Podcast Transcript

Blurred Lines: Focusing on Antitrust and Privacy

Date: August 2, 2020

Guests: Ann M. O'Brien, Jeewon K. Serrato **Host:** Amy Kattman

Run Time: 20:42

For questions and comments contact:

Ann M. O'Brien

Partner
Washington, D.C., Philadelphia
T: +1.202.861.1650 | amobrien@bakerlaw.com

Jeewon K. Serrato

Partner
San Francisco
T: +1.415.659.2620 | jserrato@bakerlaw.com

Kattman: Do this, don't do that. Handling big data is a balancing act. Companies want to use data to compete, innovate and serve customers that faced increased scrutiny from antitrust and privacy enforcers in the U.S. and abroad. I'm Amy Kattman, and you are listening to BakerHosts.

On today's episode we'll discuss the blurring lines between antitrust and privacy regulations, and the implications for companies holding large amounts of data. Joining me for our discussion today are Ann O'Brien, a partner in BakerHostetler's Antitrust and Competition team, and Jeewon Serrato, a partner and co-leader of BakerHostetler's Digital Transformation and Data Economy team. Welcome, Ann and Jeewon.

O'Brien: Thank you for having us.

Serrato: Thanks.

Kattman: I wanted to jump right into this topic, because I know you two have prepared several real-world scenarios in which companies navigate this issue. Let's talk through some of these situations, what to anticipate, with the privacy and antitrust enforcement risks. So, here's a first scenario, we'll call this the killer acquisition. You've got an Alpha company that runs a popular app, and seeks to acquire Beta company, a small recently created competitor that has reached a new consumer segment. At first glance, there is currently little competition between merging parties. From an antitrust perspective, Ann, what concerns does the acquisition pose for enforcers and regulators?

O'Brien: Yeah, this scenario involves the hot topic of nascent competition. At first glance, there doesn't appear to be traditional antitrust concerns because there is currently little competition between the merging parties. However, antitrust enforcers could have a more nuanced concern about a couple of things. One, they could be concerned that this is a killer acquisition, that is, that Alpha company is going to kill off its potential future nascent competitor. Or, two, they could be concerned that data is acting as market power. Specifically, that Alpha could use the personal data obtained by its target to reinforce its market power in other segments, maybe advertising.

So, I'll drill down on each of those a little bit. First, the nascent competition issue. For several years there has been an increased focus on nascent competition and merger review. Nascent, or others call it future competition concerns, potentially exist where one of the merging parties has the capabilities likely to lead it to develop new products in the future. Or, where one of the merging firms is an incumbent and the other merging firm is a disruptor, who could disrupt markets with new technology or a new business model. And this is addressed in the horizontal merger guidelines.

There have been a couple of high-profile cases raising these issues recently in the social media and online razor sale space. Interestingly, nascent competition, a nascent company that's viewed as an industry disruptor, may actually draw increased scrutiny as it attempts to be acquired. But, what if the founders of Beta in our example want to be acquired? And an acquisition was part of their original business plan? Some have argued that the theory that nascent competitors are better left on their own rather than as part of a larger company, may actually harm innovation and disincentivize startups and app developers, particularly those whose primary goal was to be purchased one day by a larger tech company. So, going too far with the killer acquisition concerns could actually be an innovation killer.

Second, there could be possible antitrust concerns regarding data as market power in an adjacent market. Antitrust agencies could scrutinize or challenge the Alpha/Beta merger based on concerns that Alpha could use the personal data obtained by Beta to reinforce its market power in other segments such as advertising. And this has recently come up in the wearable tech data space.

Kattman: So, Jeewon, from a privacy perspective, what are the key considerations that would be on the mind of enforcers and regulators?

Serrato: As Ann pointed out, I think this issue of nascent competition or killer acquisition is really interesting from a privacy perspective because I think the focus here is, is what is in the minds of the customer. Privacy issues really tend to be, stemming from what would the data subject, the person whose data has been collected by, let's say, company Alpha. What did they expect versus company Beta, the target. And, let's say that there was a choice between these two companies and there was a set, maybe a smaller set of customers that chose to go with the smaller startup company, because they provided more privacy protections. And so, if this merger is approved and, let's say, the company Beta had said to their customers, something like we will never sell your data, or we provide you x, y, z privacy protections. The privacy enforcers and the regulators would be interested in looking at, would this merger in an acquisition by the Alpha company lead to a reduction of privacy rights of the target company?

If there is this transfer of customer database, that company Alpha is able to basically purchase the set of customers who were being serviced by the target company, is this going be to the detriment of the customers' privacy rights? And so, the concept of the companies providing a different level of privacy rights, and certain promises that were made by the target company and how that should go into consideration in this Alpha/Beta merger is gonna be top-of-mind.

Kattman: So, let me pose a different scenario. We'll call this the data grab. A company which holds unique data sets, such as biometric data, and wishes to expand its offerings by collecting additional data or acquiring another data heavy company. Jeewon, we'll start with you. Why are privacy regulators and enforcement authorities concerned with a company that has a large amount or a unique set of data?

Serrato: I think there are three reasons why this question about data grab is really becoming a top issue in the minds of regulators today. One is that this explosion of digital transformation initiatives by companies have created really unique sets of data. The fact that you are, you're taking automotive transportation methods from one place to another, that data used to not exist. And we have that because of the ride-hailing apps that we have. The fact that you are renting certain vacation rentals and using those instead of hotels, we have that set of data in a digital format that we didn't have before, and the list goes on. So, there are now unique data sets that are available in a digital format that can be collected and used and shared across multiple industries. And because these unique sets of data that we never had really access to before are really kind of bringing into focus, what does that mean to have big data?

So, when we're talking about these tech giants and big social media and platform offerings, we're not just talking about, let's say, a cab company that is servicing San Francisco. We're talking about a global company that is in operation across, let's say, 10, 20, 30 countries. And when you are able to bring, one, unique data sets into play that is collected across the globe and in a big data set then the third issue comes into place which is customer profiling. So, would, or should, companies have certain responsibilities for considering the privacy issues, cybersecurity issues, data ownership and use restrictions that come with this

powerful data set? That the fact that it's unique, never been collected before, the fact that it's big and there is the volume. And then, three, this can be used and tracked across time and across platforms. Those three issues, I think, makes the data grab issues challenging and something that is of top concern. Because if a company is acquiring another data-heavy company that allows this combined entity to have more, I guess, data monopoly to borrow Ann's word, or the abuse of power that comes with this data, then the regulators would be interested in raising these issues.

Kattman: Ann, what about the competition concerns?

O'Brien: This is what I love about antitrust, is that antitrust has to react to our lives, and what Jeewon sets up is really, we all have our phones with us all the time. That means, we constantly have a lot of data in our pocket related to us that companies now have. And, that's what leads to antitrust authorities, academics, Congress people and some consumers expressing fears about what companies are gonna do with that data. And they have large amounts of data. As Jeewon described, that can also create barriers to entry and can be viewed as data power, market power that then can be abused. So, notably, it's not just big tech companies that may be subject to increased antitrust and privacy scrutiny when it comes to this data collection and access. It can really be any company that holds large amounts of data.

Now, the antitrust laws have been around for a very long time. And a traditional antitrust analysis maintains the competition laws are intended to protect competition, and are not intended to protect consumer privacy. And really, people have the view that current antitrust laws are sufficient to address antitrust harm in digital markets. Now, there's a countervailing view that's been popularized recently as, hipster antitrust or, the New Brandeis approach. And that espouses a shift of focus from really price-based consumer welfare to competitive market structure, and including access to data by rivals as a constraint on monopoly power.

So, what are companies going to do with all that data? And in Europe, antitrust regulators have already attempted to make this data and competition connection under an abuse of dominance theory. That's what the European phrase for monopolization. And we're seeing this play out in a current case brought by the German federal cartel office, the Bundeskartellamt, against a social media giant. This is also likely to play out in the ad tech space, as competition enforcers and privacy regulators really try to sort out the boundaries for data usage for advertising purposes and across platforms.

Kattman: So, I have one more scenario to pose. Let's call this data potentially facilitating collusion. You've got an independent company that aggregates and holds data from competitors in the same market, in connection with the service it provides in the industry. Ann, what should this company do to ensure that this sensitive pricing, or competitive information, is not accessible or shared among competitors?

O'Brien: From an antitrust perspective, a company that holds data of multiple competitors in an industry does not want to be accused of participating in, or facilitating collusion among horizontal competitors. In a worst-case scenario, if not sharing would be deemed price fixing, bid rigging or market allocation, it could carry criminal penalties, including large fines for companies and even jail time for involved executives. It really can be company killing stuff. Therefore, it's critical that, an aggregator or even a holder of competitor data be aware of that, and have sufficient controls in place.

The good news here is that such guardrails can be put in place through a robust antitrust compliance program. For instance, anonymizing data or sharing historical data are good starting points.

Kattman: Jeewon, are there any additional privacy concerns in this case?

Serrato: Yeah, I think what Ann is suggesting is good. Anonymizing data and sharing historical data rather than real-time, proactive data is clearly, in terms of privacy principles, a good method. I think what's challenging is that often times that's not where the value is. That the revenue really is driven by, not historical data but, more proactive and real-time data. And anonymizing the data often reduces the value that the data has. And the trend that we see is that the companies are looking for, more personally identifiable, and more targeted, and more proactive and real-time data. And because, the way that you phrased the question, we're talking about horizontal competitors, right. I will call this a platform problem. That there is, I think, some sort of a fight between how to think about the market share that you have and often times the service providers will say, we have, we are the top service provider, we have 70% or we have 90% of this type of market penetration.

And so, when you are marketing yourself as being this biggest player in the market, that's great from a competitive perspective and marketing perspective. From a privacy perspective what that means though, just the same way that Ann had described it from a collusion perspective, is what does it mean? Are you collecting data that belongs to, let's say, 15 different airlines? And perhaps the service that you provide is for one purpose but is there some unique value because you're providing the same service to 15 different airlines that maybe the airlines will say give us analytics. Maybe they'll say hey, tell us some trending, tell us some targeted customer profiling. And maybe what the company wants to do is not to just provide that service for which the data was collected initially, but to come up with an alternate revenue stream that will be done in a person-identifiable way. So, be able to a track, let's say, a air passenger that purchases, one ticket from one airplane, one air carrier to the second ticket. So again, when you are tracking a person across platform, across time, and the reasonable expectation by the customer is that that data is not co-mingled. That data is not gonna be sent to one party that has access to this global view. I think that is what the privacy concern is about, that this platform may abuse the data that they have access to, to come up with a secondary use for that data, that was not within the reasonable expectation.

What is interesting to note is that this issue seems to be top-of-mind from a legislative perspective and from a regulative perspective. We talked about, in the previous conversation, how big data, unique sets of data lead to the question about customer profiling. Laws like GDPR, General Data Protection and Regulation in the EU and California Consumer Privacy Act in California, seem to really go to the heart of this issue. And, I am based in San Francisco, so I'm gonna give an example that comes out of the CCPA. Within the regulations that are put forth by the California DOJ AG's office, there is a term that says that a service provider that has collected the data on behalf of a business, may use it for internal use. Again, internal use, not to be shared with third parties, to improve or to build the quality of the services and products.

So this is talking about, if you are using the data that you have collected from the customers, and it's being used to do product improvement, internal use only, that is allowed for the service providers. As long as you are not building or correcting or augmenting data and building a customer profile. So that is in the regs right now. The California DOJ is proposing and the enforcement of the CCPA began as of July 1.

So clearly, this is something that is top-of-mind to the regulators and legislatures, as we see about 15 different states looking at adopting laws in the United States as similar to CCPA. What is the purpose for which this data can be used, and should there be, I guess an overlay of concerns by companies that are providing this platform where data from multiple competitors may be housed?

Kattman: Based on today's discussion it's clear that virtually any company that collects consumer data is facing intense government scrutiny, both from the antitrust and privacy perspectives. Ann and Jeewon, I have one final question for you. What is the number one thing companies can do to act and mitigate this risk proactively? Why don't we start with you Ann?

O'Brien: Know what data you hold and its uses, is I the think number one, and there's little parts to that. Know who your competitor is and potential competitors are with respect to that data, because those may be different from your competitors for your primary line of business. And make sure you have an effective antitrust compliance program in place that can put up those guardrails and save you from problems later.

Kattman: And Jeewon, from a privacy perspective?

Serrato: In order to do the data mapping and data inventory, understanding what data you have and how it moves through the organization. I think one thing a company can do is to establish a multistakeholder process, and some companies are creating steering committees that are focused on privacy and cybersecurity. But it's really made up of, not just privacy and cybersecurity counsels, legal and compliance, but IT and information security and even sales and marketing and business. By having an accountability process that exists internally, cross-functionally and really kind of looking at what framework this steering committee will look at to understand, the data that is ingested by the companies at different business

events. And how it moves through the organization, how it's used and to whom it's shared, seems to have really been effective.

Kattman: This is really helpful information, thank you Ann and Jeewon. If you have any questions for Ann or Jeewon, their contact information is in the show notes. As always, thanks for listening to BakerHosts.