CENTRE FOR EUROPEAN REFORM
LONDON ★ BRUSSELS ★ BERLIN

Insight

# The EU's plan to unlock industrial data needs a rethink

by Zach Meyers, 8 July 2022

**The EU's ambition for industry to better exploit data is a worthy and realistic one. But expanding some of the GDPR's rules to industrial data would be a mistake.**

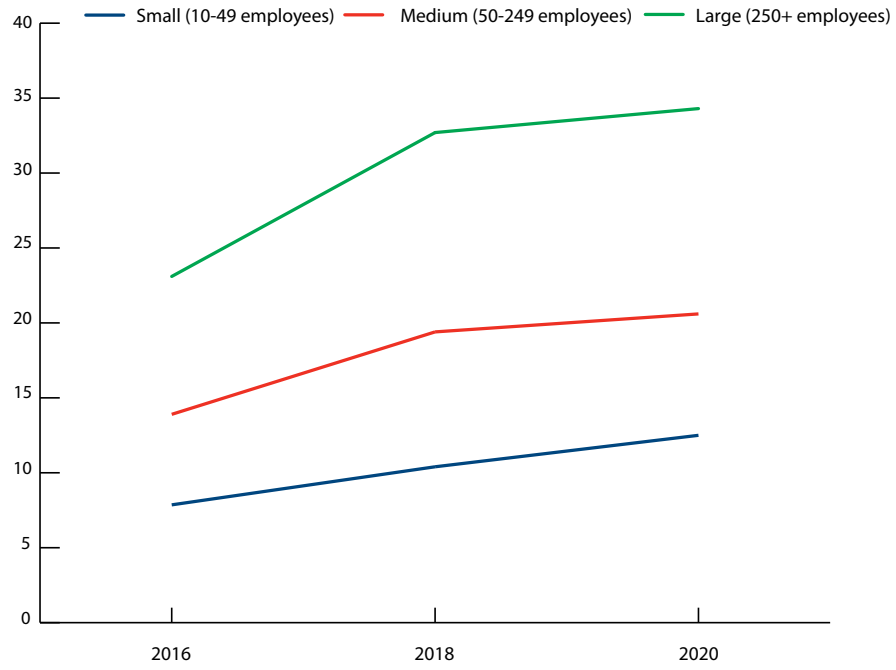
In recent years, the EU has cemented its status as a first-mover in tech regulation. Having completed the Digital Markets Act and the Digital Services Act, EU member-states are now turning to another digital priority: fulfilling the 2020 data strategy. The strategy encourages European firms and governments to better exploit industrial data, which can essentially be defined as any data which is not personal.

Industrial data is a sensible focus for Brussels. Europe has failed to create large-scale, consumer-oriented digital giants of the scale of Google and Microsoft. But the EU remains an industrial powerhouse. It therefore has a realistic chance of becoming a global leader in the 'Internet of Things' – consumer or industrial devices which are networked and continuously communicating data which is not always linked to identifiable individuals. These devices could include connected cars, medical devices, factory sensors, industrial robots and usage data from smart household appliances. To lead in these areas, European industry will need to adapt quickly: economic value in the Internet of Things sector is quickly moving away from hardware and towards software and services, such as artificial intelligence systems which use industrial data, which are not Europe's traditional strengths.

The EU has already passed sensible regulations to help unlock commerce in industrial data – so that data can be obtained by firms best placed to exploit it. For example, the EU requires public authorities to open up their datasets; it removed barriers to non-personal data transfers within the EU; and lawmakers recently agreed the Data Governance Act (DGA) to encourage voluntary data-sharing in the private sector. The Czech presidency of the EU is now prioritising the Data Act, a ground-breaking proposal by the European Commission. The proposal represents a radical departure from the EU's (sensible) 2020 data strategy. The Data Act instead applies concepts from the General Data Protection Regulation (GDPR) – which protects personal data – to industrial data. That is a bad idea, given growing evidence that the GDPR has reduced innovation by small firms.

The Data Act aims to address the concern that 80 per cent of industrial data collected in the EU is never used. To some extent, this seems to be a valid concern – only a minority of EU firms use big datasets, and for medium and large businesses the figure is starting to flatline (Chart 1).

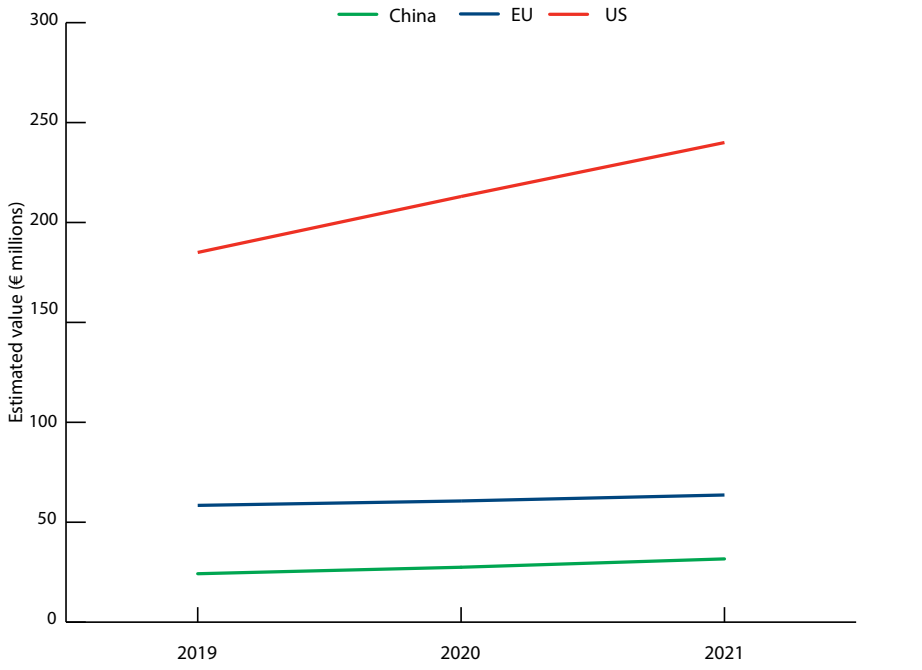
**Chart 1: Percentage of EU enterprises analysing big data**




*Source: European Commission, Digital Scoreboard.*

Furthermore, as Chart 2 shows, the EU's data market – the aggregate value of demand for digital data in the EU – significantly lags the US. The EU is not currently on a trajectory to catch up.

**Chart 2: Value of the data market in the EU, US and China**




*Source: European Commission, Data Market Study.*
*Note: "Data market" means the marketplace where digital data is exchanged as "products" or "services" as a result of the elaboration of raw data.*

Most economic value from the Internet of Things will arise from the analysis of data in worksites and factories – which could generate large productivity gains – rather than in consumer-facing digital services where the US is stronger. Given its manufacturing base, Europe could therefore disproportionately benefit – if its existing businesses learn to harness the potential of data, or if it manages to better nurture data-centric start-ups.

The Commission identifies a range of reasons why data is not being shared with those who could benefit from it – including uncertainty about legal ownership, lack of trust about how it would be used, and the 'hoarding' of data by a few large firms to maintain their competitive positions. But rather than addressing these specific problems, the Data Act wrestles control of industrial data away from device manufacturers and gives it to users (such as consumers or industrial customers). Device users could, for example, force manufacturers to provide data collected by their device to any third-party firm. This 'data portability' right already applies to personal data under the GDPR. But applying it to industrial data would undermine innovation in the EU's data economy.

First, consider how it affects device manufacturers' incentives to generate and collect data. If manufacturers are collecting data for later use, this suggests they are doing so because they hope to discover an innovative use for it in future. The Data Act will make such innovations more difficult – it will increase the cost of collecting that data, because products will need to be redesigned so any data collected is accessible to the user or transferable to a third-party, and the manufacturer would no longer be able to exclusively profit from the data. Manufacturers will probably respond by simply collecting less data.

Second, consider firms which may try to use the Data Act to obtain this data. They will struggle to innovate. The Data Act would prohibit them from using the data to compete with the manufacturer's device – a protection intended to protect manufacturers' incentives to collect data – and they could only use the data for purposes agreed with the device user. So data could probably only be used to serve so-called aftermarkets, such as repair and maintenance of the device. That may improve competition in these aftermarkets, but is unlikely to create major innovations, which require the ability to freely experiment. Radical innovation – such as 'training' artificial intelligence models – also requires vast amounts of data. However, the Data Act would require recipients to obtain individual consent from each user whose data they collect. This will make it unnecessarily difficult to obtain data at scale, compared to negotiating with a single manufacturer to buy information *en bloc*.

Many firms would also find it hard to use data they receive under the Data Act. They will only receive data of the type, format and quality that the manufacturer happens to collect. The Data Act includes no requirement for device manufacturers to collect new data (even if this is essential to create a new service) and no provisions for standardisation (so data recipients could integrate different manufacturers' datasets) or for data quality (so data is trustworthy enough for the recipient's intended way of reusing it). These would all be important so that firms could create new datasets and combine existing datasets to create new value. Imposing any of these requirements would be difficult to justify given their cost and complexity: standardising transfers of simple types of data like phone numbers and banking data has taken many years. But the failure to do so means the benefits of the Data Act will be relatively limited.

Rather than adopting sweeping GDPR-style rules – which try to impose uniform data-sharing requirements for sectors as varied as healthcare, transport, consumer appliances, and industrial sensors – the EU should stick to its 2020 data strategy. That strategy rejected widespread mandatory data sharing. Instead, the EU should continue to increase firms' incentives to collect data by strengthening

their intellectual property rights; continue to use competition law to encourage greater data-sharing by dominant firms; and make targeted regulatory interventions in particular sectors, where there is evidence that the benefits of data standardisation and mandatory sharing outweigh the costs. The EU is making progress in particular sectors, such as in the automotive industry, and the UK is taking a similarly targeted approach focused on energy and finance. Regulating data access comprehensively in these sectors would be more effective than applying the same broad-brush but ineffectual rules across the entire data economy.

Next, consider cross-border data transfers. Reducing barriers to these transfers is essential to digital trade: cross-border data transfers allow technology firms to operate more efficiently; lower the costs of entering new markets; and enhance competition. They especially disadvantage EU tech firms, because global firms can usually better afford the resources to segregate EU customer data so it does not leave the EU. Yet the EU has imposed tough restrictions on these transfers.

The GDPR's constraints on cross-border personal data flows are already costing the EU and countries which do business with it. Under the GDPR, EU nationals' personal data can only be moved to another jurisdiction without additional safeguards if the EU has decided the other jurisdiction provides equivalent protection to the GDPR (a so-called adequacy decision). The US, for example, has painstakingly negotiated arrangements with the EU to allow seamless transfers of personal data to continue. But those arrangements have been repeatedly struck down by the European Court of Justice, most recently in July 2020, because the court was worried US authorities had excessive powers to demand European citizens' personal information. Despite European and American officials working frenetically to develop a replacement adequacy arrangement, and announcing an agreement in principle, the details of the new arrangement are still not settled. In the meantime, the EU's data protection authorities have increasingly ruled that EU-US personal data flows should not continue at all, even with the additional safeguards companies have put in place.

Restrictions on transferring personal data can at least be justified by privacy concerns. But the EU has recently expanded these GDPR-style restrictions on cross-border flows to industrial data. The Data Governance Act forces public authorities, and certain firms, to take "all reasonable technical, legal and organisational measures" to prevent data from being accessed by foreign governments, if this would conflict with European law. The Data Act would now extend this to cloud computing providers (firms which store and process industrial data as a service). The Commission is also reportedly asking the EU's cybersecurity agency to require that cloud computing providers store data in Europe and are immune from foreign laws – for example by being headquartered in Europe – to obtain the highest level of security certification.

These are all perceived by many commentators to be tactics to marginalise US cloud computing giants and protect European equivalents. The EU's impact assessment implies Chinese and American intelligence gathering is of equivalent concern: a strange comparison, at a time when EU and US co-operation has never been more important. The rationale for limiting cross-border personal data transfers was to protect EU nationals' privacy rights. There are fewer justifications for banning transfers to protect EU firms' intellectual property. Firms can make their own risk-based decisions about which cloud computing services meet their needs, including providing adequate protection of their intellectual property.

The Data Act therefore seems likely to require firms with European industrial data to store more of it in Europe. That may be a boon to European cloud computing services – which the EU is desperate to

help compete against US giants. But, overall, it will harm the EU's data economy, by preventing cloud computing firms from leveraging global infrastructure and scale, imposing significant costs on firms engaged in cross-border trade in data, and preventing the EU data economy from being integrated with the rest of the world.

Europe has the potential to be a global leader in the Internet of Things, unlike consumer-facing tech, which is often based on commercialising personal data and where most European firms struggle to go global. It is therefore surprising that the Commission wants a regulatory model for industrial data which is adapted from how the GDPR controls personal data. The GDPR's rules may have set an important regulatory standard and helped assert Europe's fundamental values – but they do not seem to have European firms much competitive advantage over US digital platforms.

To take advantage of industrial data, the EU would be better off protecting firms' incentives to collect that data and keeping its regulatory interventions targeted. Even more importantly, it needs to ensure funding is available for firms to invest in radical data-based innovation. The Commission's announcement of a New European Innovation Agenda seems to recognise the importance of enabling European tech firms to obtain patient, risk-tolerant sources of private finance and of reducing regulatory complexity. The Data Act is the wrong approach and will not help Europe achieve its potential.

**Zach Meyers is a senior research fellow at the Centre for European Reform.**