

ACCESS DENIED?

Should regulators worry
about the weaponisation of
data in markets?

2021

ACCESS DENIED?

Should regulators worry about the weaponisation of data in markets?

Data is assuming an ever more central role in economic activity and day-to-day life. From the computerisation of trading in financial markets in the 1980s to the digitisation of buying and selling just about everything today, the activities of consumers and businesses are increasingly leaving a digital footprint that can be collated, analysed and used to design new, improved products and processes. Talk abounds that data has become the new oil: useful for pretty much everything and essential for modern businesses to function, but also vulnerable to being weaponised by governments and companies to exert control and advance their own interests at the expense of rivals.

Debates about the control and abuse of data touch all parts of society – ranging from concerns about protecting personal privacy to issues of national security. In the sphere of economics, competition authorities have also been taking note. Worries about the control and use of data have increasingly coloured antitrust watchdogs' thinking in recent market studies and merger investigations. The EU's competition commissioner, Margrethe Vestager, has spoken extensively about access to data as a critical factor that can make or break the fortunes of small companies looking to challenge larger rivals. These concerns are now finding their way into competition authorities' formal guidelines as well. Witness, for example, the UK Competition and Market Authority's new merger assessment guidelines, which are strewn with references to data access issues (in marked contrast with the previous guidelines, in which such issues did not feature at all). And perhaps most tellingly, in 2019 Commissioner Vestager was promoted to lead the EU's drive to create "A Europe Fit for the Digital Age" alongside her traditional responsibilities as Europe's competition watchdog-in-chief.

ALEXA, WHAT'S THE PROBLEM?

In recent merger investigations, competition authorities' worries about data have fallen into three broad categories:

- 1 **Concerns that powerful companies might force consumers to "pay" for services with their data.** In some

EXEC SUMMARY

The proliferation of data has created opportunities for innovative business to shake up – and in some cases revolutionise – tired sectors of the economy. But with the explosive growth in the volume of data being produced, antitrust watchdogs are increasingly questioning whether the businesses that control access to the most valuable data could "weaponise" this advantage to harm competitors and, ultimately, consumers. Are regulators right to worry and, if so, do they need a new framework for policing the behaviour of businesses in data-heavy industries?

recent investigations, antitrust watchdogs have suggested that merged companies could abuse their power to demand that people share more or their personal data with them as a precondition for using their services. Consumers might be unhappy about this and yet have no option but to assent because access to the company's services is essential.

- 2 **"Efficiency offence" concerns.** These worries stem from the idea that a newly merged company might have access to a richer combined body of data than any of its rivals. In and of itself, this would be a good thing if it allowed the merged firm to improve its offering, but it might also make it harder for data-poor rivals to compete effectively. If these rivals were marginalised or forced to exit the market, this could in principle damage competition, thereby leaving consumers at the mercy of a single company. A common variant of this theory of harm holds that the resulting mismatch in access to data could also damage competition by creating a barrier to entry and deterring would-be new firms from trying to set up shop in the first place.
- 3 **Vertical foreclosure concerns.** These theories of harm can arise where an "upstream" firm that generates data merges with a "downstream" firm that makes use of this data for its own services. Typically, the worry is that the upstream firm's data is an essential input for not only the downstream partner but also its rivals. In these circumstances, the upstream firm could potentially foreclose these rivals – to the benefit of its downstream partner – by degrading or impairing access to its data or even refusing to share the data altogether.

The first two types of concern have been the subject of a lot of talk, but have so far struggled to gain real traction in many merger investigations. There are good reasons for this:

- Concerns about consumers being forced to "pay" with data are predicated on the assumption that they would be unhappy to share their data with businesses unless "forced" to do so. But this idea runs into difficulties when looking at evidence of how people actually behave. A number of studies have identified evidence of the so-called "privacy paradox" whereby customers claim to value their privacy, but then appear to act in ways that suggest they place little value on it in practice. For example, many people repeatedly choose to share their data with a wide range of organisations without any deliberation and for little reward (introspective readers may want to consider the number of "cookie consent" boxes they have unthinkingly ticked when browsing the internet in the past month). Similarly, only a small proportion of internet users opt to take advantage of "increased privacy" settings or options for online services when these are available. Further studies have shown that, while consumers may value their privacy, they would nonetheless be happy to share some of their data if this allowed the businesses in question to fund themselves through targeted advertising and thereby offer their services to users free of charge. All this can make quantifying "bad outcomes" a difficult exercise.
- Similarly, "efficiency offence" concerns – while potentially valid in principle – are notoriously hard to substantiate in practice. To ground such a theory of harm in economic logic, it would be necessary to show that:
 - the merger would provide the resulting entity with access to data that it could deploy to make its service more attractive to its users;
 - rivals would be adversely affected by this improvement in the merged entity's service and so be less profitable;

- rivals would react to this loss of profitability by competing less fiercely (or not trying to enter the market in the first place); and
- the negative effects of this reduction in competition from rivals would outweigh the direct benefits to users of the improvement in the merged entity's service.

- All four of the conditions would logically need to hold in order for a merger to give rise to concerns. In practice, the third and fourth conditions are particularly hard to substantiate. Showing that rival firms would be placed at such a competitive advantage that they would effectively throw in the towel is no easy feat (and conflicts with competition authorities' standard view, which is that an improvement in the competitiveness of one firm's offer incentivises rivals to "up their game"). And weighing up the potential harm to consumers from the loss of competition against the benefit from an improvement in the merged firm's own services is even harder.

Despite these challenges, these worries can still feature prominently in merger investigations. For example, in its recent investigation into Google's acquisition of Fitbit, the European Commission questioned whether Google might use Fitbit's health data to improve the personalisation of its advertising, to the detriment of rival advertising channels. This worry was straight out of the efficiency offence playbook: it involved Google taking actions that would improve its service to advertisers and that could only prove detrimental if the improvement were so significant that it marginalised rivals and damaged competition. For its part, Google maintained that the Fitbit data was not useful in the way that the Commission was suggesting and that it had no intention of using it for these purposes. Perhaps for this reason, Google was willing to commit to a "data silo" remedy whereby it promised not to use Fitbit's data for its advertising services – even though it is debatable whether the Commission had thoroughly worked through all four of the steps necessary to ground an efficiency offence concern of this nature. Indeed, perhaps tellingly, the Commission only concluded in its [Decision](#) that it "could not exclude" such concerns, rather than claiming it had clearly substantiated them.

A CRITICAL INPUT?

This leaves the third category of concerns – foreclosing rival firms by refusing to provide access to data. On one level, the same worries would apply to any other "critical input" in a production process – be that a physical component in a manufacturing process, investment capital or technical know-how. Following the standard playbook, authorities would first need to establish whether the firms in question would have both the ability and incentive to withhold access to data and – if so – what effects this would have on competition and, ultimately, consumer welfare. These are not always easy questions to answer, but competition authorities in Europe and the US are well versed in investigating them in relation to other types of inputs. Indeed, such concerns are increasingly taking centre stage as the main theory of harm in merger investigations where the companies in question operate at different levels of a supply chain (a trend that we have explored in a [previous article](#)).

It is perhaps for this reason that input foreclosure theories of harm have assumed greater prominence in recent merger investigations involving data services. For example, data access concerns were a central theme in the European Commission's recent probe into the \$27bn acquisition of fintech data and analytics business Refinitiv by the London Stock Exchange Group (LSEG). The Commission ultimately cleared the deal after an in-depth investigation, but it made its approval conditional on LSEG committing not to

withhold or impair access to data generated by trading activities on its platforms from analytics businesses that are rivals to Refinitiv. Similarly, the Commission made its clearance of Google's acquisition of Fitbit conditional on Google promising to continue to provide access to Fitbit's health and fitness data to third-party software applications, to assuage any concerns that Google might foreclose competing apps by withholding access to this data.

LOOP THE LOOP

These investigations have also shown that "data" can have distinguishing features that they do not share with other types of input, a characteristic that can influence the way in which debates about input foreclosure play out. Perhaps most distinctively, data is often generated as the by-product of another economic activity: for example, a stock exchange will only generate valuable data about equity trading activity to the extent that it can attract traders to use its platforms; and companies such as Google and Amazon will only be able to throw out data about the interests and preferences of consumers to the extent that they can attract people to use their search engines and e-commerce platforms. This can have important implications.

First, the fact that data is a by-product can introduce feedback loops between the value of the data and the value of the economic activities that are generating the data.

- When business is good, these feedback loops can be self-reinforcing in a positive way: for example, the more people that use a search engine, the more it can learn about their preferences and tailor its algorithms to meet their needs, which in turn attracts even more people to the search engine.
- However, feedback loops can also go into reverse. Take, for example, a share trading platform: the "ticker" data that the platform generates is useful for those trading shares on the venue – after all, traders need to see what other transactions are taking place on the platform to make informed decisions about what stocks to buy and sell and when. When lots of people are using the platform, the data that it produces can be highly valuable. But if the platform were to restrict access to this data, people could be discouraged from trading on it in the first place – particularly given that they could trade exactly the same shares on a number of rival platforms for which real-time trading data was more readily available. This loss of business would damage not only the platform but also the quantity and value of the data it generated.

These feedback loops can therefore introduce a new type of dynamic risk into foreclosure strategies that hypothesise restricting access to data: even if a company's data is an essential input for rival businesses today, the very act of trying to leverage this dependency by limiting access to the data could reduce its value and potentially prove self-defeating. This stands in marked contrast to "standard" foreclosure cases, where restricting access to an input would have no impact on its value to businesses and could in fact increase the price that the input can command by creating artificial scarcity.

These feedback loops can make inhibiting access to data a risky strategy for businesses and complicate the assessment for competition authorities. However, the status of data as a by-product can also create a headache for companies looking to offer remedies to assuage any residual concerns that a competition watchdog might nonetheless have about input foreclosure.

- First, it can make “structural” remedies significantly more costly. In some merger investigations, the merging businesses might offer to divest the assets that competition authorities are worrying they could try to exploit – for example, if the concern focuses on one specific input into a manufacturing process, the merging businesses could potentially sell the relevant production line to an independent company in return for securing clearance from regulators for the rest of the deal. However, because data is often an inseparable by-product of another economic activity, it cannot be divested without also hiving off that activity. While this may still be possible, it could make for a hefty divestment.
- This may leave “behavioural” remedies – whereby businesses commit to refrain from certain practices (rather than divesting any assets) – as the only practicable option for some firms. However, once again the status of data as a by-product can restrict the range of behavioural remedies available. For example, a competition authority might want a guarantee that the business will charge a “fair and reasonable” price for its data so as to ensure that any rivals relying on this data are not unduly squeezed. However, when data is a by-product of another process, it can be difficult to determine what a fair and reasonable price would be. This is because the data and the underlying economic activity are inseparable, joint products. The business needs to be able to cover the costs it incurs in producing both. There is no single “economically correct” methodology for establishing what proportion of these costs should be recovered through fees for the data as opposed to fees for the underlying economic activity that is generating the data.
- In practice, this may leave simpler “access” remedies – in which the merging companies promise to make their data available to third parties on a non-discriminatory basis, but do not specify what fees they should charge – as the only practicable remedy that businesses can offer.

In many situations such access remedies might still be acceptable to a competition authority. In the recent LSEG/Refinitiv transaction, for example, the European Commission accepted a commitment by LSEG to continue to provide access to its data to competitors without stipulating the exact prices that LSEG should charge. However, other watchdogs may be more sceptical. The UK’s Competition and Markets Authority (CMA), for example, has repeatedly made it clear that it has a strong preference for structural remedies over behavioural commitments. Indeed, the CMA’s chief executive recently [strongly hinted](#) that it would have rejected the data access remedy package that the Commission agreed with Google in its Fitbit investigation, had the CMA had jurisdiction over these deal. With many European transactions now needing to gain clearance from the CMA as well as the Commission following Brexit, the CMA’s scepticism could be about to become much more of a headache for data-intensive businesses.

NOT REVOLUTION, BUT EVOLUTION

What conclusions can we draw? First and foremost, it is not necessary to rewrite the rulebook from scratch to take account of data concerns in competition investigations. As noted above, data on one level can be viewed as just another input into the production process – like capital, technology and expertise. Moreover, the concerns around access to data that competition authorities have explored in recent merger cases are not fundamentally different to those they have addressed in relation to these more conventional inputs. Nonetheless, the distinctive features of data can certainly colour the way in which the assessment of these concerns plays out. In particular, the fact that data is both an output of and an input into production processes – and the feedback loops that this can create – can shape both the competitive effects of mergers

and the hunt for remedies to address any worries about these effects. As to the prognosis for getting any form of remedy package past the CMA to tackle data access concerns in future cases? Well, more data is required...

AUTHORS

JAMES BAKER
Associate Director

WANT TO KNOW MORE?

WWW.FRONTIER-ECONOMICS.COM

HELLO@FRONTIER-ECONOMICS.COM

+44 (0) 207 031 7000