Before the Ohio Senate Judiciary Committee

Testimony of
Dennis D. Hirsch
Professor of Law, The Ohio State University Moritz College of Law
Faculty Director, the Moritz College of Law Program on Data and Governance
Professor of Law, Capital University Law School

October 17, 2019

Chairman Eklund, Vice-Chair Manning, Ranking Member Thomas and members of the Senate Judiciary Committee, thank you for allowing me this opportunity to share my thoughts on platforms, competition and privacy. I am a Professor of Law at both The Ohio State University Moritz College of Law and at Capital University Law School. At Moritz, I direct the Program on Data and Governance, a research program that focuses on how to govern big data analytics in order to enable society to achieve its many benefits while reducing the violations of privacy and other harmful impacts that it can cause.

Today I will be making three key points, and providing four recommendations.

The three key points are:

1. Platforms’ collection and use of big data can produce not only privacy harms, but also data-related harms that include manipulation, perfect price competition, and other harmful effects on consumer welfare.
2. Where platforms occupy a dominant market position, this can insulate them from competition over non-price qualities such as privacy protection or responsible data use. This may produce more of these harmful impacts on consumer welfare than a competitive market would generate.
3. It is within the scope of antitrust law to take account of, and seek to address, these non-price data-related impacts on consumer privacy and well-being.

The four recommendations are:

1. Ohio competition authorities should seek to understand better platforms’ data-related, non-price impacts on consumer welfare, and how insufficient competition in the platform economy can increase them.
2. Ohio competition authorities should assess data-related, non-price impacts on consumer welfare when evaluating proposed mergers between big data companies, such as platforms. The legislature should evaluate whether this requires a statutory amendment and, if so, consider amending Ohio antitrust law accordingly.
3. In addressing violations of Ohio’s antitrust laws, competition authorities should consider conduct remedies that will reduce data-related harms and increase competition over responsible data use. The legislature should evaluate whether a statutory amendment is required in order to give competition authorities this remedial power and, if so, consider amending Ohio antitrust law accordingly.
4. When it comes to regulating platforms and other big data companies, Ohio competition authorities should coordinate with consumer protection and privacy authorities and should consider potential synergies between these overlapping regulatory areas.

Platforms and Personal Data

Major digital platforms such as Google or Facebook make their money largely by targeting advertisements to their users and charging advertisers for this service. They are able to target such ads more efficiently than other businesses due to the copious amounts of personal data about their users that they employ to develop targeted and personalized ads. The services that these platforms offer serve as a vehicle for collecting this valuable personal data. For example, Google provides free services that include Search, Maps, Docs, Calendar, Gmail, and Youtube, among others. Google employs each of these to collect data about its users and then employs these data in its advertising business.

Platform’s massive collections of personal information—big data—actually enables them to produce a second level of information about individuals. The first level is the specific information that the platform collects about the person. I call that “surface data.” But platforms can look for patterns in big data in order to infer other information. For example, I am an Amazon customer. It knows, for example, that I purchased a travel thermos on its site. That is part of my surface data. But Amazon does not just satisfy itself with this. It looks for patterns, correlations in its massive set of customer purchase data. Of those who bought travel thermos’s, what else did they buy? Once they find this correlation, they can infer that Dennis, who bought a travel thermos, may be interested in these other items as well. This is a very simple example of how big data analytics takes surface data and uses it to produce inferred data.

Platforms’ collection and use of personal data can harm consumers

Inferences of this type can be highly useful and beneficial. Amazon’s big data recommendations allowed its users like me to receive ads that correspond to our interests and enable Amazon to grow its business. So far, so good.

But platform’s use of big data can also harm consumers in important ways. One of these is data breaches. The larger the data set, the more people that the breach will injure through identity theft or otherwise. From 2012 to 2017, Amazon, Facebook, Google and Uber suffered a series of breaches that impacted about 100 million people. Data breaches as a whole are estimated to cost society about $375-500 billion per year.

Inferred data can also produce privacy harms. For example, a group of researchers at Cambridge University showed that, using only individuals’ Facebook likes, it was possible to infer their ethnicity, religious and political views, personality traits, sexual orientation, use of
addictive substances, age, gender, and whether their parents had separated when they were children.¹

But we need not rely on academic research for this. The Facebook-Cambridge Analytica incident shows us something very similar. As you probably know, Facebook shared 81 million users’ Facebook “likes” data with a researcher, who disclosed these data to Cambridge Analytica. Cambridge Analytica used big data analytics to infer the psychological types of each of these users. It then targeted them with political advertisements that appealed to their unconscious and that they would find very hard to resist. This type of manipulation can undermine voters’ ability to make independent, conscious choices about which candidate they support and so undermine the very foundations of our Democracy. Either party could use this technology against the other. This is not a partisan issue. It is about protecting our Democracy.

Platforms and other big data companies could also use big data to infer a person’s precise reservation price. They could then personalize pricing so that they charge each individual the maximum that they are willing to pay, thereby capturing the entire cooperative surplus from the transaction and fundamentally altering the balance of power between seller and buyer. I cannot cite to you any actual examples of this as of yet, but it is well within the realm of the possible.

Note that big data’s potential harms include privacy invasions but also extend well beyond privacy to manipulation, perfect price discrimination, and other issues. We need to big tech to address all of these harms, to handle data responsibly across the board. The term for this is data ethics. We need big tech and platforms to engage in responsible data practices and pursue data ethics, not just to protect privacy.

Platforms’ dominant market position can generate excessive data-related harms

Three main types of law can produce more responsible use of big data: privacy law, consumer protection law, and antitrust law. Privacy laws can make sure that, before they collect our data, companies notify us as to what they are collecting and give us a choice as to whether or not to allow this.

Consumer protection law can require platforms and other big data companies to use personal information responsibly and fairly. Section 1345.02 of the Revised Code makes unlawful any “unfair or deceptive act or practice in connection with a consumer transaction.” Perfect price discrimination, excessive manipulation or other big data-enabled exploitation of consumers could potentially be deemed “unfair” practices under this law, and the consumer production authority could address them.

Antitrust law, the focus of our discussion today, also has an important role to play. In a competitive market, platforms and other big data companies that engage in irresponsible and

¹ https://abcnews.go.com/blogs/technology/2013/03/facebook-likes-used-to-predict-personal-information/
unfair data practices will lose users and market share. By the same token, firms would have an incentive to protect consumers better than their competitors, to be more responsible, in order to capture market share. That could be the most powerful check on big data misbehavior.

But here we have a problem. Analyses suggest that platforms such as Google or Facebook possess a dominant market position due to network effects, switching costs and consumer lock-in. Such a dominant market position can insulate them from competitive pressure and so allow them to adopt far less protective practices without serious market consequences. In this regard, consider that Facebook stock bounced back shortly after the Cambridge Analytica scandal.

Antitrust law, by promoting more competitive markets, could push platforms to more responsible use of data analytics. In this way, competition law could work in concert with privacy law and consumer protection law to ensure that platforms protect privacy and use data responsibly.

Bring antitrust law into the digital era

In order for antitrust law to play this important role the field needs to evolve, potentially through new legislation. Antitrust law generally conditions liability on evidence that defendant raised prices or restricted output. That works for auto companies, clothing manufacturers or other, traditional targets of antitrust enforcement. But it does not work for platforms. Platforms offer “free” services. Under traditional antitrust analysis, they cannot be said to be seeking excessive, supracompetitive prices. To the contrary, regulators appear to assume that, at the price of “free,” consumer welfare must be protected.

But platform services such as Google search of Facebook social media are not free. They require us to share with them our personal information so that they, in turn, can target advertisements to us and reap tremendous profits. So there is a price. We just pay it in a different currency: personal data, rather than money.

Antitrust analysis generally looks to whether a firm uses its dominant market position to raise the price or reduce the quality of a product or service. Once we understand that users do pay a price for the use of platform services, we can see how each of these forms of antitrust analysis could apply in the platform context. Platforms can use their dominant market position to demand far more data than a competitive market would allow. That is just another way of forcing the consumer to pay a supracompetitive “price.”

The Facebook-Cambridge Analytica incident suggests that platforms can also use their dominant market position to invest less in protecting our data and in ensuring that it is used responsibly than a competitive market would allow. Arguably, in a more competitive market, Facebook would have put more resources into monitoring who gets its users’ data and how, exactly, they are using it. Seen in this way, Facebook’s dominant market position may have enabled it to provide services of lower quality than a competitive market would have produced.
Thus, platforms could be using their dominant market positions to both raise prices and lower quality – the very type of consumer welfare injuries that antitrust law seeks to address.

**Recommendation:** Ohio competition authorities should seek to understand better platforms’ data-related, non-price impacts on consumer welfare, and how insufficient competition in the platform economy can increase them.

**Practical steps forward**

Legislators and competition regulators should take three, practical steps to promote competition over responsible big data collection and use and to otherwise protect people from data-related harms.

First, they should build data aggregation, and data-related harms, into their analysis of mergers between companies that possess large quantities of personal and inferred data. Data aggregation, and the machine learning and efficiencies that it enables, can entrench existing firms and make it highly difficult for new entrants to compete. Moreover, platforms or other big data companies that use mergers to achieve a dominant market position will insulate themselves from privacy-and ethics-based competition and so be able to charge supracompetitive data prices and provide products and services of lower ethical quality. Competition regulators should consider these negative impacts on consumer welfare when evaluating the overall worthiness of the transaction. That is not to say that the privacy and ethical harms will necessarily outweigh the merger’s benefits and efficiencies. Echoing Professor Peter Swire, my main point is that they should be part of the analysis. If a statutory amendment is required to enable Ohio competition authorities to consider these non-price harms, then the legislature should pass such an amendment.

**Recommendation:** Ohio competition authorities should assess data-related, non-price impacts on consumer welfare when evaluating proposed mergers between big data companies, such as platforms. The legislature should evaluate whether this requires a statutory amendment and, if so, consider amending Ohio antitrust law accordingly.

Second, competition authorities could impose conduct remedies that require big tech and platform companies to achieve the level of privacy protection and data ethics that a more competitive market would provide. For example, it could prohibit perfect price competition or the more flagrant types of analytics-driven manipulation. That would protect people. It would also give a competitive edge to firms that could figure out efficient ways to get the benefits of big data analytics without producing its harms, and so promote competition that truly benefits consumer welfare.

In a very interesting recent case, the German competition authority, the Bundeskartellamt, did something along these lines recently in an antitrust action against Facebook. The Authority ruled that Facebook’s dominant market position enabled the company to extract too great a privacy price from its German users. It required the company to adopt the more protective
privacy practices that, in the regulators’ judgment, a more competitive market would have produced. It will take more study and policy work to determine how, precisely, such conduct remedies might work. But they merit exploration.

**Recommendation:** In addressing violations of Ohio’s antitrust laws, competition authorities should consider conduct remedies that will reduce data-related harms and increase competition over responsible data use. The legislature should evaluate whether a statutory amendment is required in order to give competition authorities this remedial power and, if so, consider amending Ohio antitrust law accordingly.

Finally, antitrust authorities should coordinate more closely with consumer protection and privacy regulators. As I have already alluded to, these regulatory areas overlap in important ways. Consumer protection authorities can use unfairness authority to require platforms and other big data users to desist from unfair practices, such as perfect price discrimination. Privacy law and consumer protection authorities using their “deceptiveness authority” can require platform and other firms to provide clear notice of their data collection and use practices and to uphold the representations that they make in those notices. Strong privacy and consumer protection rules would not only prevent consumer injuries. They would also create a competitive advantage for firms that could figure out how to achieve the goals at least cost.

Privacy law can also promote competition more generally. For example, the California Consumer Privacy Act, to which many Ohio companies will become subject on January 1, 2020, requires firms to allow individuals to download their data and port it to a competitor. If properly implemented, this privacy law mechanism could have important, pro-competitive effects. Privacy regulators will be well served by coordinating with the fellow competition authorities on such policies, just as competition authorities that seek to assess privacy harms or design privacy-related conduct remedies will benefit from the input of consumer protection and privacy regulators. Also three regulatory areas – antitrust law, consumer protection law, and privacy law – have consumer welfare at heart. Protecting consumers in the big data era requires coordination among these three types of regulators.

**Recommendation:** When it comes to regulating platforms and other big data companies, Ohio competition authorities should coordinate with consumer protection and privacy authorities and should consider potential synergies between these overlapping regulatory areas.

Thank you for giving me the opportunity to share these thoughts with you today. I welcome your questions.