that the opt-in consent regimes favor large firms that offer a range of services because it is easier, there is, in the economist jargon, smaller transactions costs for consumers to go through the procedures once with a large company offering range of services than with many smaller companies.

And, increasingly, regulations, such as the CCPA, are being adopted that make it more difficult for data to be sold or otherwise transferred to third parties, and regulations like these can also be a barrier to entry because firms entering a market often need data on characteristics and preferences of potential customers before they can get started and collect data of their own from actual customers.

These regulations can also raise costs for data brokers, which also can be a barrier to entry. Data brokers can realize economies of scale and scope and data that can benefit entrants and other smaller
companies that cannot realize those economies on their own.

And, finally, in addition, making it difficult to share with third parties can lead companies to integrate with other companies in a way that would be otherwise inefficient and, therefore, may lead to antitrust concerns.

Thank you.

MS. FEMENELLA: Thank you, Tom. And thank you, everyone, for your statements.

Let me go ahead and jump into questions now. I would like your thoughts on whether data-driven pricing threatens consumer welfare directly by enabling firms to extract more surplus from consumers for any given level of market power, and if so, whether there is anything that the antitrust laws can or should do about that?

Ramsi, would you like to lead us off on responding?

MR. WOODCOCK: Yes. I think that the answer to that question is yes. I mean, it really flows from sort of basic economics involving differentiated products. I mean, think about an airline in the midst of a price war in a highly competitive market, it is still able to charge more to first class passengers
than to economy passengers, and that is because products are differentiated, if only in brand name, which consumers care about, however irrational that might be for them to do so. And the result is that every firm always has a little bit of power over price.

And as a result, the more data firms have about their customers, the more they are able to exploit that data to raise prices for those customers who turn out to be willing to pay more regardless of how competitive the market is.

That is why I like to think about data as really presenting a sort of second dimension of market power where the first is determined by the level of competition in the market and the second dimension is determined by the level of information you have about your customers.

MR. LENARD: I think the -- I mean, the question basically is about price discrimination, which also was covered by several people in the previous couple of days. It is true that price discrimination transfers some, and in the case of perfect price discrimination all, of the surplus from consumers to producers. But price discrimination also is efficient in terms of increasing overall welfare.
when it increases the total output of the market.

So particularly in the case of products with high fixed costs and low marginal costs -- you know, one example is airlines, airline tickets -- price discrimination may be necessary for the good to be produced at all. If airlines could not price discriminate, we would have -- it is not likely we would not have any airlines, but we would have fewer flights.

Lots of goods in the digital economy and the information economy, like apps and software, also have high fixed and lower or even zero marginal costs, and price discrimination may, in fact, be essential for those goods to be produced.

Also, price discrimination, I think contrary to what sometimes is said, I think price discrimination generally favors lower-income consumers because it really involves charging prices based on a consumer’s ability to pay. A consumer’s ability to pay is, in general, related -- charging on the basis of a consumer’s willingness to pay. A consumer’s willingness to pay, in general, is correlated with their ability to pay, which implies that price discrimination otherwise -- other things being equal, is going to charge lower prices to lower-income
consumers who otherwise might be unwilling or even unable to purchase the product.

MS. MCINNIS: If I could just jump in.

First of all, this use of first-degree price discrimination or dynamic pricing is a harm to the consumer, first of all, because it is -- these decisions are made about the consumer based on data collection, which they did not agree to, and is rather privacy-invasive.

Second of all, they do not have any sort of transparency for how these prices were calculated. And we have seen in markets that this is not necessarily -- [3459] different pricing of different products is not necessarily a good result.

We recently did a report on car insurance pricing and found that people in a lower-income community were being charged more for their car insurance because they used a proxy of a zip code and decided they were more at risk based only on their zip code, which happened to be a minority majority neighborhood. So this is not necessarily good.

Second of all, having dynamic pricing diminishes the consumer’s share of the consumer surplus, which is not helpful either. And third of all, consumers are unable to compare prices which is
one of the ways that we have competitive market. If I
cannot compare one price of an airline ticket to
another because they are all raised because I have
been searching for airline prices to New York all day,
that does not allow me to actually choose which
airline would serve me best.

Thanks.

MR. WOODCOCK: Well, just to put a finer
point on that, Katie, and sort of in conversation with
Tom here a little bit, price discrimination, when it
is imperfect, can benefit consumers. It can bring
consumers into the market who otherwise would be
priced out of the market at a higher uniform price.
But as price discrimination becomes more perfect --
and that is where we are heading; that is the whole
point of the data economy, to personalize the price
and get it up to willingness to pay -- the consumer’s
benefit from that goes to zero.

So while it is correct that price
discrimination -- perfect price discrimination is
efficient, all of the efficiency gains go to the
producer and zero go to consumers. And under
antitrust, we operate under a consumer welfare
standard, not a total welfare standard. So a policy
that drives consumer welfare to zero is not an
antitrust interest.

Just to put it in intuitive terms, think about the hypothetical disadvantaged consumer who is brought into the market through personalized pricing. If they are charged a price exactly equal to their willingness to pay, which is where we are going with personalized pricing, by definition, by economic definition, they are indifferent between having access to that product and not. They get nothing from it.

MS. BOHM: So I feel like I need a mic drop to follow Ramsi. So I am a little intimidated. But I do want to add one thing about sort of who is benefitting, and price discrimination, you know, probably means lower-income folks can afford to buy things. I think the data sort of demonstrate that that is not always true.

So Katie gave us one example that I think is really good. Here is another one. The Wall Street Journal recently did a study of price discrimination and they were looking at Staples and if you were in various zip codes what it would cost to buy various products there. They found, unsurprisingly, that if you lived closer to a rival store, you were getting lower prices on Staples.com. That is rational, right? They want you to buy online from them instead of going
to the Office Depot down the street.

It also turns out that the people who lived near the rival stores tended to be higher-income. So folks who lived further from stores, who were getting higher prices, were also poorer folks. So I think there is not only everything Ramsi said, but there is also a real risk of further entrenching the economic divide in this country because the people who do live close to stores tend to be the people who live in wealthier areas where stores want to come.

MS. FEMENELLA: So switching gears a little bit, do you think businesses will start competing or, in fact, are already competing for customers based on consumer privacy choices? And if so, how do you think this will affect privacy practices? Eric, do you want to start us off?

MR. NULL: I am going to let Katie actually attempt that first.

MS. MCINNIS: So we do see rise in the use of consumer privacy-protective practices, such as use of ad blockers is about to reach 30 percent this year, more consumers have been interested in the use of a virtual private network since Congress rolled back the broadband privacy rule that the FCC passed in late 2016. But we also here at Consumer Reports, where we
released the digital standard, we have seen a great
response from businesses where they responded within
the next few days after we introduced the standard to
see what kind of criteria we were using and when we
would be rolling that out for all of the products to
have connectivity.

But we have seen consumers have been really
interested in our evaluations of product space and
privacy and security because they do not have the
tools available to evaluate these products. So I
think that we are only going to see a rise in
consumers being interested in products that preserve
their privacy and data security.

We have seen a great use of home products
like Alexa and Google Home and the rest, but, at the
same time, consumers are concerned about how much
these products are listening to them. So they are
interested in these accessibility and these
convenience products, but they are also really, really
interested in how much privacy their privacy is
protected. But, unfortunately, they just have not had
the tools to evaluate these products.

So that is one reason why Consumer Reports
has entered into this process of evaluating privacy
and security, but also another reason why consumers
need a data privacy law in order to even the playing field a little bit here. But we have also seen that consumers are asking more from their companies. We have seen a drop-off of membership for Facebook after the Cambridge Analytica scandal. So breaches of consumer data do have a repercussion for the company, especially in consumer trust.

So we see that this will only continue to rise as consumers become more and more aware of how much they are being tracked and how much their on and offline activities are being correlated in order to make decisions about them and their buying practices.

MR. NULL: Yeah, I will just jump in here really quick. I think there are certainly lots of privacy-protective services out there, SpiderOak for cloud services, ProtonMail and FastMail, you know, Signal for communications, DuckDuckGo for searching, and so I think we will probably continue to see these privacy-protective competitors sprout up.

As I mentioned before, it is sort of hard for a privacy-protective social media network to sprout up for a variety of reasons. But I think in terms of whether -- you know, how could we get more competition, consumers -- I heard this a long time ago that consumers are not very good at internalizing,
like, potential harm in the future. People still
smoke even though there is a potential that they might
get lung cancer when they are older.

And the same thing is sort of true with
privacy where if you are looking at a free service
that you have to give a bunch of data to and you are
looking at another service where you pay $10 a month
or $5 a month or something, but it protects you from
privacy intrusions by ideally not collecting data
about you or collecting a very minimal amount of data,
it is a lot harder for a consumer to look at that and
say, well, that is worth X number of dollars to me,
even though in the future if you go with the free
compány and they get breached and information gets
leaked about you, it may lead to identity theft. It
may lead to a variety of other harms, you know,
secrets about you getting leaked that you do not want
to know, you do not want the world to know.

And so it is hard for consumers to actually
make that comparison. I think maybe there is just a
way to be more explicit about it and maybe the
advertising for these privacy-protective companies has
to be clearer about that. I do not know. But I
think, as a consumer, me in particular, like it is
hard to part with dollars out of my wallet when I can
just go with a free service and sort of pretend that there are no potential harms that could come from that collection.

MR. WOODCOCK: If I can jump in. It does seem like there is a serious market failure here when it comes to privacy. But it also seems like consumers recognize that not being completely private with their data does benefit them, which is why I have tended to focus more on sort of increased competition in markets as being a potential solution to this problem rather than increased privacy protections. Because in very competitive markets, data cannot be used against consumers so much, but firms still have access to that data and they can use it to do the sort of beneficial things with data that we all love, you know, computers being able to serve us without us having to ask them, and so on.

MR. NULL: And I will just add that I have done a lot of work in -- well, a lot of us have done a lot of work in broadband privacy, and one thing that we have not seen in the ISP market is -- market, if you can call it that -- is no one competes on privacy even in the wireless market where people tend to think that is, at least, a somewhat more healthy competitive landscape, and I have found that interesting in terms
of, you know, if you have a competitive market, you will probably get some providers that will compete on privacy. But we do not see that in the ISP market.

MS. FEMENELLA: What is the role of interoperability in addressing big data, privacy, and competition? Allie, do you want to start us off?

MS. BOHM: Sure. So this will be relatively brief. Interoperability is super important, and it can be helpful for allowing new players to enter the market and for individuals to leave privacy-violative services. So if, for example, Facebook were interoperable with this fantasy, really, privacy-protective social network, you might actually go over there if you could still message your Facebook friends from there because you could leave without sacrificing your contacts or your content from Facebook. But it is not a panacea.

So email is a great example of something that is fully interoperable. Yet, the vast majority of people are on Gmail, you know, whether that is because it has more storage or it is the best product. I do not know. But people have gravitated there and given it a disproportionate market share. So I think there is a risk that even if we have full interoperability, we are still going to have certain
players emerge as dominant and it is not actually going to solve all of the problems in this space.

MR. NULL: So, I mean, I mentioned this in my opening and so there are -- so separating out data portability and data interoperability, data portability is a much easier question to answer. I think it is easier to sort of -- for lack of better term, legislate it from the top down and say in some way that there has to be some kind of data portability option. I mean, we see it in the GDPR and we see it in the California law.

And it is really -- the benefit there is to make sure that users, if they want to, can move their data from one service to another without having to reestablish their entire social lives on a different service and the provider -- the social network provider gets the benefit of all that data to then be able to target that person and potentially other people.

So portability is relatively straightforward. There are some thorny issues there. Partially, something that we may get to is, you know, what data should you be allowed to move between services, what data that shouldn’t you be allowed to move, should that data be deleted from the social
network that you are moving it from? There is lots of
in-the-weeds sort of questions that come with that.

But it is the platform interoperability that
is a much tougher issue. So a lot of it has to do
with protecting privacy versus allowing
interoperability and portability to a certain extent,
depending on what you are porting out. My director,
Kevin Bankston, talked about this yesterday. You
know, what about your social graph? Can you port that
data out? Is that something that should be
interoperable for the user to be able to move? And so
what you are talking about now is data about other
people, rather than just data about you, and so that
gets into the question of what data can you move.

And Professor Pasquale said, you know -- or
put forth the argument that whatever data I upload, I
can then also move between services, and I think that
is a decent starting point, but I do not know if that
necessarily gets to the full issue because obviously
Facebook makes a lot of inferences about us and uses
data in a lot of different ways that we do not
necessarily know. That is why I couple the data
portability and interoperability issues with the right
to control access and amend and delete your data so
you can actually see what they have, and then that way
you can make an informed decision about whether you
want to port all of that data or not.

Unfortunately, what we have seen recently
because of Cambridge Analytica and some other issues,
that social network providers are actually locking
down their data more than they are opening it up. And
that is in part due to the public’s reaction to
Cambridge Analytica, which was swift and intense. And
so that was partially due to the ability of users to
port their social graph and be able to use that
information elsewhere. And that is something that
Facebook fixed many years ago and then is actually now
becoming more locked down as a result of the Cambridge
Analytical scandal coming to light.

So, yeah, I think that data portability and
interoperability are -- portability is low-hanging
fruit sort of, say; interoperability is a much more
difficult issue. But I think they all should be --
both of them should be considered going forward in
terms of FTC hearings and fact-finding and that sort
of stuff. So thanks.

MR. LENARD: So I think if you look at
something like portability, you need to start out by
asking yourself what is the purpose of portability.
The purpose of portability is presumably to lower
switching costs. So whether it is a good idea or not really is dependent on the context. So for example, I think for most consumer-facing applications, retail -- you know, the fact that I might not port all my data in my ten years of purchase history from Amazon to somebody else does not prevent me from buying from another retailer. There is really no switching costs to doing that.

So the value -- I am sure there will be substantial costs in a portability requirement and I think the benefits would probably be minimal. There might be other apps where -- there may be other situations where it is important. If you had a medical app where there was a history of medical treatment or various things was important, then, you know, that would be a barrier to switching.

In terms of something like Facebook, I do not even quite understand how it would work. I mean, you could port yourself, but you cannot port all your friends. And if you are not going to be able to port all your friends, I do not see why --

MR. NULL: I mean, you can port your friends. That was the Cambridge Analytica scandal.

MR. LENARD: You are not porting them to another social network --
MR. NULL: You are sharing their information.

MS. BOHM: Well, that is actually how most of the social networks started was they said, hey, can we have access to your email account and we are going to send emails to all your friends asking them to join this social network. And I think one of the tricky questions with data portability is, do I get to port my social graph? And if it is Facebook, if I am friends with Eric, is that Eric’s data that we are friends or is it my data and do I get to port it? And that is one of the tricky questions where portability is going to sort of be effective from a competition-enhancing perspective. So I think you are stepping on a very live question here.

MR. NULL: Sorry to --

MR. LENARD: I suspect -- I mean, I do not know obviously, but I suspect a lot of people would be unhappy if they found themselves ported without their permission.

MS. BOHM: I think you are right. I think that is one of the issues.

(Laughter.)

MR. NULL: Well, you are talking about signing other people up for news services.
MR. LENARD: Well, you are porting all of their -- put aside Cambridge Analytica, just as a common practice to say, well, I want -- you know, it just seems to me there are problems with it.

MR. WOODCOCK: I just wanted to point out that even if we solve -- sort of data portability is about solving the kind of economies of scale problem with sort of data-intensive businesses --

MR. LENARD: I think it is about reducing switching costs.

MR. WOODCOCK: Right. But by reducing switching costs, you sort of make these markets contestable in some sense, right. Because, you know, there certainly are huge economies of scale associated with data. I mean, that is why Gmail is the dominant email platform because the more you know -- the more users you have and the more you know about them, the more you are able to sort of filter out spam and protect your email servers, and that is a big part of why Gmail has gotten so big.

So portability is sort of -- it will not necessarily deconcentrate a market because you still have those economies of scale and data, but it will make the markets more contestable. So that if some other platform comes along and it is willing to offer
something better, everybody can sort of switch and
port their data to the other platform and now you will
have a new platform, which will be the dominant firm
in the market until another one comes along.

But even if we solve that problem, that does
not eliminate the exploitation problem. I mean,
whether the market is contestable or not or whether it
is even highly competitive or not as a result of
portability, whichever firms have your data can use
it, can exploit it, to help the companies that you buy
from charge you higher prices. So there are two
separate issues at work here, I think.

MR. NULL: I am actually fascinated by Tom’s
argument that the benefits would not necessarily
outweigh the costs of data portability and that
switching costs is the only benefit -- or reducing
switching costs is the only benefit. I mean, I think
the other benefit is that the new social network also
gets access to a treasure trove of data on you that
they can now use to target you with ads. Like that is
the business model, right? A free service -- free,
quote, unquote, a free service where you get targeted
with ads.

And a startup social media company has
access to basically no data. I mean, they have access
to public data, but they do not have access to, like, all my posts going back 12 years now on Facebook unless I am able to move that data with me. And so you do that with X number of people, assuming X is enough to make the business model sustainable, you know, you have a viable competitor in the social media market then.

So I think switching costs is obviously a big one, but right now switching costs are basically irrelevant because there is no one to switch to.

MS. MCINNIS: So we have been --

MR. LENARD: Let me just say one thing. I have not done the analysis and I have not seen anybody else who has done a general analysis of what a portability requirement -- what the costs and benefits of a portability requirement would be. But I do not think -- it is probably straightforward and I do not think -- I think it is probably quite context-specific. It depends on which -- you know, what things you are going to port.

MS. MCINNIS: Yes, that dovetails nicely actually to what I was going to say, which is we have just been discussing portability of social media data, which I think is a little more of a life question, like Allie stated. But there are other kinds of data
that consumers should be able to port in order to reap consumer benefits, such as being able to port my financial data to a new broker so that they can offer me better tools and services based on past financial history.

Part of the -- one of the letter of HIPAA is portability, right? Like this law from over 20 years ago is a law that acknowledged that we had to have portability of your data in some means in order to have some sort of protections around your medical data. So I think the portability has to be included, in some way, in this data privacy law that we create. And I think this kind of really tough issue that we have touched here today is a good reason why the FTC should be viewed with rulemaking authority under this law so that they can figure out some of these thornier issues and we do not have to bog down Congress while they figure out some issues at hand.

MS. FEMENELLA: So let’s flesh out a little bit of what you guys have all been discussing. So you have addressed this a little bit, but does data actually affect the bargaining power of consumers, vis-a-vis, firms, and if so, how? And does it give the firms an advantage or could it actually help consumers fight back, leading to no net effect?
Ramsi, do you want to start off?

MR. WOODCOCK: Well, I think it is sort of an interesting question whether data could be -- so I think it is fairly obvious that data enhances the bargaining power of firms because it lets them know more about -- it lets them guess -- better guess what the sort of maximum willingness to pay of consumers is for products. But it is an interesting question whether consumers could somehow benefit from data as well.

Because just as there is a ton of data about consumers out there, firms now have much more data about their own costs than they ever did before. And this has actually been underway far longer than sort of the -- the consumer data extraction side has been underway. For decades now, firms have had sort of hyper-accurate information about each product that is being scanned at the checkout at supermarkets, and so on. They have automated their supply chains. They have much better sense of what their costs are. That is all data that consumers, in theory, could use in bargaining with firms.

Because once -- that is sort of the flip side, the equivalent of the consumer’s maximum willingness to pay is the firm’s minimum willingness...
to accept, if you will, in terms of prices. And if there were some way for consumers to leverage that information and use it against firms, then they could at least offset their loss and bargaining power associated with the data that is being extracted from them.

The main challenge that is faced in making that happen, though, is that consumers are disorganized relative to firms. They are atomistic and so they are not able to sort of -- and they do not have any access to the data. They are not -- unlike firms which are sort of observing consumers, consumers are not out there observing firms’ cost levels directly. So we would need some way, first, to sort of force firms to give up their data on their costs and then we would need a way to sort of centralize that information and use it in a way that consumers can exploit to hold out for lower prices from firms.

It strikes me that absent some kind of legislative solution that was to do that, consumers are going to be sort of permanently at a bargaining disadvantage in the data economy.

MS. BOHM: So I tend to agree with Ramsi on this one. I think pervasive data collection allows firms to develop detailed profiles about their
customers and their customers’ willingness to pay, which allows for personalized pricing strategies and manipulations of consumer choice, placing very, very, very persuasive ads for particular consumers. Companies can do this at scale because of machine learning and algorithms. Individuals cannot.

You know, it may be true that I can now plug into the internet and say, oh, I need a new shower curtain, what does it cost at Target, what does it cost at Bed, Bath and Beyond, and, you know, price compare. But that has limited utility, particularly when, as Katie pointed out, we are often seeing personalized prices or lately, if you are searching on Amazon, sort of the sponsored things go to the top. I was trying to find a particular cell phone case and I could not even find it until I put in the brand name and, like, exactly what it was. It did not show up in just like a search for “cell phone case.”

So if you are not seeing products because of what algorithms you are doing and you are not seeing particular prices, you really just do not have the information, as an individual, to leverage data against the companies.

MS. MCINNIS: Yeah, I think data portability is -- and data access is going to be hopefully a huge
bargaining chip for consumers in the future. I do not think that we really have that ability now.

I do think that the emerging automated car market will kind of necessitate that we answer some of these questions, right? Who has access and who has ownership of my driving data? In the past, that was you and if you had an agreement with Progressive or some other car insurance company that put a black box in your car. In the future, we are going to want to have access to this car driving data in order to make sure that our automated driving systems are as safe as possible. But at the same time, it reveals a lot of sensitive information about users.

Hopefully, we want this situation between consumers and companies to be more even, and I think that as consumers have better acknowledgment of their data and where they are creating it that, hopefully, they will be able to take more ownership under a new data privacy law and use this as bargaining chip.

I also think that -- although we discussed it a lot in the last question, I do not want to dip back in. I do think that it is a huge deal for consumers to be able to avoid lock-in with any one service. Consumers should be able to shop for whatever group respects their choices the most. And I
think that is one of the huge issues that came out of
the Equifax breach, is that consumers felt the
immediate effect of this breach. Equifax really did
not in the long run and, yet, they have no
relationship with Equifax at all.

So having some sense that you have control
over your data is obviously an emerging thing in the
U.S. And I think that, in the future, we are going to
see more and more consumers leveraging their data in
order to get a better product or service or hopefully
maybe even change dynamics -- change the kind of
services that were being offered in the first place.

MS. FEMENELLA: So going back to the
portability issue, do you think there should be a fee
associated with being able to port your own data?

MS. MCINNIS: I would say no. I think the
question of, like, ownership rights over data is kind
of a thorny one because it is somewhat of a mutual
process between you and whatever service you are
interacting with. However, I think that as we saw,
again, with Equifax breach of having to protect your
data and to pay a fee for it was hugely onerous to
consumers.

I also think that having a fee associated
with the portability of your data could possibly
prevent the change from one service to another. So it
could affect some consumers more than others.

In addition, I think that this already is
asking for consumers to make a pretty deliberative
step to take their data and move it to another. I do
not think you should put a further burden on that
change.

MR. NULL: So I agree that consumers should
not have to pay to port their data. The question of
whether the receiving provider should have to pay is
an interesting one that I have not really thought a
lot about, and what that would mean and how much is a
reasonable amount to charge for that sort of thing. I
could certainly see exorbitant fees being charged and,
therefore, companies do not want to pay for the data,
but also could see some potential benefits there as
well.

Good question, though. Interesting. I will
continue thinking about that.

MS. MCINNIS: Yeah, I guess that brings up
an interesting solution. I guess it would be better
if companies could organize with each other what sort
of level playing field they can figure out so that
consumers do not have to pay a fee or -- and that is
actually a more, I think, conducive situation to
realize in an equitable outcome.

MS. BOHM: So I feel like I am sort of bristling a little bit at this question. So my organization comes from the philosophical, if not -- you know, certainly not the legal position, but the philosophical position that you own your own data. So if I own this information about myself that I have given over to a company, let’s call it Facebook right now, and Facebook has been able to profit off of that data -- so they already gotten a lot of value out of it, it does not seem fair to me that I would then have to pay to get my data back.

I am not even sure about another company having to pay for me to be able to then bring my data over and use that other company because it seems to me that Facebook has already gotten a whole lot of value out of this thing that I philosophically, if not legally, should own. I do not think -- sort of the philosophical ownership is not a controversial idea that Public Knowledge dreamed up. I mean, if you heard Mark Zuckerberg testify back in April over and over again, you own your own data, we believe that you own your own data, which is a really interesting thing to hear from him.

So I do think that there is increasing
consensus in that space from that sort of philosophical underpinning, and if that is the underpinning, I just do not see how fees get involved.

MR. LENARD: Let me just -- I mean, I agree this ownership question is obviously a difficult question. But if you analogize it like what was just done in terms of you paid for the service with your data -- let’s, for example, say, well, you paid for the service with money, does that mean it is still your money?

MS. MCINNIS: Well, I think that is a false comparison because data is dynamic and you are always creating it and there is always future ways that data can be used, right? Like that is one reason why companies want to make sure that they have such a large network in order to then extract the amount of data and then use data for future purposes. I do not think that a lot of us could have anticipated the kind of growth of a lot of the properties that we gave data to in the early days of the internet and how they would use it in the future.

There is also that -- yeah, I just do not think that those are comparable things. But I do understand that the payment idea maybe ruffles that a little bit.
MS. FEMENELLA: Does data soften traditional innovation-based arguments against antitrust enforcement by ensuring that firms are able to extract greater profits from less concentrated markets and, therefore, to maintain R&D spending despite increased competition in their markets?

Katie, do you want to respond to that?

MS. MCINNIS: Sure. I do not think the framing here is exactly correct. I think sound antitrust enforcement is conducive to innovation and data does not soften that argument. A lot of startups use their employee’s data in order to get into the market. That kind of R&D spending is already encapsulated in the startup market that we already have.

In addition, you see that there is further concentration on markets even with great use of data from employees or small data sets. The goal now for a lot of startups is to be bought by one of the big ones, which is not necessarily creating a full market where there is a lot of competition, but rather further centralization and that is still including data.

In addition, I think that the R&D spending - like the R&D spending here, if it is going to be
based on data, that is a much smaller cost, I think, than it used to be in the past. You can create a product like Fitbit based -- in the beginning, based on employee data, which was not necessarily -- that does not change any kind of competition or antitrust arguments in my opinion.

MR. WOODCOCK: I think the jury is still out on whether sort of concentration is more conducive to innovation or competition is more conducive to innovation.

But if we accept the sort of argument, which I think antitrust has largely accepted since the late '70s, that some amount of sort of monopoly power or concentration can be conducive to innovation because it allows firms more profits which they can invest in research and development, if we accept that and we also accept that sort of the decline in antitrust enforcement that took place starting in the '80s and which has really persisted until this day was largely a response to the view that maybe concentration is good for innovation and so we do not want to deny firms too much in the way of profits, the fact that data now allows firms to extract more profits from consumers, to extract more value from consumers than they did before should raise an important question
about whether, therefore, sort of the balance that was
struck by antitrust starting in the ‘80s has been
upset.

Now, perhaps we have too much profit going
to firms. And if we were to ramp up antitrust
enforcement and increase competition in markets, if
that were to drive prices down a bit, that would
simply offset the increase in prices, brought about by
data and just return us to the sort of balance between
consumer and producer interest that was struck
starting in the ‘80s.

So if we think that this sort of balance
that was struck starting in the ‘80s was actually
conducive to -- you know, sort of struck the right
balance between funding innovation and benefitting
consumers, all we would be doing by ramping up
enforcement would be returning to that balance that
both sides of the equation seem to agree was the right
balance. So I think that, ultimately, data does sort
of reduce the power of arguments that increased
antitrust enforcement would harm innovation.

MR. LENARD: I mean, I agree with Ramsi that
I think the economics literature has not -- you know,
there is no clearance to the question of what type of
market structure is most conducive to innovation. We
do have -- I mean, in the tech economy, you know, we
have -- and it is not only in that, but it is
certainly a more prominent -- perhaps a more prominent
characteristic of the tech economy is you have these
kind of winner-take-all markets and races to be -- you
know, competition for the market. Certainly, one can
argue that those are quite conducive to innovation. I
mean, it ranges from Microsoft to Google to Facebook
and it is, to a significant extent, because there are
large significant network effects and other economies
of scale.

And when you have technologies like this
where there are large network effects and economies of
scale you do not want to -- you know, if you make the
market more, quote, competitive or more atomistic, for
want of a better word, you may very well lose those
network effects and those network effects and
economies of scale benefit consumers.

MS. FEMENELLA: Going back to the price
discrimination point addressed earlier, can you talk
about the difference between old-fashioned price
discrimination, like charging more for flights closer
to the date of departure, versus the use of modern
data-driven price discrimination?

MR. WOODCOCK: So would you just repeat the
question? I want to make sure that I have a good handle on it.

MS. FEMENELLA: Sure. We are trying to understand the difference in price discrimination now because of the amount of data that is available. So before, maybe they were price discriminating based on the timing of when you bought your flight. So if you needed a last-minute flight, you paid more money. But, now, with all of the data that is available, they can price discriminate differently not just at the last minute.

MR. WOODCOCK: So one of the things that data has allowed is sort of firms to exploit new information about changes in demand in a way that they could not in the past. So if you think about in the past a firm might set one price and then after a month or two would look at that price again and have more information about how many orders were coming in, for example, and then change the price in response, today, a firm can do that almost in realtime because it has information about -- for example, it might be getting information through its website about how many consumers are coming to the website and it has a history associated with that that tells it that when the number of consumers come to a website goes up,
1 generally, the willingness to pay goes up as well.
2 And firms could have even tested that by varying price
3 in response to the factors to come up with a robust
4 result.
5 What that means is firms now can change
6 prices much more quickly than output would be able to
7 adjust. So if you think about going back to the firm
8 that had to wait a month before it could change
9 prices, it might be an industry in which production
10 can also be varied over that timescale. And as a
11 result of that, today, when prices change, supply is
12 generally fixed for firms. So when they raise prices
13 it is basically acting as a rationer. It is rationing
14 access to a good that is in fixed supply. So it is
15 able to use the price increase to extract more value
16 from firms.
17 In the past, when the demand went up over
18 that time period, it would simply sell out of the
19 good. And from an efficiency perspective, it does not
20 matter whether the good sells out or whether the good
21 is rationed based on price because supply does not
22 change over those periods. But from a distributional
23 perspective, there is a big difference because when
24 price goes up, consumers end up paying more for the
25 good than they would if the good had just sold out
under sort of the old regime in which firms could not vary price.

MS. BOHM: So I will take it out of the economics for a second. There is sort of the old-fashioned dynamic pricing, the airplane tickets gets more expensive as we get closer to the flight. That is true if you are buying the plane ticket from Dupont Circle or from Anacostia. It does not care who you are; it cares about the day that you are buying the ticket. I think many of us find that less problematic.

Then there is sort of the dynamic pricing we are seeing today, which is there is all this data about me as an individual. And so I live in Dupont Circle and I am a lawyer and they have all of this data and they say, oh, she really wants to go to New York, so I bet she will pay more for the ticket, whereas, you know, someone else who -- you know, maybe it is because they can pay less and, you know, some of us might think that that is actually a good outcome. But maybe it is because, you know, they have sort of figured out by data profiling this person that they do not really want to go on this trip, you know, or they do not -- you know, whatever the conditions are, and they are given a cheaper ticket.
And it is not -- it is personalized pricing now -- personalized dynamic pricing as distinguished from sort of the price increases for everyone because we are closer to the time of the flight, since we are using airplanes.

MR. LENARD: Yeah, I think -- this is kind of following up on that. I think it is -- at least conceptually, it is important to distinguish between two things. One is I think what is normally called price discrimination, which is basically based on differences in demand and differences in willingness to pay. It is also the basis for public utility -- for efficient public utility price regulation and what is called Ramsey pricing.

So that is one element that is based -- now, the thing about filling empty airline seats is really a different phenomenon. It is just, you know, you get close to the flight and half the plane is empty and you lower the price to try to sell those tickets. That is really kind of a different phenomenon as is, for example, Uber surge pricing if there is a big increase in demand or whatever it is at 5:00 to rationally available Ubers, you know, they may raise the price. But that is different than price discrimination.
MR. WOODCOCK: I like to distinguish between
-- so I define dynamic pricing as really the adjusting
of price based on new information, whereas price
discrimination, which can happen dynamically in the
sense that it is going to involve charging different
prices at different times depending on who the
customer is, is pricing that is based on sort of prior
information about the profile of the consumer or group
of consumers who are coming to buy at that particular
time. I think that may be a useful way to distinguish
the phenomenon.

Because when you price discriminate, unless
everybody comes to buy at the same time, you are going
to be charging different prices at different times,
but you are doing something slightly different from
dynamic pricing, which is we are able to sort of
incorporate new information and change price in
realtime.

MR. LENARD: Well, I think price
discrimination is really based on differences in
demand elasticities and willingness to pay. I do not
know exactly what is now included in dynamic pricing.
But the other phenomenon is really based on what is a
disequilibrium in the market. There is either an
excess demand or an excess supply and the price is
moving to try to move towards equilibrium.

MS. FEMENELLA: So with our time left, we will switch gears a little bit. Many companies and NTIA have been calling for a risk-based approach to comprehensive privacy legislation that would base the rules and remedies on the sensitivity of the personal information involved and the risk associated with breach disclosure or misuse. What are your reactions to that approach?

Tom, do you want to start us off?

MR. LENARD: Sure. Well, obviously risk is an important element in the whole thing. I guess what I think any new approach needs to yield net benefits relative to the status quo. The status quo really is the current FTC approach of ex post case-by-case enforcement-based privacy regulation. And I think it is -- you know, obviously, there is disagreement about that. But I think it is a pretty good approach.

Since, as I said before, benefits by definition consist of a reduction in harms, you need to start out by identifying the harms you are aiming anything new at in order to get any estimate of benefits. If there are benefits, you need to assure that the benefits are sufficient to outweigh the costs.
There is another element in the -- I think there were two elements that I read that kind if stood out in the NTIA document. One was the risk-based approach and the other was what they call their focus on outcomes, that they want to focus on outcomes rather than dictate specific practices, which I think could be a good thing if what they mean is something like performance standard like in the environmental context. A performance standard would say, well, we are going to set the maximum level of pollution for a plant and let the plant figure out how to do that in the most cost-effective way. Well, that can be an efficient way to do it. And then the relevant outcome should be a reduction in privacy of harms.

But I think what the NTIA calls outcomes, I really think of as inputs. I mean, they call outcomes things like transparency, access, and control. I think they are really inputs and they are supposed to produce privacy benefits. But they do not really explain how that happens, how those inputs are going to produce privacy benefits, because they do not really talk about privacy harms.

MS. BOHM: So I want to build on Tom’s discussion of harms. So when I hear risk-based approach, I hear the industry saying, hey, we only
want to be held accountable for legally cognizable harms. That may sound great, but it is actually really hard in the case of privacy to prove legally cognizable harms. So it is usually like financial injury or physical injury. And, often, when it is financial loss, they are really, really hard to trace back to the source. Was your credit card number stolen because of Target’s breach or Home Depot’s breach or, I don’t know, Lord & Taylor’s breach, right, tracing it back.

Even if you could trace it back, often, your bank is going to pick up the damage so you are not going to have any financial loss. There is not going to be a legally recognizable harm. But there are number of harms that come from misuse of data, from data breach. There are a number of sort of nonlegally cognizable harms that we need to take into account.

So this can be embarrassment or reputational harms that jeopardize job or social opportunities. Those could be re-endangering a domestic violence victim when her data are accessed by her former stalker or her former abusive partner; that could be not having access to opportunities because the data said you should not be shown this particular ad for housing or this particular ad for senior management.
position. This could be informational harms, so, you know, the fragmented news, fake news. They could be things like Cambridge Analytica influencing people in the voting booth.

That is not to say that privacy legislation or regulations should solve all of these major societal problems. But it is to say that when we think about what harms we are addressing, we need to think really, really broadly about what the harms are.

Second of all, when we talk about sensitive/nonsensitive information -- so many, many folks, particularly our friends in industry, say, oh, you know, yes, yes, we want to protect privacy, but only for sensitive information. And by that they mean first and last name, credit card information, maybe your health status, maybe protected class status, but everything else should be fair game. And in today’s world, it is so trivial -- first of all, so-called nonsensitive information in the aggregate or even point by point can, in fact, reveal very sensitive information.

So take, for example, health status, often a sensitive category. So the fact that someone has cancer, probably sensitive, there are probably restrictions there. Shopping history, usually
nonsensitive. But if someone is shopping at Headcovers.com or TLCdirect, those are both websites that specialize almost exclusively in hats for chemotherapy patients. That information likely reveals health status and can be used as a very, very effective proxy to advertise based on or discriminate based on or sort of fill in the blank based on health status.

Also, nonsensitive information is often used for very sensitive purposes. So if you believe Cambridge Analytica, or for that matter, the Obama Campaign, which used very, very sophisticated -- I think I heard a presentation, do not hold me to the potato chip types -- where they had figured out whether you liked Cheetos or Doritos meant you were more likely to vote Democrat or Republican. No one is going to make your chip preference sensitive. But if it is being used to influence you in the voting booth, maybe it is sensitive.

So I would encourage, as we are thinking about privacy in the digital age, that the sensitive/nonsensitive distinction really in the age of big data no longer makes sense.

MS. MCINNIS: So I would just like to jump in on that. To take back to the NTIA’s risk-based
approach here, we disagree entirely with the framing. Consumers will always have privacy interest in their data. Once it is in the hands of another, they have an interest in how that data is used, possibly breached, and how it is later passed to another party.

So we would rather that the NTIA use more of a focus that we have seen in other privacy laws, like the Wiretap Act or the Video Privacy Protection Act, where the invasion of privacy was a de facto harm. We would suggest that that is the framing here for the NTIA, and that will be in our comments that we will submit tomorrow.

In addition, we really encourage a broad sense of what consumer privacy harm is. As Allie mentioned, it is really hard to trace back the consumer harm to one specific breach or another. But we do know that consumers experienced a large amount of financial and identity theft and reputational harm based on the huge number of breaches in the past few years, and we think a privacy law should recalculate the incentives for businesses so that they actually take into account consumer data privacy and protect the data that they have either been entrusted with or for whatever reason now have control over in order to make sure that consumer data privacy is respected just
as much as whatever other incentives that -- whatever
other priorities the business has.

Thanks.

MS. FEMENELLA: With our last two minutes,
does anyone want to have any last thoughts before we
end our panel?

MR. WOODCOCK: Sure. I think it is fairly
obvious that consumers are not in a position to make
sort of optimal choices about how their data is used.
It requires a level of knowledge that I think it is
unfair to require of individual consumers. And it is
also the case that data leads to efficiency benefits,
you know, things that consumers like.

So the question is whether if we cannot sort
of create a market-based solution for the problem of
extraction of data, perhaps we can create a
market-based solution for the problem of exploitation
of data for purposes of harming consumers. And one
way to do that would be to promote much more
competitive markets across the board in the economy
today than we currently have in my view.

MR. LENARD: To pick up on something else,
actually. There is -- really the data available on
privacy harms is really pretty inadequate. I mean,
even the most tangible types of privacy harms, like
identity theft, identity fraud, there is really not
very good data. There was a paper a year or so ago by
Josephine Wolff and Bill Lehr, which makes that point.
And having looked for the data over the years, it is
pretty sparse.

Both the FTC and the NTIA have said that
they want to promote research in these areas. So this
might be one thing to do.

MS. FEMENELLA: Well, thank you all for your
valuable insights and for being on the panel.

We will be taking a short break now, then
starting back again promptly at 10:45. Thank you.

(Applause.)
FORMER ENFORCERS PERSPECTIVE: WHERE DO WE GO FROM HERE? WHAT IS RIGHT, WRONG, OR INDETERMINATE ABOUT DATA POLICY?

MR. GILMAN: Welcome, everyone, for -- I do not want to say the last panel of these big data hearing, I will say the ultimate panel of these big data hearings. We have the former enforcer’s perspective. Where do we go from here? What is right, wrong, or indeterminate about data policy?

We have assembled a small, but very distinguished panel here to have a wide-ranging discussion of issues we have been covering these past two-and-a-half days, both looking at what has been done and what has been learned and also looking forward to data policy.

So let me just introduce, first of all, my colleague, Katie Ambrogi, who is, like me, from the FTC’s Office of Policy Planning. And then our panelists, Bill Baer is a partner at Arnold & Porter. Previously, he served as Acting Attorney General at the Department of justice, Assistant Attorney General for Antitrust Division at the DOJ, and Director of the Bureau of Competition at the FTC. Prior to that, he was Assistant General Counsel and Director of Congressional Relations and an Attorney Advisor to the
Chairman of the FTC.

Julie Brill is the Corporate Vice President and Deputy General Counsel for Global Privacy and Regulatory Affairs at Microsoft. Julie is a former Commissioner of the FTC, where she served from 2010 to 2016, and was widely recognized for her work on internet privacy and data security issues related to advertising and financial fraud. In 2015, she was named one of the top 50 Influencers on Big Data.

Maureen K. Ohlhausen is a former FTC Commissioner, serving that role from 2012 to 2018, and as Acting FTC Chairman from 2017 until May of this year. Before that, she was a partner at Wilkinson Barker Knauer, where she focused on FTC issues, including privacy, data protection, and cybersecurity. She previously served 11 additional years at the FTC, most recently, as the Director of Policy Planning where she led the FTC’s Internet Access Task Force. Before that, she worked at the U.S. Court of Appeals for the D.C. Circuit, serving as a law clerk for Judge David B. Sentelle and as a staff attorney. She has authored a variety of articles on competition law, privacy, and technology matters.

As we said in previous sessions, anybody just arriving, this is being photographed and recorded.
and transmitted as a webcast and an archive. And that is our notice about public use of your images and anything you might say. And we will collect question cards.

But, now, I want to turn it over to our panelists, each of whom will have brief opening remarks before we get into a more free-ranging discussions.

So let’s start with Bill Baer.

MR. BAER: Thank you. I am going to make very brief opening remarks because, in fact, the two former FTC officials to my left and right have actually been in that unique position of enforcing Section 5 of the FTC Act, which does bring together these issues of antitrust enforcement and consumer protection enforcement. But I would say -- and we will talk about this more, I think, as things go on -- I do think it is important analytically -- and the Commission has done a good job of this -- of separating what is an antitrust problem and what is a consumer protection problem where data privacy, security need to be addressed.

The competitive market can create these sort of externalities where competition is not taking into account certain costs to society and the consumers
from a lack of competition on privacy and data
security. And those are areas where I think the
Federal Trade Commission, and to a lesser extent
certain other regulatory agencies, have a unique
ability to influence how we think about it, how we
regulate it to the extent the authority exists, and
how the Executive Branch and the independent agencies
interact with Congress to make sure that we are
actually making sure that consumers are not bearing
unreasonable and inappropriate costs of competition in
these markets.

MR. GILMAN: Julie?

MS. BRILL: Well, it is great to be here.
Thank you to Bilal and to Dan and to Katie for
inviting me to speak about this incredibly interesting
issue.

What I thought I would do to begin just with
my opening remarks is to talk a little bit about one
of the questions that I have noticed was discussed and
interwoven in many of the conversations over the past
couple of days. And that is, are companies competing
on privacy and what does it mean to actually be
competing on privacy?

And in my last slightly over a year at
Microsoft, as well as my year serving as the head of a
major law firm’s global privacy and cybersecurity practice, from my perspective and my vantage point, I can say that companies are vigorously competing on privacy, but it might be in ways that might not be quite as intuitive or obvious to some individuals. So I would like to talk about that briefly.

So, first of all, from Microsoft’s perspective, you know, we are competing in many, many different types of markets, but if you want to break it down into two just for the moment, we serve -- obviously, we have a very large cloud business where we are providing services in the cloud to many other businesses and individuals. And in that context, our ability to protect data and to provide tools to our customers so that they can be compliant with privacy laws around the globe is a very important differentiator, a very important competitive aspect from what we do. Similarly, we differentiate with respect to our use of data for end users, for consumers.

So it is important to think about the actual business model that is involved and to think about what it is that entities are doing to differentiate themselves in terms of their data practices and their data policies.
I would like to drill into this a little bit more if I can. Let’s see if my slides did get loaded. There has been a lot of conversation, I think, about GDPR also over the last couple of days, and I have learned an awful lot about GDPR over the last couple years and I think it is important to truly understand what GDPR does do and actually what it does not do.

There is a meme that runs through Washington that GDPR requires consent for all sorts of data use and it is very heavily focused on a consent-based regime. That is actually not true at all. Indeed, for having been written seven years ago, it as a remarkably agile law. Is it perfect? No, by no means. No law is perfect. We could sit around and talk about any law, whether it is COPPA, FCRA, GLB, and we could talk about the need to update and modernize.

But GDPR for a law that is a baseline privacy law that governs all forms of data use for an entire continent and, actually, indeed for the entire globe in many respects is remarkably agile. And I will be getting to the competitive aspects of this in a moment, but I just wanted to lay some baseline understanding of the law.

There are three essential aspects to it:
Transparency, empowerment, and accountability. GDPR does require very robust disclosures to be provided to end users and also to be provided on behalf of processors to customers; that is, to a processor’s controllers. So I will not get into too much lingo here, hoping that everybody sort of understands some of the basic lingo and terminology that GDPR uses. But transparency is a very important aspect. Empowerment is also a very important aspect of GDPR. It provides all forms of control or many forms of control to end users for how they can understand their data and access their data and do things with their data, like delete it, like correct it, things like that. There is also a large emphasis on accountability under GDPR where companies need to make robust risk assessments about how they are using data and document that risk assessment.

The core data subject rights, which I am going to talk about in a moment -- I am getting signals that my time is up. I am going to ignore that if you do not mind. So thank you for letting me know, but I am going to keep going, as a former Commissioner often will do.

So there are some core rights at the heart of GDPR with respect to end users that many companies
needed to implement in order to get ready for GDPR. And as I was mentioning, these are some of the empowerment tools that are given to end users. It is the right to delete your data, to access your data, to port your data, to correct it, and to restrict the processing of it.

Now, in order to provide those kinds of rights at scale, it required a company like Microsoft, which is not only dealing with our own data, the data that we have and that we need to provide data subject rights with respect to, but also we needed to enable all of our customers to be able to comply with GDPR. So we were, in many ways, kind of at the fulcrum and a very important player in the entire ecosystem of driving compliance with GDPR.

With respect to our own data, what we have been able to do over the last five months or so since GDPR went online is we have been able to measure the extent to which individuals have accessed our tools for complying with GDPR. And what we discovered is that we have so far about eight million users around the globe who are interfacing with their data, who are actively looking at their data on our dashboard and potentially doing other things with it.

One of the important lessens that we have
learned from our data, from our dashboard and being able to analyze the number of individuals who are accessing their data, is that actually in the United States we have a lot of interest in individuals controlling their data, seeing what it is, and exercising some of their rights. Indeed, there are more individuals in the United States who are accessing their data than there are in all of Europe, which is a truly remarkable statistic.

So as of right now, again, about eight million users worldwide are accessing their data, and out of those, it is about two million Europeans and 2.9 or basically three million individuals in the United States.

So what does this say? This says that individuals deeply care about controlling their data. They want to have tools to be able to control their data. We have been able to provide that kind of information and those kinds of tools for them.

And does this indicate that we think that there is a space and appropriate activity with respect to a competitive play on privacy and providing these kinds of tools is a differentiator? Absolutely. For us, it absolutely is a differentiator. It kind of plays more, though -- I think if you poll the market
and the kind of studies that we do internally, it is not so much competition around privacy alone. It really -- I think privacy needs to be understood in a broader narrative around trust. And I think that companies are positioning themselves in terms of trusted players in the market. So privacy, security, providing other tools, for instance, accessibility, these all are part of a broader trust narrative on which companies are absolutely computing.

So why don’t I stop there, but I am sure we will pick up the conversation more broadly.

MR. GILMAN: Thank you.

Maureen?

MS. OHLHAUSEN: Well, thank you to the FTC for inviting me to participate today in this discussion with my fellow former enforcers, Bill Baer and Julie. And thanks to Dan for giving that nice introduction. He mentioned my long government service, but now I am enjoying some time off for good behavior.

(Laughter.)

MS. OHLHAUSEN: So I am sure the other panelists before us have described the tools that can pull useful information from the flood of data that we are enjoying these days and the tools that have great
potential to make our lives better and provide significant benefits for consumers and businesses and Government. But also I am sure they have discussed that these tools raise some privacy and other consumer protection concerns.

Now, data and big data can also be important factors in competitive markets. Although there are many facets of the interface between data and competition, in my limited time today, I want to touch briefly on just two points. The first one has been rarely discussed and the second one has been discussed much more frequently.

So the first point is about how competition can help address concerns that inaccurate big data analysis may harm some consumers. And my second point is about consumer data in a competition analysis.

So turning to my first point, many observers, including the FTC in its 2016 report called Big Data: A Tool for Inclusion or Exclusion, so many have raised concerns about the effect of potential inaccuracies in big data analysis that my harm low-income or disadvantaged or vulnerable consumers. And, indeed, although I agree that big data can provide many benefits, it is simply a tool. Like all tools, it has its strength and its weaknesses and it can be
misleading and wrongly applied.

For example, data sets, though large, may not represent the real world. And also there is the multiple comparison problem or comparisons problems where researchers discover irrelevant statistical correlations that do not reveal anything useful about actual causation.

Now, concerns about the effects of inaccurate consumer data are legitimate and I have long supported frameworks like the Fair Credit Reporting Act that give consumers insight into data used to make important decisions about them and the chance to correct it. But regarding broader concerns about big data itself harming disadvantaged consumers, policymakers need to evaluate such concerns in the larger context of the market and the economic forces companies face.

Businesses have strong incentives to seek accurate information about consumers, whatever tool they may use. Indeed, they use big data specifically to increase accuracy and our competition expertise suggests that if one company draws incorrect conclusions about consumers and, therefore, misses opportunities to serve them, competitors with a better analysis will strive to fill the gap. Thus, big data...
analytics combined with the competitive market may help provide low-income and other disadvantaged consumers access to improve competitive offering.

Now, my second point is about the role of consumer data in an antitrust analysis. And this is not a new concept for U.S. antitrust agencies. The agencies have analyzed consumer data in the context of numerous merger reviews, such as in the 2009 DOJ review of the Microsoft and Yahoo joint venture to combine portions of their online search and search advertising technology. There are also court decisions resolving private antitrust actions that evaluated data as a commercial good, particularly consumer credit data.

So these agency actions and court decisions demonstrate that acquisitions or conduct implicating consumer data can be examined under traditional antitrust laws. And, also, as Julie has mentioned, companies are competing on the terms of privacy and trust.

Now, I have concerns, however, with proposals to use antitrust to stop mergers or acquisitions by data-rich companies simply to address privacy concerns, not where the transaction or the behavior reduces privacy as a nonprice attribute of
1 competition or where a merger would create undo power
2 in the market for consumer data.
3 Although concerns about the creation of
4 large data sets with personal information are not
5 baseless, attempting to address these concerns by
6 fitting them into an analytical rubric preoccupied
7 with economic efficiency creates more issues than it
8 solves. For example, it ignores the fact that
9 consolidation of data across business platforms often
10 creates significant efficiencies and gains in consumer
11 welfare.
12 Moreover, concerns about big data often
13 revolve around the concept that compilations of even
14 small and disconnected pieces of data, including data
15 previously gathered and held by different parties, may
16 be analyzed to reveal additional personal information
17 about individuals, which then may be used for new
18 purposes.
19 If the perceived privacy harm is the same,
20 however, it would be strange to treat data combined
21 through a merger differently from that compiled
22 piecemeal by another type of entity, such as a large
23 internet company, through its own connection and
24 analysis. And, furthermore, modifying the antitrust
25 laws to encompass privacy concerns does not
necessarily solve those privacy concerns, but instead
creates incentives for firms to alter deal structures
or enter alternative contractual relationships to take
advantage of this asymmetric treatment under the law.
And then, finally, this approach risks
reducing competition and innovation from new products
that the combined data may enable, making all
consumers worse off, even those who do not share the
same privacy preferences or who are willing to trade
some reduction in privacy for increased quality or new
offerings.
So in sum, competition law offers, at best,
a convoluted and indirect approach to addressing
privacy concerns in connection with big data. Now,
although consumer data can be part of an antitrust
analysis, the more direct route to protecting privacy
lies in the consumer protection laws.
So thank you, and I look forward to
discussion.
MR. GILMAN: Thank you.
So we have been having for a few days --
well, and for years -- discussions about the
competition side, the consumer protection side, and, I
mean, to some extent, the nexus between them as well
as the divide between them. I think we would like to
start with something that is more competition-focused. And this is a question for the entire panel, but maybe we will start with Bill Baer.

So for the three of you, during your tenure at the agencies, antitrust matters involving data crossed your desks, whether it was a recommendation to close or to take an enforcement action, open an investigation. In your view, what were one or two of the most salient matters involving data while you were at your agency? What challenges did they pose and what do you think about the resolution and what we might learn from the matter going forward?

MR. BAER: Thanks, Dan. Let me talk about a couple of matters that came across my desk. Indeed, the first day on the job in early 2013, I was presented with a representation to challenge a consummated merger, the Bizarrevoice-Power Reviews consummated merger. And while a lot of that challenge related to a merger to monopoly and the potential price effects from that, the fact that combining really the only two commercial enterprises that were going out to online retailers and selling a software product that would allow for product reviews to be compiled, basically centralized a whole lot of data, a whole lot of information in the hands of one firm, in
a market that looked like it was really combined to
those third parties that were offering that service to
retailers.

And while, as I said, the merger monopoly
pricing benefits that these companies unwisely
discussed at great length in their business merger
planning documents, evidence that we got and was
successfully introduced to the Northern District of
California in an effort successful to block that
merger, we did also allege and express concern about
whether or not the combination of these data sets
would create significant insurmountable barriers to
entry.

We looked at the network effects associated
with everybody basically going to one service. We
looked at how that made for very, very high switching
costs and how that would potentially enable
Bizarrevoice to have unusual market power over price
and stifle innovation and basically be in a position
to prevent -- foreclose entry.

Data also came up in a manner we did not
challenge. We looked very hard at Expedia-Orbitz, an
online travel service combination that occurred in
about 2014, ultimately concluding that there was
enough competition from the retail sites themselves,
airlines, hotels, rental cars, that consumers actually had options. And that there was not going to be a unique set of data in the combined hands -- in the hands of a combined Expedia-Orbitz. So we issued a closing statement saying we just did not see a competitive effect.

I will say if you go back over the years, you know, looking at these issues has been something both agencies -- and I have been at both of them -- have done. You can go back to reservation systems back in the '80s. You can go back to the effort of Westlaw and Lexis to combine, a matter looked at by the DOJ some 20 years ago. Having unique ability to control information and access to information was both a price and a nonprice effect wherein the concerns tended to be the same, which is will there be pricing benefits, but also will there be an inability of other firms to enter or expand into the market because there is unique control over information, which, as I understand it, was part of the DOJ concern in the Westlaw-Lexis merger some 20 years ago.

MS. OHLHAUSEN: We have seen lots of mergers where data was part of the important collection of assets that the companies were trying to combine. We have had mergers involving things like real estate
title plans or fire insurance maps, and we do a
traditional or the agency did a -- while I was there,
did a traditional antitrust -- I cannot say “we”
amore -- did a traditional antitrust analysis, much
like Bill talked about. The agency would look at
whether data can be an important asset, is it unique,
is there some kind of barrier to entry that this
combination will create such that -- or market power
in this.

But, often, consumer data is easy to
replicate. It can be gathered easily. The FTC’s
Consumer Protection Bureau has done some important
studies on the prevalence of data brokers and the
large amounts of information that are available in the
market to purchase. So there really has not been a
case that I can think of where consumers’ data was
considered -- that the combination of that would
create some sort of competitive issue.

Now, when I was there and the Commission
looked at Facebook’s purchase of WhatsApp,
commentators did raise privacy concerns saying, well,
the WhatsApp data was collected under a certain set of
promises and
if Facebook combines it with its data, then those
promises may be violated.
But I saw that as a privacy issue. And what the Commission did there was the head of the Bureau of Consumer Protection at the time issued a letter reminding the company that it needed to adhere to those promises to those consumers. If they did not, then I would see that as a fairly straightforward consumer protection issue.

Now, one of the other challenges, I think, about looking at data in an antitrust review is where we have found problems. The remedy has been to share the data more freely; to make a copy of the data set or the -- you know, of the title plant information, which is how you do title searches for real estate. And so importing a privacy analysis, you know, privacy concerns into this analysis, again, is a very awkward set because I do not think the people who are concerned about privacy say, well, what a great outcome, that data will be shared more freely, more widely.

MS. BRILL: So I would -- rather than talking about actual cases, just to distill out a little bit what we heard from Bill and Maureen, I would say that from a regulator’s perspective, there are two challenges to how you deal with whether it is mergers or other potentially anticompetitive practices.
dealing with data.

One is to determine whether the data is competitively significant. And as we have heard, you know, there is a lot of nuance to that issue. The first question I think that would need to be answered by the investigators and the regulators would be, do the parties at issue actually own or control the data or are they merely processing it for others? That seems to me to be a major gating issue, right. If you are not -- if you do not actually own or control the data, but are merely processing it for others and others are the ones who own and control it, then I think you have much less of a competitive problem potentially.

The second issue to determine whether data is competitively significant is whether it is a critical input or -- you know, assuming that you do own it. Unless you are actually marketing that data and there are two merger parties that are marketing the data, there will be some increase in concentration in that market for that particular type of data.

It is pretty -- in terms of whether data is a critical input, you know, it could happen, but I do not think we have seen that much of it at the FTC or elsewhere. And that is because even if a party kind
of has its own data and its own data set, the real
issue is what are they doing with that as an input in
the downstream market. If there is competition in
that downstream market, even if someone -- other
players do not have that critical input, but they are
able to compete, then you really have to think a
little bit more broadly about whether, indeed, you
have a competitively significant data set. And then,
of course, there is the issue of reasonable
substitutes.

So all of those are questions that go into
just the first challenge of determining whether or not
the data is competitively significant. Maureen
pointed out that that is just sort of the beginning.
Once you do have competitively significant data that
you want to address in the context of a case, then the
question becomes what is the remedy. And we are
hearing a lot more about calls for sharing data,
sharing data sets.

First, of course, you need to get over that
first hurdle of do you have competitively significant
data and in the world of multi-homing and consumers
placing their data in many, many different places and
also in a world where what is really significant is
not one data set, but the heterogeneity of data that
is used for AI. And, hopefully, we will get to that in a little bit.

It is really hard to say that in the area of consumer data you are going to have one single data set that is competitively significant. But once you get to this issue of needing to find a remedy, sharing data -- I think what I would urge regulators to think about is if you are automatically going to kind of go to that place -- well, first of all, are you breaking some of the sort of normal traditional U.S. rules about having some sort of legal basis to impose compulsory licensing? You know, do you have a refusal to deal. Are you in that world?

And then it is sort of at a bigger picture sort of policy level. If data gets shared pretty easily, you do have the concern that Maureen raised about potential privacy issues. But also more focused on the competitive effect, what does it mean if data gets shared pretty easily in terms of innovation by other parties? I mean, don’t we want to incentivize parties to really go out and compete with respect to some of these issues and with respect to driving innovations so that data becomes more competitively significant kind of across the ecosystem. Easy sharing, I think, actually would maybe inhibit that
kind of innovation.

So this issue of the remedies, assuming you are in a place where you do have competitively significant data and you do have a problem that needs to be addressed, I think the issues of remedies is actually the hardest of the issues as opposed to just sort of getting through that process of do we have a competitive problem to begin with.

MS. AMBROGI: Thanks, Julie. I think issues involving innovation and how to best support that are certainly things that we will keep discussing throughout this panel.

One other question specific to antitrust and big data, we are on the third day of our hearing on the intersection of big data, privacy, and competition, there has been a lot of discussion, and leading up to this point, ink spilled about this topic. We have heard about essential facilities, refusals to deal, price discrimination.

My question is simply, are the concerns about big data and antitrust warranted? And then a secondary question is, can a merger involving consumer data, if not a product or service for sale by horizontal competitors, but rather an input used by both merging parties give rise to an antitrust
violation, and if so, under what circumstances?

Maureen, would you like to start with that?

MS. OHLHAUSEN: Sure. So let me jump in first about the issue of the essential facilities argument and refusals to deal. I do not see why for big data that would be any different than the concerns and the analysis that we have in -- analysis involving other types of property. Like we have hashed this out quite a bit in intellectual properties and their concerns about forced sharing. I mean, intellectual properties really is just a kind of data, right? You know, how do you -- what is the formula, what is the code, something like that.

So I would definitely have concerns about saying well just because it is big data we are going to make it more likely to find an essential facilities argument or more likely to say there is a lot of refusal to deal that violates the antitrust laws. I mean, now that it is impossible, but I think it should be -- well, I am not a fan of the essential facilities doctrine really for the reasons that Julie mentioned. I think it suppresses investment and affects dynamic competition down the road.

And then in the merger context, I think it is theoretically possible that you could say consumer-
level data is such a key asset that the combination of
these two data sets could lead to market power in some
way. But I think there is a lot of reasons why it
seems less likely in this area than in other areas
where you found those combination of assets to be
problematic. It would have to -- again, the things
that Julie mentioned, that someone else could not
replicate it, that someone else could not -- there
could not be reasonable substitute for that data.

So I think that while it is theoretically
possible, I would be a little -- you know, it would be
interesting to see the first case that brings that.

MR. BAER: Let me pick up on that and focus,
Katie, on the question you raised about the input
market. And really, it is, again, traditional
antitrust analysis. If a merger is going to allow a
firm to, in some ways, create market power over a
critical input at the next level of competition, that
is a legitimate antitrust question, whether it
involves big data or not.

I mean, if you look back to a case I was
involved in 20 years ago, the Mylan case at the FTC,
that was actually single-firm behavior where a generic
firm basically was able to create market power in the
generic market for a number of generic products by
basically tying up the few suppliers of the key active
ingredient for a series of generics. And if you have
that situation involving data, I think you would
analyze it the same way the Commission did in the
Mylan case.

For me, switching over to a concluding point
Julie made, an interesting issue is the point Julie
raised about remedy. If you assume that you have in a
transaction, a merger, or an acquisition, the
potential for there to be control over whether you
call it an input or some sort of data that creates
market power, how do you remedy it? And if the answer
is not a license to somebody to give them the same
opportunity to compete -- and I understand the reasons
why Julie said that can be problematic -- what is the
answer? Is it simply seeking injunction against the
transaction?

MS. BRILL: It may be. So I am actually a
big believer that the antitrust tools that we have are
robust enough to deal with these issues, but I do
think it is important for the regulators to actually
understand the issue at hand. So as you may know or
keen observers of the FTC may know, I actually only --
even though I was a majority nonchair commissioner, I
did dissent, and when I dissent -- I dissented about
10, 15 times -- each one was in an antitrust matter, not a consumer protection matter. And each of my dissents was because I felt that the agency was not taking a robust enough position.

So my view has long been that the antitrust laws are actually -- we have some really good tools at our fingertips to deal with issues, including, I think, issues around data. My concern has long been that regulators -- when I was a regulator, my concern was, and my concern still is, that regulators really are not thinking creatively and using the tools that they have when they can be used.

So I do think that, as you said, the remedy might simply be that look, if the problem would be that sharing data raises the types of concerns that I talked about, maybe you do look at simply stopping the merger or doing some other creative things.

I think what I want to address though was sort of the predicate of your question which is that we have big data. I think it is important to think about, like, what is big data. So on some level, as Maureen, you know, the FTC has written a couple of reports about this. And it used to be that we talked about the three Vs, volume, velocity, and...

MS. OHLHAUSEN: Variety.
MS. BRILL: Variety. Thank you.

I think I would actually now in -- now that I am seeing things kind of on the ground and from the side of a tech company, I would say that, yes, there is volume; yes, there is velocity. Variety is super important, too. I would say that we would probably need to add in analysis. I cannot think of a V word for that. But algorithms are an incredibly important aspect of what is happening with respect to big data. And how the incredible increase in computing power that we now have, along with data science, marrying that up, really makes big data very significant when it comes to the issue of analysis.

But what is significant about big data is not just its bigness. So I think it is a misnomer to simply think about volume. So maybe I would subtract that V from what is competitively significant.

Instead, I think it is really important to be thinking about the actual nature of the data, the sensitivity, if we are thinking about privacy of the data, and its relevance to any particular algorithm or analysis at hand.

As you think about -- and you will be as regulators thinking about the competitive significance of big data in an AI world, I think you need to be
thinking more about heterogeneity than about bigness. In order to really have a robust AI technology, you need to have a variety of inputs. So that, to me, more than -- I mean, volume is important, but what I am hearing from data scientists, what I am hearing from technologists is that computing power, analysis, and variety heterogeneity are really what is key and then, also, of course to the extent that you have specialized issues at hand.

So to your point about like thinking about Mylan or thinking about medical data, thinking about roofing analyses we did back when Maureen and I were both on the Commission, that is highly specialized data and often that is very difficult to replicate. So I think as regulators move forward in an AI world where AI is going to provide so many benefits to society, but also needs to be dealt with appropriately and responsibly I think it is going to be important to be thinking about big data with a lot more subtlety than simply waving your hands and saying, you know, bigness is bad and we need to worry about large data sets.

MR. GILMAN: Here is a question that follows up maybe some on Julie’s slides, but also on both policy discussions and empirical work that were
presenting yesterday having to do with GDPR. Just to frame the question, I want to at least distinguish having real grounds for competition concerns on the one hand from having done a full-blown analysis on the other.

So both GDPR and the new California Consumer Privacy Act of 2018, which will go into effect in 2020, assuming that things go as charted, extend certain protections to consumers by imposing new responsibilities and, of course, costs on firms. Some smaller firms have said the compliance costs under GDPR are particularly burdensome for them. There is some preliminary evidence of GDPR’s impact on tech investment and some ad hoc reports of U.S. firms declining to do business in Europe.

And, of course, there is an interesting dynamic here when we are talking about tradeoff. We have both theoretical and empirical work suggesting -- I mean, in some ways, even large firms doing their darndest to be good actors can support standards policies that are very hard for smaller firms, innovators, entrants to meet.

And so here reflecting on provisions of GDPR, which does make some, but maybe not other, small firm/large firm distinctions, the California Act, do
compliance costs at some point or come to some point,
raise special concerns for innovation and competition?
Do these types of laws place, at least under some
circumstances, privacy rights or interests in tension
with competition or innovation?

MS. BRILL: Can I jump in on this one?

MR. GILMAN: Yes, mm-hmm.

MS. BRILL: Okay. So I will kick this off.

This is actually a really interesting, I believe
ultimately philosophical, question about the role of
any regulation and its competitive impact. I have
heard a lot of the discussion around GDPR as
potentially imposing competitive barriers for small
firms. I think we need to take a step back and really
think about regulation in any space and what it could
do to small players or players that are not ready to
comply.

Think about the Food and Drug Act. Think
about auto safety laws, Sarbanes-Oxley, even if I
daesay COPPA. All of these regimes are developed
whether it is because Congress or the European
Parliament or other policymakers decide that there
needs to be some boundaries placed around competition.
That is what regulation is. You are basically saying,
you know, you are no longer free to do anything you
want in this space; you are going to have to comply
with some rules.

And when those rules are put into place,
there is always disruption. I mean, I will focus
on -- you know, we could do the tobacco law, we could
do Food and Drug. The Food and Drug Act was probably
first enacted over a hundred years ago. You know,
suddenly, selling snake oil was not okay. Is that
disruptive? Yes, it is disruptive. Does it affect
competition? Sure. For snake oil purveyors, it
affected competition.

But what it means is that society has said
there are certain boundaries we are going to place and
these policies that we are now putting in place are
going to need to take a precedent over free rein in
that particular space in the economy.

Does GDPR do the same thing? Arguably, yes.
It does create boundaries around the way in which data
can be used. It creates rules and a system for
dealing with data and dealing with personal data.
Does this have a disruptive effect? Yes. Will the
effect be temporary or permanent? I think that is
going to be a big question. So some of the data that
was cited yesterday, four months' worth of one
particular type of data, I would really want to see
how that compares to what happened when other regulatory regimes were put in place in terms of investment.

But the real question is what is going to happen in the long term and whether the policy decision to impose those boundaries made sense over the long haul. And I would say that with respect to GDPR, what you are going to see is there will be a huge amount of procompetitive impact from laws like GDPR. I do not want to talk about California yet because I think we are still waiting to see what that will actually look like. It does not go into effect until 2020, I believe. And there may be some further amendments to it.

But from my perch, we have seen a lot of competition with respect to GDPR, particularly in the cloud space. That is, you know, you have cloud providers, Microsoft being one, that is informing -- we are informing our customers we will help you comply. We have a comparative advantage just as we do in security. We have the technologists. We have the ability to figure out how to keep your data secure. We have the ability to create tools for you to comply with GDPR. You come to the cloud and what will happen is you are free as a medium, small or even very, very
large company, you are free to focus on your business and you do not have to focus on building an infrastructure that we have built for you. And by the way, if you come to a place like Microsoft -- and we are not unique in this. I mean, there are other cloud providers that are doing this, too. If you come to us, you will be able to tell your consumers, your end users or your business customers that you are using a very trusted cloud provider and that they can trust where their data is going. So there is huge amounts of competition in this space.

So I would say that you know -- I could go on, but I want to let my fellow panelists address this issue. I would say the real issue is not is GDPR anticompetitive because it is hard for small players to comply. The real issue is, is there competition happening because of a regulatory regime being put in place. And the answer to that is yes. Will small players have difficulty? The truth is, from our perspective, the smallest of the players are actually the most agile and the new startups are actually more agile. They are able to build to GDPR.

The real difficulty that we are seeing with respect to some of our customers is medium-sized, older firms with legacy data systems, they are the
ones that are having the most difficulty. So it is really, again, not an issue of smallness versus bigness; it is an issue of agility or not agility; Newness, not newness. And then when you are looking at the competitive landscape, you really need to look at those entities that are providing these kinds of services and using kind of the Adam Smith philosophy of, you know, we have a comparative advantage, you go do your business, we will do our business, and we will help you do your business better.

MR. BAER: I agree with, as I often do, with most of what Julie had to say. And to the extent I elaborate, it is more of an elaboration than a difference.

We are talking about a competitive market where we talk about privacy and data security, big data, where the market may not work to reward the people who do the best job of providing data security or where the incentives may be to focus on sales and less on protecting your individual privacy rights. And so in that context as a political decision, there may well be, as Julie says, a need for governments to intervene not as antitrust enforcers but as regulators. We do not like to do that. We would prefer the market correct problems, but there are
situations. The environment is a good example, as is food, drug, and cosmetic safety. And so we intervene. We know that there is some cost to intervention. But, again, as Julie said, focusing, channeling through the regulatory process competitive incentives to make privacy more of a concern is a legitimate goal of government. It kind of trumps the presumption in favor of free markets if the harm or risk of harm is big enough.

But I think part of the reason you go there in this space is even though Microsoft may be extraordinary at providing protection for privacy and for security and is able to market that, it is very hard for the average consumer out there to know whether it is marketing material -- it is a privacy snake oil, right. So having GDPR, other kind of regulatory things, that set a floor in terms of what you must do, channel incentives, is actually a way to basically allow us to make decisions about a provider we are going to use, knowing there is some kind of privacy safety net out there. Without that, I think we are left out on the wilderness.

MS. OHLHAUSEN: So I agree with both Bill and Julie that any regulation is likely to have a competitive impact. That is one of the reasons why
the FTC has had this long history of robust competitive advocacy, where the agency has commented on regulations and their likely impact on competition. And it is across the board. It is not just privacy; it is health, dental hygienist, nurse practitioner, you know, the list goes on and on.

So I do not think the question is should there be regulation or no regulation. I think there is fairly wide agreement that privacy is an important value, it should be protected to a certain extent. I think the question for competition and innovation down the road is are you protecting it at the right level such that in the long run consumers are going to be better off. Because what is not necessarily capable of easy measurement is the innovation that is not happening because the use of data is being restricted too much.

I think that is a harder question, but often people raise the question about whether the European regulators are picking on American companies, right, the big American tech companies. And they say, no, we are. These just happened to be the companies that are in this space doing this. And I like to back up from that and ask the different question of why is it that the American companies have been the ones who have
really innovated in this space and created these new products or created these new markets and satisfied demands for consumers and lead to a whole lot of benefit in consumer innovation.

Now, that does not mean, oh, we should have no regulation. But I think we need to think about it at that level, also. Are we going to make innovation by using data too difficult, such that we are going -- consumers are going to miss out on some benefits down the road that could actually be well worth the exchange in how much their privacy and data is protected.

MS. AMBROGI: So we have a question from the floor, this one on the issue of potential remedies or solutions for some of the big data challenges. Could a broad data portability requirement offset some of the call or need for compulsory data-sharing as a remedy? And my annotation is, even if not an antitrust violation, would such a requirement increase competition by reducing switching costs?

MS. BRILL: So I will jump in on that. GDPR does have a portability requirement in it. And it is interesting when you sit back and think about that requirement to provide users with the ability to port their data. It is an empowerment tool. It is
focusing on privacy as control as opposed to the right
to be left alone. So it is a much more -- it is part
of a much more modern concept of privacy. But also
from, I think, a U.S. regulator’s perspective, it
looked a lot more like an antitrust or competition
element to GDPR.

So I actually think that the portability
requirement could have a lot of procompetitive
effects. Portability needs to be coupled, though,
with interoperability. Because it is one thing to
give a user their data; it is another thing for them
to be able to actually upload it and use it in a
functional way on another platform.

So one of the things that is happening right
now is that a couple of the very largest players,
Microsoft being one, Google being another, we are
working on an open source project to have sort of some
uniform standards by which data can be ported so that
it will truly be interoperable. So we are sort of
recognizing the call that the Europeans have made that
portability should help augment competition going
forward, but the only way it is really going to work
is if you have truly interoperable portability, and so
we are working on that through an open source project.

I do think it has promise. It is going to
take a little bit of time. If you go back to the dashboard that we showed you and all that interaction, eight million people looking at their data, correcting their data and whatnot, we are not seeing a lot of portability requests because like where would it go?

MR. GILMAN: What is the denominator?

MS. BRILL: Of what?

MR. GILMAN: Eight million over what?

MR. GILMAN: Millions and millions and millions. But, having said that, it as a very significant number. And I think what is especially significant is the relative proportionality or the relativity of that interest in control.

And this goes to something that I was going to comment on Maureen’s point about being careful when we develop laws in the United States about privacy and what the effect might be on innovation. I absolutely agree that that is something we need to take into consideration, but we also need to see that relative to the rest of the world, U.S. citizens seem to care an awful lot about privacy and that we need to sort of debunk this notion that privacy is of lesser importance than some of these other policy matters like innovation. It is very important.

MR. BAER: Just one quick add to that.
1 Relating to the degree of difficulty involved in
2 making portability work, you think about the
3 procompetitive benefits of the FCC rule some years ago
4 that allows you to tell your cell phone number from
5 one carrier to another. That is like wading into a
6 baby pool at a public swimming pool as compared to the
7 ten meter, you know, 3.0 degree of difficulty dive in
8 terms of finding a way to make sure that even though
9 you have portability, that you have functionality, you
10 know, interoperability with it.
11 So it is important, it is possible, but it
12 really requires a whole lot more than in a simpler
13 situation, a simpler world.
14 MS. BRILL: Right.
15 MS. OHLHAUSEN: And my only question there
16 is will consumers really use it. Will it achieve the
17 goal that the drafters -- you know, the people who
18 came up with requirement in GDPR want it to achieve?
19 And if it does not --
20 MS. BRILL: And I think that is a good
21 question.
22 MS. OHLHAUSEN: And if it does not, then
23 where do they go from there?
24 MS. BRILL: I think it is a great question,
25 but until we get to a place where it is functional or
interoperable, we will not know. So that is why we need -- you know, industry is really taking the lead here. We are working with the regulators in Europe and they are very pleased that we are moving forward with this open source project to help that, to see the reality to their dream of being able to truly port data. I think your analogy to the cell phone portability -- the cell phone number portability is a great one.

MR. BAER: You can use it.

(Laughter.)

MS. BRILL: I have.

MR. GILMAN: Can I maybe just follow up here a little bit. So it seems there is a consensus on the panel, not controversial. I think in the larger world, consumers have privacy interests that might be more or less well served by competition in one domain or another. There is a consensus that regulations can serve varied ends and will have some competitive impact. It does not mean that they are a net loss for consumers. There is a question what they are supposed to do and achieve, right, are they responding to some sort of significant and demonstrable market failures that would likely be durable. Can the harm be efficiently ameliorated?
So in one sense, of course, we have regulation here. In another sense, one model or another. The snake oil example seems to me to be instructive and maybe -- well, we have two out of three former FTC Commissioners here. FTC has done a lot of work on snake oil, nutrition marketing, dovetailing with FDA, calibrating regulations, and certain sorts of assurances in [10359] with the actual risks.

So how do we get at sort of not the question whether there are legitimate consumer concerns that something -- whether it is GDPR or FTC enforcement might respond to, but the magnitude and species of consumer harm we are addressing, the question whether the tool is well tailored to meet it. How do we assess, not the question whether there should be some floor or not, but where the heck it should be on the competition side or the consumer protection side?

MS. OHLHAUSEN: So let me offer just by analogy some of the things that have been really useful. You mentioned in the FDA context. So the FDA used to prohibit health claims about foods, essentially. And a cereal manufacturer felt that the science showing the benefits of having more fiber in your diet was so strong that they decided to push
the envelope and just go ahead with the advertising
in that.

The interesting thing that happened from
that -- and there is good FTC economic studies about
this -- is it led to this great increase in consumers
eating fiber in their diets because they -- the
competitive dynamic that happened of a company saying,
hey, you know, eat our cereal, it has fiber in it, and
consumers read their cereal boxes a lot more than they
read any government advice about diet, and then other
companies came in and they also introduced these
products.

So we need to be careful. And that showed,
actually, that that advertising restriction was
actually making consumers worse off, was suppressing
very useful information, and the products were not
appearing in the market because the companies could
not advertise them.

So I think that looking at some kind of
natural experiment like that through an economic
study, if possible -- I do not know whether it would
be looking at where innovation has happened in
products that use data in the U.S. versus other areas,
you know, trying to get at that, like where -- how do
we figure out what the right level is, because it is
very difficult to measure in the abstract what does not happen. You have to be able to compare it against something else.

So I do not know if it is possible to use an economic study that looked at where were data-intensive businesses developed, in what part of the world and then what their privacy regimes look like. I mean, the hard part is also there are a lot of different factors that go into business success. But just looking at other examples from other types of regulation, we have been able to do that kind of experiment.

MS. BRILL: I just want to throw one concept out here for us in the U.S. It is a somewhat foreign notion, but many people around the world do not think of privacy as simply an attribute of a product, but think of it as a fundamental right. I think to the extent that we have global players or companies that want to exist on a global market, you have to take into account the fact that the rest of the -- many regions around the world do not look at privacy and data use in the same way that we have traditionally looked at it.

Frankly, I think if you take a close look at the California law and what is going to be happening,
what is happening in other states, there is a paradigm shift in the way that privacy is being thought of. And I am not disagreeing with the question. I think it is an important question to ask what is the harm, but when you are thinking about harm, I think we are going to have to start looking at the harm to rights in addition to the harm to sort of what we more traditionally think of for individuals, because that is a way that privacy and data use is shifting around the globe.

MS. OHLHAUSEN: I mean, I think that is right and I think it is often articulated as a fundamental right outside the U.S. In the U.S., you know, it is a constitutional right. It is very important. But what --

MS. BRILL: Vis-a-vis, the Government. Vis-a-vis, the Government. Absolutely.

MS. OHLHAUSEN: Right, right. But, also, I mean rights, different rights need to be balanced. So one of the things that I -- one of the examples of taking these things too far that I heard, which I found so sad, was that in Japan after they had the tsunamis and the nuclear incident, some local groups -- and, you know, there were so many people in need -- said could we get a list of people who are
blind or disabled because they may be stranded and, you know, they cannot kind of get out on their own. And the answer they got was, well, no, because that would be a privacy violation. I think your right to, you know, receive life-saving services from the Government would need to be balanced against your privacy.

So I do not think that saying it is a fundamental right is the end of the discussion. I think it is important to realize that even fundamental rights can be in conflict with each other and need to be balanced.

MS. BRILL: So I agree with that. I was pointing it out because I think it is important to understand that if companies want to be competitive on the global stage, they need to either embrace this notion and understand what it means or not. But if you fail to embrace the notion that in many other very important markets, privacy is a fundamental right then you will not be able to effectively compete in those markets.

In terms of problematic issues that arise in the data space, I am aware of that circumstance you are describing and I think that that was a tragedy. Yet, we can find examples on the other end of the
spectrum where the failure to have broad-based privacy laws in the United States may have led to other major problems. We could look at the Cambridge Analytica scenario and the extent to which data was for a time very freely shared with third parties without consumers having control or understanding about it.

You know, had there been -- it is a question I am asking. I am not going to say that GDPR would have stopped that, but had there been some kind of baseline privacy legislation in the United States, the question is whether that type of activity would have been less likely to have happened or potentially less severe. And I think that is an important question to ask.

So I agree with you, we need to balance rights for sure. But we also need to understand where the rest of the world is going if we actually want to have companies that are competitive around the rest of the world.

MR. BAER: I think that is a great point and even if companies failed with a U.S. regimen, failed to adhere to it, the fact of FTC enforcement action and significant penalties, you would prefer it to be a deterrent at the front end. But at the back end, other companies will learn if sanctions are imposed.
MS. AMBROGI: So this is, in part, a question from the audience, but it touches on issues that Maureen and Julie have raised in terms of company analytics and the role for competition to provide a venue by which good analytics rise to the forefront.

So a two-part question, how can society operationalize Julie’s point about assessing the type of analysis that firms can do with their data, and then also for Maureen, what is the mechanism by which competition could produce accurate consumer-enhancing data analytics? Is there a role for enforcement or advocacy? And I know we have just a couple minutes.

MR. GILMAN: Yes. If everyone could just take a minute and then we are done.

MS. OHLHAUSEN: I will go first on the part addressed to me. Has anybody read the book, Moneyball? So Moneyball is all about using better analytics, using data more accurately to come to a better outcome, right. The Oakland A’s were terrible, so they hired a good data cruncher who had this idea that the way players were being chosen was not -- the data was not being used appropriately, other types of data.

So I do think that, you know, the same kind of thing can happen in a whole host of products. If
you have better analytics, you can target better
opportunities or make your product better. So I think
that is the common kind of thing. But I would
recommend Moneyball to anyone who wants to know one
particular application.

MS. BRILL: To the first part of the
question about how does one operationalize this issue,
I think it is really important. I am going to talk
about operationalizing it from the regulator’s
perspective. I always used to say that regulators
were about five or six years behind where technology
was. That has definitely accelerated. I think having
chief technology officers and having the technology
folks at the FTC and at other regulators has
definitely helped kind of shrink that gap. But even a
six-month gap is enormous these days because
technology is moving so quickly.

I would say that if you really want to
operationalize an analysis of how data is used in
these sort of more complex AI systems at the FTC,
which it has been doing through these hearings, really
needs to get a deep understanding of what is going on
today and what will likely be going in six months and
a year at some of the firms that are really thinking
about this deeply.
MR. GILMAN: Good, thanks. Well, in the seven seconds remaining, I think that all I can really do is thank our panel for your time and really the substance of your excellent contributions. And thank everyone watching here and over the webcast. Thank you very much. And we will see you at the next hearing.

(Applause.)

(Hearing adjourned.)
CERTIFICATE OF REPORTER

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

LINDA METCALF, CER
Court Reporter