PRICING ALGORITHMS & COLLUSION

Maurice Stucke

Maurice Stucke: Okay, let's get started. I'm going to talk today about three things. The first is algorithmic collusion. Second is "behavioral discrimination." Third is "frenemy." What does frenemy mean and where does the power reside in the digital economy?

How did this all start? I was on a sabbatical at the University of Oxford, and my colleague Ariel Ezrachi and I were ready to go to lunch. We were talking about how Amazon has increasingly dominated the retail sphere and how it relies on pricing algorithms. Next, we were talking about Walmart—this is before it acquired jet.com—and it too would likely rely on pricing algorithms. What would happen if these algorithms could collude with one another? That got us going, so we went back to Ariel's office and started mapping out these anticompetitive scenarios of algorithmic collusion.

But before we discuss algorithmic collusion, what are potential benefits and promise of the algorithm-driven economy? We have all heard about how algorithms can make markets more competitive by lowering our search cost. Now, instead of having to go to different stores you can go easily online, find the item that you want, and purchase it. The digital marketplace could lower your search cost, and increase transparency, so that you could easily find what different retailers are charging. This is still very much true.

It can also make it easier for companies to enter because now a company here in Knoxville could be selling to people all around the world.

We recognize there are significant benefits of the algorithm-driven economy.

The other thing is that we are not anti-tech or anti-technology. As we describe it, big data and big analytics are neither good, bad, nor neutral. It depends on how firms use the data and algorithms, their incentives, and the characteristics of the key market in which the technology and data are being employed.

The first antic-competitive scenario that came to our mind was collusion. After publishing our initial working paper,[1] we started getting inquiries

[1] Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, 2017 U. ILL. L. REV. 1775; Oxford Legal Studies Research Paper No. 18/2015; University of Tennessee Legal Studies Research Paper No. 267 (available at

from the press. When we spoke with Sam Schechner with the *Wall Street Journal*, he found instances of possible algorithmic collusion. When we spoke with reporters from the *Financial Times* and *The Economist*, they too were finding anticompetitive scenarios. Perhaps we were on to something. After the press came the enforcers, particularly the EU Antitrust Chief, Margrethe Vestager. She was expressing concerns about algorithmic collusion. And then the OECD held a workshop in which we submitted a whitepaper.[2] The OECD invited competition authorities from around the world, and many of them were also starting to express concerns about our algorithmic collusion scenarios. Among their concerns — *It's really truly a frontier now for us. This could be one of the biggest challenges that competition law enforcers have ever faced.*

So what are the challenges? Why is this becoming a pressing issue among competition officials? And how can you advise your clients regarding this issue?

Let us break algorithmic collusion down into four scenarios: The Messenger Scenario; Hub-and-Spoke; Tacit Collusion on Steroids: The Predictable Agent; and Digital Eye. We came up with these scenarios originally in our article and book *Virtual Competition*.[3] For each scenario, we'll see what issues arise.

Let's start with the easiest scenario—the *Messenger Scenario.* Here we have evidence of humans colluding. I don't see anyone from my competition law class here in the audience, but this is an antitrust no-brainer. Basically, humans agree to collude among themselves, and they use the pricing algorithm to help them collude. Why is this a no-brainer under antitrust law? If companies agree among themselves to fix prices, allocate markets, and allocate bids, they not only face civil liability but, potentially, criminal liability here in the U.S. as the executives go behind bars. That's because the illegality inheres in the agreement. Once the executives agree to tamper with the pricing structure or allocate markets, their agreement has independent legal significance that could potentially put them behind bars.

SSRN: https://ssrn.com/abstract=3308859 or http://dx.doi.org/10.2139/ssrn.2591874).

[2] Ariel Ezrachi & Maurice E. Stucke, *Algorithmic Collusion: Problems and Counter-Measures*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, https://one.oecd.org/document/DAF/COMP/WD(2017)25/en/pdf (last visited July 28, 2019).

[3] ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016).

Another key thing—and we're going to talk about this in our antitrust class next week—is that you don't need a formal agreement. If any of you have seen the 2009 movie *The Informant!*, you saw Matt Damon, who was playing the role of ADM's vice president Mark Whitacre. He was a cooperative witness who was secretly taping the meetings where the competitors colluded. In a scene from the movie, the prosecutors told him, "I don't think we have enough evidence of an agreement." So Whitacre went back to the hotel room and asked the executives, "Do we have an agreement?" and they all said "Yes!" But you do not necessarily need a formal agreement like that. The law requires a conscious commitment to a common scheme.

Right about the time that we wrote our first article on algorithmic collusion, low and behold the Department of Justice brings a case exactly fitting this scenario. Here, David Topkins and his co-conspirators agreed among themselves to fix the price of posters and then they designed an algorithm to help them perfect that collusion. That led to criminal liability.

So, the first scenario, from a legal perspective, is easy. Humans collude, they use their algorithms to help perfect the collusion, and anti-trust has the tools to punish that. The executives can go to jail as a result.

Now, let's take the second scenario, which we call the "hub-and-spoke" scenario. An example would be Uber. Here you have an agreement to fix price. Uber has an agreement to fix price with all of its drivers within its network. Now the issue is how do you characterize that agreement? Is it what you would consider a vertical agreement between one driver and Uber? Or, as some of the criminal defense lawyers in the room know, is this a hub-and-spoke cartel?

There are two famous "No's" in antitrust. Competitors cannot communicate directly, nor can they use an intermediary. If we wanted to form a cartel, one way is that we can all get together and agree. Another way is if we use an intermediary. Suppose all of us here today are competitors. The intermediary would approach each of us individually and invite us to participate in the cartel. We are not communicating directly with each another. We are all going through the intermediary. Is that illegal? Yes! That is your hub-and-spoke conspiracy.

One classic hub-and-spoke antitrust conspiracy involved Toys-R-Us. Toys-R-Us, when it was a powerful retailer, organized a group boycott with the major toy manufacturers. That is illegal.

The DOJ and FTC in the OECD workshop on algorithmic collusion recognized this as well. Suppose an intermediary gets each competitor to agree to use a particular pricing algorithm. The evidence showed the

competitor did so knowing that all of the other competitors would use the identical algorithm. That could be *per se* illegal under a "hub-and-spoke" theory. We have also seen litigation involving Uber alleging a hub-and-spoke conspiracy.

Now, what is the vexing issue here? Suppose Uber enters Knoxville and has its first agreement with its first driver. The driver agrees to use Uber's pricing algorithm for the base price and any surge pricing. That is not anti-competitive. A second driver joins Uber's platform, a third driver—still no antitrust problem. But what happens when Uber becomes the dominant platform here in Knoxville? Does it now resemble a hub-and-spoke conspiracy? Now each driver knows that no other driver will undercut them on price because Uber determines the price. The question, then, is when does it go from a series of vertical agreements to something resembling a hub-and-spoke conspiracy? Because each driver can now be assured that no other driver will get extra business as a result of charging a lower price.

This is a difficult issue. An issue that can give defense counsel heartburn. How do you advise your clients when they are on a platform like Uber's of when that pricing scheme becomes problematic?

That is one dimension of the problem. Another dimension is when your client starts outsourcing algorithmic pricing to a third party, like Boomerang. Boomerang, for example, might enlist Staples. It could then enlist Staple's competitors, like Office Depot. Now the rivals are all outsourcing their pricing to this common algorithm. Can that have the effect of softening competition? This apparently was the case with a2i Systems. As the *Wall Street Journal* brought out, the company actually promoted its algorithm as a way for the gas stations to avoid price wars. Now you have different gas stations that are now sourcing their pricing to the same third party. Is this a hub-and-spoke conspiracy? Or is this just a series of vertical agreements that would be subject to a more deferential "rule of reason" analysis under antitrust law?

Now let us turn to our third scenario, *Tacit Collusion on Steroids: The Predictable Agent*, which is creating a lot of debate. Here the competitors have no agreement, but they all recognize that if they each start using a common pricing algorithm, then that can facilitate what is called "tacit collusion." As a result, prices rise above the competitive level. Here we have no evidence of an agreement, but we have evidence of higher prices and anti-competitive intent. Is that sufficient to impose antitrust liability?

We have a couple of examples of this. In Germany, the competition authorities are concerned about higher gas prices, given that five firms dominate the off-motorway gas station business. It raises the classic

example of conscious parallelism. A gas station will look to see what its competitor is charging and then decide whether it should raise or lower its price.

To illustrate tacit collusion, we regularly do this exercise in our antitrust class. I tell my students: "Imagine you have a gas station, your competitor is across the street, and there are no other gas stations for 50 miles." And I tell them the monopoly price for a gallon of gas – say $4 -- and the competitive price, say $2.75. "What price do you charge?" The students play the role of the competing gas station owners. Some students lower their price. When they lower their price, their competitor, of course, lowers its price. "Now are you able to go on your ski vacation to Davos?" Not with a slim profit margin. In the end, the students begin raising their price. They each look to see what the other competitor does. They say, "If I lower my price, my rival is just going to lower its price again. But if I follow my rival and raise the price, we can make some profits." In the end, the gas prices inch up to the monopoly level. The students can ski in Davos. No agreement—just tacit collusion, which is beyond attack under Section 1 of the Sherman Act.

Going back to Germany. Germany had this same problem with tacit collusion. So, the government said, "What we are going to do is increase transparency. We are going to give consumers the pricing information so that they can easily determine the price for gas at nearby stations." What effect did this have? It made it worse! Why did gas prices increase as a result? Before, the competitors would have to drive around town to see what their competitors were charging. Now with the pricing online, they would have quicker access to their rivals' gas prices.

With algorithms, the speed in responding significantly increases. Let's say all the competitors rely on pricing algorithms, and each station's gas prices are posted online. If your rival were to discount, your algorithm would instantaneously find out and respond. Your rival will not likely benefit from its discounting. The same would happen if you were to discount. Neither of you would develop the reputation of being a discounter, because each of you would have the same price. Recognizing that, your algorithm, programmed to maximize profits, will raise price. Your rival's pricing algorithm, also programmed to maximize profits, will likely follow. In the end, the consumers do not benefit, as they pay higher prices.

Here, the concern is that tacit collusion leads to the same anticompetitive outcome as if the rivals expressly colluded, but there is no way to get at that behavior under the antitrust law because there is no agreement. Each competitor is just watching its rivals and responding accordingly.

What then can antitrust enforcers do to prevent tacit algorithmic collusion? This has engendered a lot of debate. Some say, "Don't worry. Tacit collusion is less likely to occur online." Others say, "No, we have already experimented with some popular forms of pricing algorithms and are starting to find that kind of tacit collusion." So, one area of debate is how likely is this scenario to happen? And when tacit collude occurs, can you challenge it if you just have evidence of anti-competitive intent?

Our last scenario, which we call *Digital Eye*, is the most futuristic. Uber has this thing called God View that enables its officials to see where all their cars are—well not their cars, independently contracted cars… It can see where all the vehicles are at any moment in any city. Once we start having sensors in products in order to increase efficiency, might competitors start having a God View of not only where their products are, but also where their rivals' products are? Now you can have the algorithms reaching a coordinated result without, necessarily, even the company knowing.

One big breakthrough in machine learning was when Carnegie Mellon brought together the world's best poker players to play against its algorithm. First the algorithm was not specific to poker. As one of developers told the press, "We did not program it to play poker. We programmed it to learn any imperfect-information game, and fed it the rules of No-Limit Texas Hold'em as a way to evaluate its performance." The AI program learned the optimal strategy. The algorithm's strategy was not always discernable to the poker players. What seemed like bad movers were actually good moves. So, the poker players could not figure out the algorithm's strategy, and they were losing to this algorithm. The poker players then banded together. They got together every night to figure out how to defeat the algorithm: "How can we identify and exploit the algorithm's weaknesses?" But, at the same time, the algorithm *itself* was looking at the shortcomings of its strategy, and adjusting its strategy. So the next morning when the poker players tried to exploit the algorithm's weaknesses, the computer already identified and corrected these flaws. The players lost even more money. After twenty days of playing poker, the players lost a significant sum.

We also saw this with Google's AlphaGo algorithm, which defeated in 2017 the world's best Go player. The algorithm's strategies were unfamiliar to even the most experienced Go players.

Even though our fourth scenario may happen far in the future, what if the competitors' pricing algorithms figure out a way to stabilize pricing above competitive levels in a way that the companies never envisioned? The

companies don't even know that they are tacitly colluding. Are the companies liable?

Here, we don't have any evidence of an anti-competitive agreement. Nor do we have evidence of anti-competitive intent. But we have an anti-competitive outcome. Should the companies be liable as a result? That remains unclear.

So, will tacit algorithmic collusion occur in every industry? No. It will occur on the margins. The risk will increase for some industries that are already susceptible to tacit collusion. The competition agencies have identified several factors that would make tacit collusion more likely: industries with few competitors; where the goods and services are not significantly differentiated; high entry barriers; where you don't have powerful buyers; where you typically have small, regular, and frequent purchases; and where the algorithms can readily monitor the pricing. The key takeaway here is the speed. The algorithm can monitor any sort of deviation and promptly react, thereby reducing the rival's incentive to discount.

So, how do you advise your clients? When we were speaking at the ABA, we came up with this PowerPoint slide of some clear do's and don'ts for your clients. As for the Don'ts —

- Don't agree with competitors to fix price, allocate markets, or rig bids.
- Don't adopt specific algorithms to implement an illegal agreement. Just because the algorithm fixes price does not absolve the humans of liability. Remember, it's the agreement itself that is illegal.
- Don't agree with competitors to use similar pricing algorithms. Now there is an agreement that would be subject to antitrust scrutiny.
- Don't agree to use a third-party pricing algorithm based on the assurance that your rivals will use the same algorithm—particularly if the vendor says that your joint use of the algorithm can help avoid ruinous price wars.
- Don't communicate or meet with competitors about their pricing algorithms (at least without first consulting with antitrust counsel).
- Don't discuss with, or complain to, a third-party vendor of pricing algorithms about its pricing for competitors. That might suggest that your client expects the vendor to act as the hub in a hub-and-spoke price-fixing conspiracy.

- Don't agree to share data with rivals' algorithms before making the data publicly available.

  The antitrust agencies are concerned about these types of agreements. When I was at the DOJ, we had cases whereby the shared information wasn't particularly important for consumers but it was very important for the rivals to help them reach an anti-competitive outcome. The agencies went after that.

A few Do's —

- Do discuss with clients why they are switching to pricing algorithms and any expected legitimate business rationale. If your client is going to use a pricing algorithm, understand their pro-competitive business justifications for doing do. You would want to make sure that that is being documented.
- Do consider the antitrust risks when outsourcing pricing to vendor that is also pricing for rivals. If they are going to outsource their pricing to a vendor, you'll want to know if that vendor is pricing for any rival to your client. How will the data be treated? And will having multiple competitors use the same vendor likely raise price above competitive levels?
- Do consider what data is being publicly shared and the extent the data benefits customers versus rivals. And the concern here with the agencies is "cheap talk." There was this famous antitrust case involving airlines, United States v. Airline Tariff Publishing Co., where the airlines were using these platforms to share information with the public and one another. But the information really didn't help the customer. Instead it helped the rival airlines come to an agreement to raise prices above competitive levels.
- Do consider whether the company's conduct can be construed as a "plus factor"— for example, evidence that the firm acted contrary to its economic interest if done unilaterally (e.g., a subset of firms restricts production when prices and profits are increasing). Even though there might not have been a formal agreement like in the movie *The Informant!*, is there a series of behavior, including the rivals' switching to algorithms, that the agencies will likely infer an illegal price-fixing agreement?

Margrethe Vestager from the European Commission also spoke about compliance by design. That may work when designing simple pricing algorithms. But we are a little bit dubious about its working with machine learning. Even if you program the algorithm to not expressly collude, will

the algorithm circumvent that in finding ways to tacitly collude, which, by itself, is not necessarily illegal? Nonetheless, what she expressed is important, namely that a company to some degree should be accountable for its algorithms.

And the Commission is starting to crack down in this area. It recently brought a case involving vertical restraints, resale price maintenance, in which the industry-wide use of pricing algorithms facilitated the anticompetitive conduct.

So, after Ariel and I came up with our article on algorithmic collusion, we thought "Is this it? Is this the end of the story?" And then we came up with the opposite scenario: Behavioral Discrimination.

Here you have an ecosystem where you are individually tracked, where information is compiled about you in order to induce you to buy things that you might not otherwise would have purchased at the highest price you are willing to pay.

Suppose, for example, you book a trip using a MacBook. One study found that the hotel price that you will likely pay will be higher than if you used a Dell laptop.

We are seeing two things. First is the ability to price discriminate: to identify the highest price that you are willing to pay as a consumer. And the price that you are willing to pay might differ from the price that the person sitting next you is willing to pay. Each of you will get your own individualized price or your own customized product offer. The second thing is the ability to increase consumption, by knowing who you are, your particular tastes and preferences, and your weaknesses.

Anyone who pays college tuition might say, "Tell me something I don't know." Because colleges are very good in knowing how much to extract from you. They do not leave any money on the table. But, at least with college education, we can say, "Alright, that price discrimination creates opportunities to allow people who may otherwise not be able to afford the university to attend. That enriches everyone's educational experience."

With our scenario, we may not necessarily have those social benefits. In tracking you, collecting your personal data, and experimenting different offers on you, companies will learn to identify what you are willing to pay and how to induce you to buy. So, there was internal memo by Facebook that was leaked to an Australian newspaper. Facebook denied that it was aimed at advertisers. But Facebook noted how it could help advertisers target teenagers in moments of vulnerability. Facebook would know, from the profiles it developed, when the teenager felt "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," "overwhelmed,"

"stressed," and "a failure." Facebook could identify when teenagers needed a confidence boost in order to induce them to buy.

When we presented this scenario at one of the competition agencies, their chief economist said, "Well, there are over 100 documented examples of different cognitive biases and imperfect willpower. So, it is not surprising that an advertiser could find one to exploit."

So, why don't we see more of it? One reason is push back. This is one of the ironies: when we discussed this scenario, the economists were often agnostic about price discrimination, less so about what we call behavioral discrimination. But when we spoke to judges, lawyers, and others, they were outraged. When you look at the research, consumers think price discrimination is unfair.

But behavioral discrimination can be achieved subtly through targeted discounts. It can also creep in through dynamic pricing. We will live, in a way, in our own unique *Truman Show*—where your reality will differ from other people's reality. We will no longer have one price. Each of us will be offered different prices. At first, we might chalk this up to dynamic pricing: When you book a flight online, you don't expect that the price that you pay today to be the same price that you would pay next week. That just reflects the difference in supply and demand.

But once we become accustomed to dynamic pricing, it is easier for companies to go a step further and price discriminate.

The airlines from the data collected about you will know whether you have flown business class before. They know the other websites that you have visited. They can predict that you will likely pay a higher price than someone who primarily flies with Spirit Airlines.

That's our second scenario. In our first scenario, as a result of collusion, everyone pays a higher uniform price. In our second scenario, we will each be charged individualized prices in order to extract the most amount of money from us.

Our third scenario is what we call "frenemy." To illustrate, we have the tale of two apps. Suppose one app is called *Brightest Flashlight*. You install the app on your smartphone. When you use it, it turns on all the lights on your phone to make it a flashlight. Unbeknownst to you, the company that developed the app, Goldenshores, also tracks your precise location, which it sells to others, including advertising networks. Goldenshores doesn't tell you, when you're using its app, that it is tracking your location. The FTC cracks down on the app developer's deception, and Goldenshores enters into a civil consent decree.

The other app is called *Disconnect*. One of Disconnect's founders once worked for Google. He discovered that Facebook tracks you not only when you're on Facebook's platform, but on any website that has the Facebook "Like" icon. So he created an app to prevent Facebook from tracking you. After leaving Google, he and others created an app that helps prevent you from being tracked and thereby limit the amount of targeted behavioral advertising you receive.

Which app gets kicked out of the Google Play store? The one that the FTC found engaged in deception? Or the one that provided consumer's greater control in not being tracked?

How many of you say Brightest Flashlight, by a show of hands?

The rest of you, I assume, say Disconnect?

Absolutely. It was Disconnect.

When we presented this scenario, a member of the audience said, "Well it makes sense that Google would kick out Disconnect. Google's business model relies primarily on advertising revenues. It profits from tracking users." As he aptly observed, "Why would you invite an arsonist into your house?" We really liked his analogy. Why would anyone invite the arsonists, when they could potentially destroy your entire business.

So, where does the power reside in this ecosystem? A Wall Street analyst said apps are worth millions but platforms are worth billions. Platforms control the oxygen supply, and they have this frenemy relationship.

We can see this frenemy relationship between Google and Uber. It's good for Google to attract app developers because that increases the popularity of its Android phone. But once Google starts competing against, let's say Uber, then its incentives change and it has a greater ability to then hinder the competitiveness of the app developer.

And this was part of the European Commission's case against Google with comparison shopping sites. Google recognized, according to its internal documents, that its comparison shopping product was inferior to its rivals' products. But Google's rivals relied on the traffic from Google's search engine, which is the dominant search engine in the EU and US. So Google systematically favored its own comparison shopping product in its general search results. It placed its own product on the first page of its search results, and demoted its rivals to the fourth or fifth page. As the European Commission found, if you want to hide something, put it on the fourth or fifth page because, as the data shows, very few people go to the fourth or fifth page of the search results.

Google gave its own product an unfair advantage and hindered rivals and competition. So we can see how Google's incentives changed. Google demoted the other comparison shopping products only after it vertically integrated and started competing against them.

Returning to Uber, we can see how Google and the rise sharing app are friends. Google needed Uber to be on its platform to attract phone users to Android, which in turn would attract other app developers. Uber needs to be on Google's Android platform in order attract users. But Google today is a dominant mobile platform. Once it starts developing driverless cars for a ride-sharing app, then its incentives can change. It can become the enemy.

So these powerful platforms can have a frenemy relationship with the millions of apps, websites, and developers that rely on the platform to reach users. *The Economist* had a whole edition about how these data-opolies can abuse their dominance.

The interesting thing is where are we going. If you remember Microsoft in 1990s, you remember the era where PCs dominated. Even today Microsoft has a monopoly for operating systems on desktop and laptop computers. But we can see how mobile phones displaced personal computers. As people shifted their attention and time to their phones, the power increasingly shifted to Apple and Google.

Where is the next area that is likely to be contested? It will likely be voice — that is, the rise of digital assistants. Today, Google, Apple, and Amazon are all vying for the space — to control the platform that controls all of your smart appliances, and primarily engages with you. There was an article in today's *Wall Street Journal* about how Alexa will be increasingly embedded into or integrated with your smart household appliances. You have this device in your home that is collecting all this data about you. It will know when you might need toilet paper, and recommend what toilet paper to get. With all this personal data, and the many opportunities to interact with you, the platform with the dominant personal assistant will have even more power in our economy. We discuss in our 2016 article in *Wired* how we don't pay our digital assistant's salary. Our digital assistant is paid by Google, Apple, or Amazon. When their incentives and interests differ from ours, we can be harmed as a result.

What about a purist butler? What about getting a digital assistant motivated to serve only our interests? That is a possibility. But there is a significant hurdle in these data-driven markets. Namely, data-driven network effects. A network effect is basically where your utility increases as other people use the product or service. A classic example is a telephone. The more people who have a phone, the more people you can

call. The more people who are on Facebook, the more people with whom you can connect.

But there are other types of network effects. For example, is your being on Google really going to be a benefit to this side of the room? Yes. It's an indirect network effect, which we call "learning by doing." As more people use a particular search engine, the search engine has more opportunities to predict and identify which responses are more relevant, the more feedback the search engine receives of any errors, and the quicker the search engine can respond by recalibrating its offerings. The quality improvement attracts additional users, who help the search engine identify relevant responses for both popular and less frequent queries.

With digital assistants, there are several network effects at play. Given these network effects, it can be really difficult for a purist digital assistant to subsequently enter the market, after it is dominated by Google, Apple, Facebook, or Amazon.

So, is the future of virtual competition necessarily bleak? No. There are significant potential benefits from the data-driven economy. The transformative innovations from machine learning and big data can lower our search costs, lower entry barriers, create new channels for expansion and entry, and ultimately stimulate competition.

But we cannot ignore the risks. Before this conference, I was at my ophthalmologist's office. He asked, "What are you going to talk about?" After I told him, he mentioned how the pricing of many pharmaceuticals have gone through the roof. He is now recommending to his patients to get some of their medicine from Canada just because of how expensive it is here in the U.S. It's not just pharmaceuticals. As we are gathering and examining data on multiple segments of our economy, we are finding a "market power problem." Many industries are dominated by a few players. Profit margins are widening, not because of efficiencies, but because of market power. Ariel and I recently did some research for the European Commission, and we found that this market power problem is also having an adverse effect on innovation. So, we can't ignore the risks of algorithmic collusion, behavioral discrimination, and powerful platforms. These digital markets will not necessarily self-correct.

So, what are we going to do about it? That is the question. We went to one competition agency and were expecting a lot of push back. The head of the agency thought about it and said, "Quite good, but what are we going to do about it?" That is the pressing issue. Here's a great quote by Barry Nalebuff, who is a game theorist at Yale. He said, "When the masses get mad enough, perhaps they will elect a new trust-busting Teddy Roosevelt for the digital era." Are we there now?

The good news is that the European competition officials are very much engaged in this issue. And the evolution in thinking in just the past three years is astronomical. Yesterday it came out that the European Commission is investigating Amazon on how its use of consumer data could disadvantage others who compete on its platform.

Here in the U.S., the FTC is now holding a series of workshops including issues that we just went over today — algorithmic collusion, behavioral discrimination, and the power of these super-platforms. That's a good thing.

So, I leave you with a few key take-aways.

First, to what extent, as we move into the digital economy, does the "invisible hand" still govern? Has it been displaced by the digital hand? The digital hand can be very powerful. Think about Uber. Uber does not employ the drivers. It doesn't own the cars. Yet it can determine the market clearing price in so many different geographic markets. As Uber's market power increases, does that end competition as we know it for ride sharing services?

What then is competition? In markets continually manipulated by bots and algorithms, is competitive pricing an illusion? Normally we think of competition as delivering a lower price. But in a world of personalized pricing, you don't necessarily know if your price is actually better than the price that your neighbor receives. There was a recent article about facial recognition software. Suppose to preserve your anonymity, you shop offline in the brick-and-mortar stores, and you forego any loyalty card. You may still get the personalized price. As even more information is collected about you, merchants will have even more information about what you are buying, your credit history and risk, and how much you can afford. It used to be, when you purchased your car, that you could put on your grubby clothes, and credibly say, "Oh, that's too much money." But soon the car salesman, when you enter the showroom, will know your name, exactly how much you can afford, and how much you actually have.

Finally, as power shifts to the hands of the few, what are the risks to our democratic ideals, and our economic and overall well-being? This is a concern today across the political spectrum. Once you have the rise of these super-platforms, what are their effects — not only on our wallets, but on our marketplace of ideas and our democracy? Those are some of the overarching concerns.

If you are interested, here are a couple of books that we have written on the subject – *Big Data and Competition Policy* and *Virtual Competition* and I would love to get your feedback.

Audience: *(inaudible). The second question is on personal pricing: If I can pay more than you and I get a higher price, but at the same time I get my product tomorrow—you have to wait two to three days—that is a form of personal pricing that I might be willing to accept. If anybody is smart about personal pricing they would do things like that, blend it in, they are not going to be equal products.*

Stucke: Let's take your second scenario first. Absolutely. You might get a higher price but you might get better service. We all experience it. If you fly business versus flying coach and then you fly first class versus business. Absolutely, we all understand that.

But here are a couple of scenarios and this is what some of the data reveals. What if you are being charged a higher price, not because necessarily you are wealthier, but maybe because of who you are; who your friends are; how much alcohol you drink; how much tobacco you use.

In China they are working with their super-platforms in creating a score on each individual. Imagine we are in a world where we could rate one another, and your rating would be based on your interactions with me and my rating would be based my interactions with you. First of all, what effect does that have? Second, and the concern in China is, what if the rating is wrong? That is why we have the Fair Credit Reporting Act, because the data that the reporting agencies have on you is not always correct. Now, that might affect what you are going to see or don't see. You might be getting a worse offer because of some misconception about you, where you live, or your age. And that raises concerns when they collect data about your health.

Audience: (inaudible)

Stucke: Healthcare has a lot of its own antitrust issues. One of the things is the empirical research that I have seen to date. It suggests that the increase in concentration from hospital mergers has really paid off with the promised efficiencies. The mergers have not necessarily led to lower prices or increased quality. And then the other thing is—I live in a neighborhood with lots of doctors—what they are telling me is that you either have to organize into a larger physician practice group or, if you are out on our own, you are dead. You've got to align yourself in a bigger group. Then the question is if you have markets dominated by a few hospitals and a few physician groups are you going to have higher prices. That's a key issue today, along with the issue of pharmaceutical pricing . . . .

Audience: *(inaudible)*

Stucke: Let's take your second point first. Great idea. And that would be in fact, what we were thinking about with tacit collusion. Wouldn't it

be nice, if there was an app that would play off the various gas stations, so that when you want to come in and fill up your SUV. . . now the stations would negotiate with you a discount off of the posted price. So now, you can have this algorithmic collusion, but there is one way to destabilize it. The gasoline station might say, "I'll give you a secret discount if you fill up your SUV at my place." So you'll still have the same posted price, but you pay a lower price.

As to your first point, there is the asymmetry in information and power. Remember with our frenemy dynamic who has the power: it's the platform. If you are going to devise an app that can potentially hinder advertisements, or the advertising revenue of the super-platform, what is to prevent the platform from excluding the app from its app store and make it harder for consumers to find and use your app?

The second thing is we already have privacy policies. We have privacy policies that we have been around for years, if not decades. How many of you actually read the privacy policies? Even if you read it, what can you do? There is an imbalance in power on multiple levels. First, you are giving away your data and you are ostensibly getting a free product. But do you know if that's a fair exchange? You don't really know who has your data, what they are using your data for, how they are using it, and how it may be used in the future. So you don't necessarily know the value of your data. The other thing is that you are working for free by posting content on Facebook. Imagine this: Facebook needs all of you, because you actually provide the content to attract others to its platform so that Facebook can target us with advertisements. You are not necessarily being compensated for your Facebook posts, or your Twitter posts, or your YouTube videos. The market up to this point has not really been providing the compensatory feature. In order for a market to function effectively, you would first have to know what the value is of what you have and you also would need competitive alternatives.

Audience: *(inaudible)*

Stucke: We all know about Cambridge Analytica. Does anyone in here not know about Cambridge Analytica? Also, we know about the "hashtag" delete Facebook movement. But what result did that scandal have on Facebook? In its first quarterly report after Cambridge Analytica and delete Facebook, Facebook's revenues went up and its usage went up as well. Some people said, "Well, I'm going to delete Facebook but I'm going to go to Instagram." But Instagram is owned by Facebook. You have multiple privacy violations and there hasn't been a market mechanism to punish Facebook.

You raise a really interesting point: How do we go after it? There are two schools of thought: Wilson's and Roosevelt's. This arose during the 1912 presidential elections. Roosevelt assumed that monopolies represent the natural evolution of market power, so the government should simply regulate them.

You also hear currently how we needed these monopolies in order to better compete in the Artificial Intelligence arms-race. We need Google and Facebook to innovate in AI to compete against China. Because China have made AI one of their key missions — to become by 2030 the world leader in AI technology. So, let's just regulate these data-opolies.

The problem, though, is that once the regulator regulates the monopoly invariably the regulator will be captured or the monopoly will find ways to circumvent the regulation.

The Wilson school does not accept monopolies as either natural nor inevitable. Most monopolies do not arise naturally from offering superior services. Instead, they grow artificially and by government support.

Under the Wilson school, today's data-opolies represent the weak antitrust enforcement over the past 35 years. We need to have structural relief. And that is why you heard the Louisiana Attorney General say we should start breaking these monopolies up.

Or one can implement regulations that will not regulate the platforms per se, but weaken their stronghold. We can enact privacy regulations like Europe's GDPR in order to jump-start privacy competition, in offering greater data portability and transparency. So what are the necessary preconditions to jump start privacy competition? These laws would provide the scaffolding for an inclusive digital economy that actually protects our privacy, autonomy, and well-being. And that is what is being discussed right now in policy circles.

Audience: *They should put something in there. Right when Cambridge came out and after the first quarterly reportings of Facebook, when they reported, they did see a loss of 20% of people deleting their Facebook account. Whether to go to another Facebook platform, I'm not sure. But what is interesting though is that, don't you think the technology, as fast as it's rapidly developing, now we are in a game of extremes that we have to wait for things to get so extreme so then other competitor will counter act with the market. Maybe this is the shift that we haven't seen before.*

Stucke: You always have the risk of creative destruction from something that destroys the current market with a new unforeseen technology. We saw this creative destruction when the iPhone disrupted Microsoft's stronghold.

One problem is waiting, because it can take a really long time. A second problem is that we need these competitive portals.

To see why, let's go back to IBM. The Department of Justice investigated IBM, as some of you might recall, for decades. It's often considered a failure in antitrust because Bill Baxter, when he became the head of the Antitrust Division, shut that case down. But the DOJ's investigation actually opened a competitive portal. While it was being investigated, IBM was developing the personal computer. Because of the antitrust scrutiny, IBM decided not to bundle its software program with its PC. IBM's second president Thomas Watson, Jr. noted how the massive antitrust investigation required the company to reexamine its practices. So IBM decided to stop requiring customers to buy software, services, and hardware as one bundle. This opened up software markets to independent companies. It created a window of opportunity for Microsoft.

And Microsoft was investigated in the 1990s for tying its browser to its dominant operating system. Given the antitrust scrutiny, Microsoft was less likely to bundle, which in turn created a competitive portal for Google, Facebook, and similar companies.

But since the *Microsoft* case, the DOJ has brought only one case against a monopoly under Section 2 of the Sherman Act. From 2000 onward, only one case. During the Nixon administration, the DOJ brought over 40 criminal and civil cases against monopolies within a three-year period.

So today's data-opolies have nothing to fear when it comes to our antitrust enforcers. Antitrust can create a competitive portal. But the data-opolies, unimpeded, will continue to expand their platforms. What is the next space that they will occupy? It's our home with the digital personal assistant. With the network effects in that market, it will be hard to displace whoever dominates that platform. If "voice" is the next big space, then expect the current dominant platforms to try to leverage their power to dominate that space.

Audience: *When we talked from price discrimination and then we jumped to data privacy. Are you assuming or taking the position that if we take more privacy data protection, it can help naturally circumvent asymmetrically information, give consumers more power choosing? Is that one assumption you are rolling with?*

Stucke: Right. One thing is, I don't think the competition authorities can do this by themselves. They have to coordinate with the privacy folks and the consumer protection folks because, first of all, the tools of the competition agency right now is primarily price centric. They look at the price. What is the effect that the merger will have on pricing? If Coke

acquires Pepsi, the enforcer can tell you with a certain degree of confidence what the likely price increase will be for Coke and Pepsi.

But when we are dealing with data-driven markets where things are ostensibly for free, the government's price-centric tools don't really work. In fact, the price centric tools can point you in the opposite direction. After Facebook acquired WhatsApp, what did it do? It lowered the nominal price for the texting app, but what it got was the data.

So, the competition agency has to recognize this data component and how it could lead to market power. You are starting to see that. The European Commission investigated Apple's acquiring Shazam. The companies didn't directly compete. But the question was whether Shazam's data would help Apple obtain or maintain market power.

First, no agency can do it by itself. Second, we need a cohesive privacy policy in order to tackle this problem. But even privacy law by itself won't be sufficient. You will need greater privacy protection, but also competition, as well as consumer protection. It really has to be an integrated approach.

Audience: *(inaudible)*

Stucke: This is behavioral economics. Defaults matter. Under traditional economic theory, it shouldn't really matter if it's opt out or opt in. But study after study has found that the choice of the default option can have a considerable impact on the final outcome. So if people have to opt into having their data kept private, fewer will likely do so, and a lot of their data will be collected. If the default setting is to keep the data private, and people would have to opt out, few will likely do so, and a lot of their data will be kept private. This is a key issue.

There was one case in France involving the energy monopoly GDF Suez. Really interesting case. The regulated monopoly was using its vast customer database to target customers in an unregulated market with deals on gas and electricity. French gas customers could opt for the regulated tariffs, which only the monopoly offered, or the "market" offers, which GDF Suez and its rivals offered. In making its market offers, GDF Suez had an unfair advantage over its rivals. It was using the data it collected as a regulated monopoly to target customers with customized offers based on their usage. The personal data in question was commercially valuable. The monopoly used the customer data to squeeze out its competitors in the unregulated sector. The rivals were naturally concerned. They said, "Look, we don't have this data, we can't really compete." Now imagine you are with the French government. Should you give that personal data to the monopoly's competitors? There is a tradeoff between privacy and

competition. You can increase competition and lower energy prices. But you also lessen privacy.

So, what do you do? If you require disclosure, what should the default be? Should customers have to opt out of privacy or opt in to having their privacy protected? Here the monopoly will argue for privacy as the default. The monopolist knows that with this default setting very few customers would actually complete the paperwork to have their data shared with the monopoly's rivals. And the rivals will remain competitively disadvantaged. The rivals will argue for disclosure as the default setting. They know that few customers will actually remember to take the time to complete the form to request the monopoly to not disclose their data.

The French court, when faced with this issue, chose competition, and ordered the monopoly to disclose the data, unless the customer expressly opted out.

But, in other cases, the privacy concerns might outweigh the competition concerns, like the sensitive personal data collected by the internet service providers. There the agencies might require the data not to be disclosed to advertisers, unless the consumer specifically opts to release that data.

So the choice of the privacy default option is going to be a key issue.

Audience: *(inaudible)*

Stucke: So that's the other thing we are going to regulate. I'm dubious. I'm dubious about regulating [inaudible]. Look at the FCC. They were coopted by AT&T in the 50s and 60s.

Audience: *(inaudible)*

Stucke: Very good question. Marshall Steinbaum and I have an article coming out about the deficiencies of the consumer welfare standard.[4] Over the past thirty five years antitrust enforcers have primarily look at how mergers and restraints affect the prices paid by the customer downstream. In this light, Amazon looks great—low prices, quick service. What's the problem?

It's the effect these restraints have upstream. What anticompetitive impact does the merger or restraint have upstream on sellers and workers?

---

[4] Marshall Steinbaum & Maurice E. Stucke, *The Effective Competition Standard: A New Standard for Antitrust*, UNIV. CHI. L. REV. (forthcoming 2019); University of Tennessee Legal Studies Research Paper No. 367 (available at SSRN: https://ssrn.com/abstract=3293187).

Now, in the last few years, there is a body of economic evidence that shows how some firms have a lot of power upstream even when they have little power downstream. A great example is the franchises all along Cumberland Avenue. Franchises like McDonald's and Jimmy John's do not appear to have a lot of market power downstream. If they charged high prices, customers would go to another fast-food franchise on the Strip. But two economists came out with a study and guess what they found? In the franchise agreement, there was a provision that prevented one franchisee from poaching other employees from the same franchise in that area. So one McDonald's franchise could not poach employees from a nearby McDonald's. The effect of this no-poaching agreement was to soften competition for workers and the wages they received.

The DOJ recently came out with a joint statement with the FTC saying that no-poaching agreements among employers are *per se* illegal. And if your clients are agreeing not to poach their rival's employees, there is potential criminal liability. That is something to be mindful about. So look at your client's franchise agreements. The Washington State Attorney General's office has recently led a case against the franchises, and the DOJ has recently brought cases for collusion on wages.

I think that wraps it up. Thank you very much.