

PRO- AND ANTI-COMPETITIVE PROVISIONS IN THE PROPOSED EUROPEAN UNION DATA ACT

BERTIN MARTENS

The proposed European Union Data Act gives users access and portability rights to the data generated by their use of tangible digital products and devices. This pro-competitive measure weakens the *de-facto* monopolistic control product manufacturers have over product data. However, the Data Act would also grant manufacturers a *de-jure* right to monopolistic pricing of data transfers to third-party service providers, restoring their control over data markets. Other anti-competitive provisions include restrictions on the use of data for competition purposes and a prohibition on transferring data to platforms identified as gatekeepers under the EU Digital Markets Act. Unnecessarily fuzzy definitions of products and data that fall under the Data Act would create uncertainty in implementation and incoherence with other EU data regulations. The Data Act should be simplified by dropping anti-competitive provisions and granting users and third-parties selected by users free access to all data generated by the use of a product or a service. This would increase competition in data-driven services and prevent users paying twice for their data. It would not disincentivise producers from investing in data-driven products and services. A further step could be the creation of a level playing field between producers and users in data-access rights. This can be achieved by introducing the principle of mutual exhaustion of data rights at point of sale. This would put all data co-generating parties in a position to generate economies of scale and scope in data aggregation, or data-driven externalities, to maximise innovation.

I am grateful to Wolfgang Kerber, Jan Kramer, Inge Graef, Thomas Tombal, Jeromin Zettelmeyer, Christophe Carugati and participants in TILEC and Bruegel workshops on the Data Act, for their valuable comments.

Bertin Martens (bertin.martens@bruegel.org) is a Visiting Fellow at Bruegel and a non-resident research fellow at Tilburg University Law and Economics Centre (TILEC).



Recommended citation:

Martens, B. (2023) 'Pro- and anti-competitive provisions in the proposed European Union Data Act', *Working Paper 01/2023*, Bruegel

1 Introduction

Modern digital economies are replete with connected internet-of-things devices, including in home appliances, buildings, cars, industrial machines and medical devices. These devices contain physical sensors that collect analogue signals – light, sound, temperature, physical movement – and convert them into binary electronic data. Data is processed by embedded software, or communicated to remote servers for further processing. Device manufacturers can design open or closed data architectures. With closed architectures, technical-protection measures at hardware and software level prevent device users from accessing the data directly. Manufacturers retain exclusive control over the data and become *de-facto* owners of the data. Device users can only access the data in line with the monopolistic terms and conditions set by manufacturers. Open data architectures, by contrast, increase competition in upstream data markets and in downstream data-driven services markets.

The European Union's 2016 general data protection regulation (Regulation (EU) 2016/679, GDPR¹) took a first step towards the freeing of personal data collected by digital devices or in online services from exclusive control by manufacturers. It introduced several data rights for natural persons as data subjects, including the right to access, delete and port personal data, and the obligation of data controllers to obtain data subject consent for collection of their personal data. However, the GDPR says nothing about access to non-personal data, such as business data, or access rights for businesses that are legal entities.

The recognition that data access rights are important culminated in the European Commission's February 2022 proposal for a Data Act (DA; European Commission, 2022a), which would open up the data architecture of digital devices by introducing a data access right for device users, including the right to port data to a third-party of their choice². The DA takes a balanced approach that combines a strengthening of user rights with strengthening of the manufacturer's position, by granting the latter an exclusive right to negotiate a contract with users and third parties, charge a price for third-party data access, and other restrictions on the use of device data in services markets. This combination of pro- and anti-competitive provisions looks very similar to the economic logic that underpins intellectual

¹ Available at <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

² The DA covers other issues as well, including government access to business data, switching between cloud services and data interoperability standards. This paper discusses chapters I-III of the Data Act, which focus on access to 'product' or device data.

property rights (IPR), with monopolistic rights that result in static welfare losses that are compensated for by dynamic welfare gains from incentives to continue to invest in collecting data.

In this paper we address two research questions. First, we discuss to what extent the DA's mandatory data access rights for users will effectively weaken the device manufacturer's monopolistic control over user data and open up competition in data-driven services markets. This analysis takes a vertical-integration perspective, between upstream data markets and downstream data-driven services markets. It starts with the main pro-competitive provision in the DA, which grants 'product' or device users access and portability rights to the device data. It discusses the scope of these access rights in terms of the definition of 'products' or devices, and the type of data that falls within the scope of the DA. It assesses to what extent these definitions might promote or distort competition in data and data-driven services markets. It then explores several anti-competitive provisions, including monopolistic third-party data pricing rights for device manufacturers and data holders, and the prohibitions on using data to compete in product and services markets, and on porting data to platforms that are designated as 'gatekeepers' under the EU's 2022 Digital Markets Act (Regulation (EU) 2022/1925, DMA³).

We find that the combination of data portability rights for users and the right to monopolistic data pricing for device manufacturers tilts the balance in the data value chain in favour of the manufacturer and data holder, at the expense of users and third-party service providers. In line with other scholars (Kerber, 2022), we conclude that the DA *de jure* endorses a *de-facto* exclusive data control right for the device manufacturer, by introducing a quasi-IPR-like data right. Manufacturers already have classic IPR instruments at their disposal to protect and incentivise their investment in data-collection hardware and software in devices (Antoine and Leistner, 2022). Moreover, fuzzy definitions of the scope of the DA create uncertainty in implementation, and may result in distortions in device markets and data-driven services markets. Other competition-restricting provisions in the DA create unnecessary obstacles to the development of data markets and innovation in data-driven services markets. As a result, the DA is likely to have, at best, an ambiguous impact on competition in these markets, and may slow down innovation.

We recommend the elimination of anti-competitive and market-distorting provisions in the DA, including the third-party data-pricing right for manufacturers and data holders, the prohibition on porting data to DMA gatekeepers, and other direct restrictions on the use of data for competition purposes. The scope of the DA could be clarified by applying DA portability rights to all non-personal data generated by the use of devices, and extending its application beyond devices to services. These

³ Available at <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>.

policy recommendations are not new. They are already applied in several other EU data-regulation instruments, including the DMA and the proposed European Health Data System (EHDS, European Commission 2022b). These recommendations would contribute to greater coherence and reduced uncertainty in the rapidly emerging EU data-regulation structure, a vast and complex political-economy project in the making. While the DA remains silent on data rights for producers, we also explore the potential implications of creating a level playing field between data-access rights for producers and users.

In a second step, we take a wider perspective on the social value of co-generated data and market failures that may prevent realisation of social value in data-driven services markets. Once collected, data is non-rival and can generate economies of scope in re-use for a wide variety of purposes, without functional loss to the original use, though some uses may compete with and result in private economic loss for the original user. Data can also generate economies of scale and scope in data aggregation, or data-driven network effects. These externalities make aggregated datasets more valuable than segmented datasets. Obstacles to aggregation constitute market failures in data markets.

The DA does not address data-driven network effects. It assigns data access rights to product users and assumes implicitly that producers have full access to product and related services data. That may not necessarily be the case. Producers are in a better position to generate economies of scale and scope in data aggregation, or data-driven network effects, because they can aggregate data across many users; users only have access to their own user data. Granting producers the same data access rights as users would not only restore the level playing field between the co-generating parties – in case that field is distorted – but would also enable producers to generate data-driven network effects that may contribute to further innovation in data-driven services. We recommend that the social value of data could be maximised by introducing the concept of mutual exhaustion of data rights, for producers and users, at the point of a data product or service sale, subject only to restrictions related to pre-existing rights for the parties, such as GDPR rights for personal data or trade secrets for business data.

This paper is structured as follows. Section 2 presents the main pro-competitive provision in the DA, giving users access and portability rights to device data. It explores the scope of this right with regard to the definition of 'products' and user data. Section 3 presents third-party data-pricing rules and explores the economic implications for data markets and data-driven services markets. Section 4 focuses on the prohibition on porting of data to large platforms that are designated as gatekeepers under the EU Digital Markets Act (DMA). Section 5 examines other anti-competitive clauses that

prohibit the use of product data for design of competing products or services that affect the welfare of any of the parties involved. Section 6 explores economies of scale and scope in data aggregation and proposes the introduction of mutual exhaustion of data access rights at point of sale, as a means to maximise the social value of data. Section 7 summarises and concludes with some policy recommendations.

2 The Data Act opens access to product data

The proposed DA constitutes a regulatory intervention in digital data markets. It imposes mandatory data access rights for users of 'products', thereby circumventing any access rights negotiated or offered in commercial markets⁴. What type of market failure justifies this regulatory intervention?

Whether closed architectures result in product and/or service market failures and justify regulatory intervention depends on the relationship between device markets and aftermarket for related services produced after the purchase of the device. According to the Chicago Critique (Posner, 1978), there is no need for regulatory intervention when device markets are competitive and users have sufficient information on aftermarket services costs at the time of buying a device. Prospective buyers can add up the cost of the device and aftermarket services to compare the joint cost between competing devices. That simple formula works well when it is relatively easy to predict aftermarket services costs, for example, running and maintenance requirements for cars⁵. This is much harder for most digital devices because the data they generate enables consumption of a wide range of data-driven services, often provided through apps, with variable quantity and pricing options that are hard to predict, especially when technology and services markets are evolving fast. Most of these services are experience goods that can only be evaluated after initial use. Device users may remain trapped with a device and service that is no longer competitive. Hence regulatory intervention is important to ensure effective competition in data markets and data-driven services markets by opening up the data architecture. This enables users of digital devices to separate the choice of device and aftermarket services.

⁴ For a more detailed overview of provisions in the DA, see for example Colangelo (2022), Graef and Husovec (2022), Habich (2022), Perarnaud and Fanni (2022), Efroni *et al* (2022).

⁵ This is why EU competition policy allows an exemption on restrictions on vertical agreements in the motor vehicle sector under the EU Motor Vehicle Block Exemption Regulation 461/2010. For a more detailed discussion of the relationship between competition law and mandatory data access provisions, see Picht (2022) and Schweitzer *et al* (2022).

The producer-user relationship envisaged by the DA applies to wide range of industrial and services settings. In a complex industrial production chain for example, there may be many producer-user pairs. A firm runs a production process that uses many machines, produced and sold or leased by other firms. Each of these machines, in turn, may consist of several data-generating components produced by other firms. DA Recital (20) suggests that multiple owners or leasing parties should be given access to the data, but component producers should not, unless they retain an active role as a provider of data. The DA remains silent on the rights of data producers. The implicit assumption in the DA is that producers are in fact data holders and should give users access to the data. The reverse situation may occur, whereby users become data holders and producers have no access to the data. For example, a manufacturer of industrial robots assembles several data-producing components, produced by other firms, into a robot. The DA does not grant component producers access to their component data in that case. These data could be useful for the component manufacturer to improve the quality of his components.

With the DA, the European Commission has proposed a horizontal cross-sectoral approach to open access to digital data. It would be too cumbersome to study potential market failures in each and every product market and examine whether the Chicago Critique conditions would be applicable. As such, the DA has potentially a very wide reach across the entire digital economy, just like the GDPR. That brings us to two other key elements that determine the scope of the DA: the products and data affected by the regulation.

2.1 What is 'product' data?

The DA grants product users free access to all "*data generated by the use of a product*" (Art 3.1). That introduces the new concept of 'product' data into EU legal jargon, alongside the existing distinction between personal or non-personal data introduced by the EU GDPR. It also begs the question about the distinction between 'product' and 'non-product' data. DA Art2(2) defines a product as a tangible item that collects data concerning its use, is able to communicate data via a publicly available communications service, and whose primary function is not storing and processing data. According to Recital (14), this may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery. Recital (15) adds that personal computers, tablets, smart televisions and speakers, cameras, webcams and sound recording systems are not to be considered as products, and their data should consequently not fall into the category of product data.

Recital (14) moreover specifies that data inferred or derived from product data should not be considered within the scope of the DA. As noted in the introduction to this paper, the notion of ‘machine’ data, or data generated by a tangible physical product, has lingered around at least since the European Commission (2017) communication on data policy. The DA proposal still reflects this thinking with the introduction of ‘product’ data.

The GDPR introduced the distinction between personal and non-personal data and marked the start of various attempts to split data into different categories. The debate on the borderline between personal and non-personal data has never really been settled and leaves an ambiguous grey zone. The DA could have started from the residual category of non-personal data. Instead, the authors decided to introduce a new criterion to categorise data: product data.

The origins of European Commission thinking about machine or device data as a separate concept go back several years when, in line with Zech (2015), the European Commission (2017, pp 10-13) suggested the introduction of a data producer right that would give the owner or user of a data-enabled device an exclusive right to non-personal ‘machine’ data. Others objected to this exclusive right because it would fragment access to co-generated data and increase transaction costs in data markets (Kerber, 2017; Drexler, 2018). Since then, the idea of granting exclusive data ownership rights to a single party has gradually been abandoned⁶ and replaced by access and use rights for multiple parties. Data is usually co-generated between at least two parties who have a stake in the data and can claim access rights. However, the concept of ‘machine data’ has continued to float around. It resurfaced in the European Data Strategy (2020, p 21), which previewed the DA, and has now been given legal status in the DA. This is problematic.

Digital data does not float in thin air. All data require tangible electronic devices (products, machines) that combine hardware and software to collect, store, process and transmit data. Data that registers physical phenomena, such as user behaviour or environmental conditions, requires physical sensors that convert analogue into digital signals. Conversely, interaction between digital machines and humans requires conversion of digital electronic signals into analogue output that can be interpreted by humans. In that sense, all data is product or machine data. The dichotomy between product and non-product data is therefore artificial and makes little sense in a digital world. The DA implicitly acknowledges this. In order to maintain the idea of product, device or machine data as a separate category, it introduces a rather arbitrary distinction between products that are included (Recital 14) and excluded (Recital 15) from the scope of the DA. Creating a category of products that do generate

⁶ Though arguments in favour of data ownership rights keep popping up. See for instance Donewald *et al* (2020).

data but do not fall under the definition of product data, makes the problem even more complex and inevitably leads to borderline disputes.

These disputes already started before the DA was proposed. During preliminary discussions in the Council of the EU, the Czech Presidency of the Council in July 2022 noted that *“smart watches have a strong element of collection of data on human body indicators or movements and should thus be considered covered by the definition of ‘product’”*⁷. One could make exactly the same argument for laptops, smartphones, cameras and other devices that have been excluded from the category of ‘products’. For example, would agricultural field data collected on a smartphone or tablet be exempted from the application of the DA, while the same field data collected by a device integrated into a tractor would be subject to the DA? Many home and industrial appliances today are managed through apps that operate on smartphones and tablets. The apps are intermediaries between the sensors and the data holder who uses edge processing and communication capabilities on these devices to transmit (pre-processed) data to his own servers. Since Recital (15) excludes these devices from the DA data-governance regime, data access rights would not apply when these devices are used for data collection. This creates a loophole for manufacturers and data-based service providers to circumvent the DA and distort competition in data markets by moving their services to these devices. Medical and health devices have been included in the ‘product’ category and should thus fall under the application of DA rules. But what if medical data are collected by a smartphone that is not considered to be a ‘product’? Fortunately, the European Commission’s (2022) proposal for a European Health Data System (EHDS) (2022) bypasses this border dispute in the case of health data devices. It ignores DA distinctions between product, non-product and services data, or between primary and processed data. That unified data approach could have been a template for the DA as well.

All these problems can be avoided by dropping the product definition in Art 2(2) and Recitals (14) and (15). There is no need for a definition of ‘products’ because all data is collected and stored on tangible products. Some products or devices already provide users with access to data and the possibility to transfer data to third parties. For example, most laptops, tablets and smartphones have very open data-access systems. Users can easily access and transfer the data collected and stored by these devices to any party of their choice. They already comply with the DA. Many devices have less open access systems and do not comply with the DA, or only partially. The DA will force them to open up

⁷ European Council document 11194/22 on the Data Act, 12 July 2022, available at <https://data.consilium.europa.eu/doc/document/ST-11194-2022-INIT/en/pdf>.

access to data. Art 2(2) could be replaced by a statement that declares all data generated by digital devices and services to be subject to the provisions of the DA.

The DA offers no useful purpose or rationale for the distinction between ‘product’ and ‘services’ data. The primary purpose of the DA could be to provide a horizontal data access regime that extends data access rights beyond the GDPR to non-personal data and for business users. The Business-to-Platform Regulation⁸ took some first steps in that direction. The DMA expanded these access provisions to non-personal data for businesses to core services data in very large gatekeeper platforms. The DA can generalise these user data access rights further to smaller businesses. The DA data-governance regime would then apply to any data collected by a device or a service. Dropping the definition of product data would avoid many anti-competitive distortions, or attempts to create distortions based on borderline disputes, in data markets and data-driven services markets.

2.2 What data does the DA cover?

Recital (14) states that product data *“represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data should not be considered within the scope of this regulation”*.

This raises a new question about the data covered by the DA: where is the borderline between primary and derived or inferred data? Recital 17 states that this excludes *“data resulting from any software process that calculates derivative data ... as such software process may be subject to intellectual property rights”*. This stretches IPR law beyond its current boundaries. It extends copyright protection of software code to the data generated by that software. This would be equivalent to, for example, Microsoft claiming IPR rights on data files generated by users of Microsoft Office software. Excel spreadsheets would only give users access to the primary data that they put into Excel files but not to data calculated by the spreadsheet. The Recital gives legal endorsement to a commercial strategy that has been tried by machine producers, for example in the agricultural sector (Atik and Martens, 2021). Perzanowski and Schultz (2016) discussed why this practice has no legal foundations.

If we take Recital 17 literally, almost all digital data could be classified as processed data. The digitalisation of user actions and events in an environment implies the conversion of analogue sensor

⁸ Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1150>.

signals (light, sound, mechanical movement, temperature, etc) into digital data. That conversion requires the use of software that derives digital output data from an analogue impulse recorded by a hardware sensor. In complex machines, digital output data from many sensors can be processed in local-area networks that steer processes in these machines. For example, modern cars have several local networks that handle engine and fuel functions, automatic gearboxes, breaks, etc, in function of the driver's behaviour. Connected and semi-automated agricultural machines include many sensors and processors of sensor data, as well as complex software processes that handle machine functions at a more aggregate level, depending on the user's instructions given to the machine. Moreover, agricultural machines may process combined data inputs from third parties, including land and soil mapping providers, agricultural inputs suppliers and agronomic advisory services, to optimise machine outputs. Farmers will want to access all these types of data. It is not clear to what extent the DA definition of accessible user data would effectively make all this data available to farmers.

The European Parliament rapporteur on the DA has proposed an amendment to Art 3(1) to clarify this (European Parliament, 2022): all data generated by the use of devices that are accessible to the data holder should also be accessible by users. This amendment creates a level playing field between data holders and product users. It discards the distinction between primary and processed data and replaces it by all data accessible to the data holder. This approach has already been tried in other EU data regulations. For example, the distinction has been dropped by some data-sharing obligations for gatekeepers in the DMA and primary data portability provisions in the EHDS.

However, the proposed European Parliament amendment has its own problems. Modern digitally equipped machines, including cars, aeroplanes, robots and smartphones generate huge volumes of data, much of which is for internal use to ensure the proper functioning of the system. Modern cars for example generate thousands of datapoints and signals between components of the vehicle. All these data are in principle accessible inside the vehicle, but only a small subset is exported outside the car and accessed by the car manufacturer for technical or business use. Access, storage and transmission to an external data server would require expensive storage and telecommunication capacity that would probably be more costly than the potential benefits, at least in the perception of the manufacturer or data holder. DA Art 3.2 leaves it to the manufacturer or data holder to inform the user about the data generated by usage of a product and how it can be accessed – again discarding the distinction between primary and processed data. The proposed amendment pushes the problem at step further: what do we mean by data accessible to the data holder? Other service providers and innovators may have use cases for existing but unavailable data, some of which are not necessarily in

the business interest of the manufacturer or data holder. The DA would allow the manufacturer to act in his private interest and declare this data not available. That is not necessarily in the interest of society.

The distinction between primary and processed data takes inspiration from the GDPR that gives natural persons access rights to data provided by a person but not to data inferred or derived from that data. However, not all EU data regulations follow this principle. For example, data-sharing obligations in the DMA go a step further and include market data generated in e-commerce platforms, search engine data and advertising data. All these datasets include at least to some extent processed data, such as responses to search queries, the outcome of pricing auctions for ads presented by advertisers and ad slots offered by publishers in advertising markets, and consumer demand and sales data in e-commerce platforms. The European Commission's (2022) proposed data sharing rules for the EHDS completely abandon the distinction between primary and processed data. User data processed by medical devices or even in medical services form an integral part of the data-sharing obligations.

Another reason for sharing processed data with users is that data is usually co-generated between the device manufacturer, data holder and user. The software response would not exist without user input, and user input would not be provided if a software response was not expected. Data co-generation illustrates why an extension of IPR-like provisions to data is inappropriate. Patents and copyright are not co-generated between an innovator and the users of that innovation; they are the innovator's sole product.

Recital (20) suggests that all parties that have ownership or contractual rights to a product should be considered as co-users and should have access to the data that the product generates. This refers to machine-leasing firms for example. However, co-generation goes beyond legal and contractual rights to the product or machine that generates data. It includes parties that share the physical and/or digital space from which the device obtains its data. In agriculture for example, a drone can be used to generate spraying maps and a spraying machine can implement this map. If drone, sprayer, land owner and farmer are different firms, they may claim (partial) access to each other's business data because there are bilateral contracts between the parties.

3 Data access and pricing rules

The DA would introduce a dual-pricing regime for data access: users have free access to the data, third-parties should pay for access. According to Arts 3(1), 4(1) and 5(1), users should have access to data generated by the use of a product, free of charge and in real-time, either directly in the product or indirectly through the data holder. Data should also be made available to a third party of the user's choice, though not free of charge. Third party data recipients should pay a fair, reasonable and non-discriminatory (FRAND) price according to Art 8(1) and Art 9(1)⁹, defined as marginal costs plus a reasonable mark-up, but short of a full profit-maximising monopolistic price. If the third party is an SME, it should only pay marginal costs without mark-up. Data recipients should conclude a contract ("*license agreement*") with the data holder and cannot re-sell the data to another party or re-use it for purposes other than those foreseen in the contract. These provisions bestow IPR-like quasi data-property rights on data holders. The proposed DA remains silent on the right of users to directly transfer their data to a third party in return for benefits¹⁰. We can assume that the DA does not want to open up this possibility because it would undermine the data holder's ability to charge a price to a third party.

The DA justifies this pricing regime as a means "*to preserve incentives to invest in products with functionalities based on the use of data from sensors built into that product*" (Recital 28). It is hard to see how free third-party data transfers would undermine that incentive. Data-collection hardware, sensors and software are embedded in a product when it is sold to the user. The manufacturer can recuperate that cost in the sales price, at the point of sale. Manufacturers may update the software but cannot update data collection as such. The underlying primary data collected by the product will not change, even when third-parties pay for a data transfer. Similarly, when a producer sells a data-based service to a user, the cost of data collection and processing is included in the price of the service. The incentive to produce that service will not disappear if the producer is forced to share the service data with a third party selected by the user.

This dual data-pricing regime leaves data control effectively in the hands of product manufacturers and data holders, unless users do their own data processing. It reduces competition and innovation in aftermarket services. While some users may be in a position to produce their own services, most users

⁹ The FRAND pricing concept is borrowed from Standard Essential Patent (SEP) licensing, another indication that the DA is inspired by IPR principles. SEPs became industry standards and confer a monopolistic position on the holders of SEPs, in return for a FRAND pricing of SEP licenses. There are no meaningful economic definitions of FRAND pricing, other than pricing below the profit-maximising monopolistic price. For a more detailed discussion of FRAND pricing rules from a competition law perspective, see Picht (2022), Picht and Richter (2022) and Metzger and Schweitzer (2022).

¹⁰ Users will only sell data to a third party for other purposes than providing services to the user, because that would increase the price of the third-party service to the user.

will outsource the production of a data-driven service to a third party. The price paid for the data by that third party will be at least partly reflected in the cost of the service delivered to the user. Despite the DA's good intentions, expressed in Art 4(1), user access to their own data is not free in this pricing mechanism. Attenuated monopolistic pricing still enables data holders to appropriate and monetise at least part of the user's and third-party's surplus from data use. Moreover, this may trigger a double marginalisation problem (Staahl *et al*, 2019) when both the data holder and the third party service provider are in a position to set profit-maximising prices. That would drive up prices for data-driven services beyond efficiency levels.

We can observe the implications of a similar data-pricing regime in the automotive sector. The EU Type Approval Regulation (Regulation (EU) 2018/858) mandates access to car maintenance and repair data for independent service providers that are not part of the manufacturer's network of official dealers. However, the regulation also allows manufacturers to charge a price for the data. Hoegaerts and Schönenberger (2019, p 99) estimated that this increases the price of independent maintenance services by six percent, and possibly more depending of the number of data points that need to be retrieved. Applying the DA to cars will not change that. DA data-access provisions would only make a difference for car users who produce their own data-driven services. For example, car-rental firms and fleet managers may access the data to keep track of usage, performance and maintenance requirements in their fleets.

The DA goes a step further than the Type Approval Regulation. DA Art 8(3) prohibits price discrimination between third-party data recipients and recipients affiliated (vertically integrated) with the data holder or product manufacturer. Vertically integrated service should either be considered as a third-party service and be charged the same price, or pricing should be zero for all parties that offer a similar service. That could in principle restore the level playing field for access to data between official dealers and independent service providers. However, there are many ways to hide data price discrimination in the multifaceted contracts between car manufacturers and official dealers. It is not clear how the prohibition against price discrimination can be verified and enforced. The Digital Markets Act proposes a more transparent anti-discrimination mechanism for vertically integrated gatekeeper platforms. Rather than a data price rule, DMA Art 6(1) sets a data access or quantity rule: vertically integrated firms should not have access to market data, or all competing firms should be given equal access to the data. The latter is easier to verify.

The marginal cost pricing rule generates considerable uncertainty because it is subject to a wide range of interpretations. The automotive sector again illustrates this point. Manufacturers can make the data

directly available through an On-Board Diagnostics socket inside the car, as they have done for several decades. Installing that socket is a fixed cost that can be recuperated through the sales price of the car. With the arrival of digitally connected cars however, manufacturers started to collect car data on remote servers. Access to the data is diverted from the car to these servers. Running this remote data-server system entails not only fixed but continuous operational costs. Should all these costs be added to the marginal cost of data access, or is the near-zero direct access cost the appropriate benchmark for a 'reasonable' price? Similar situations can occur in most connected devices. The DA (Recital 21) would allow both for direct and indirect access to the data, possibly through remote cloud servers operated by a third party designated as data holder on behalf of the manufacturer. That does not help to clarify marginal cost pricing and may constitute another point of friction in user access to the data.

The European data regulation landscape is becoming increasingly fragmented with respect to data-access pricing. The recently proposed EHDS regulation (European Commission, 2022b) mandates free of charge patient health data transfers between medical service providers. Health data is personal data subject to the provisions of GDPR Arts 20 and 12, which mandate third-party data portability free of charge. It is difficult to see how the EHDS could have proposed a positive data access pricing rule.

Pricing of third-party data access exists in some sector regulations. For example, the EU Second Payment Services Directive (Directive (EU) 2015/2366) sets a "*reasonable price*" for transferring account data from banks to payment service providers. Payment service providers are competitors as well as complementors of retail banking services. They reduce transaction costs for all parties involved in a payment, in return for a fee, part of which is recuperated by banks through a third-party fee to access the data. As long as these fees remain marginal compared to the value of the transaction and do not eliminate the reduction in transaction costs, they will not negatively affect the transaction. That explains the success of the Second Payment Services Directive in terms of promoting strong competition in payment services markets. However, the example from car maintenance services above shows that this outcome is not guaranteed.

There is also uncertainty with respect to the scope of application of data-access pricing rules in the DA. It covers all "*product data*", which may include personal as well as non-personal data. DA Recital 30 confirms that processing of product data remains subject to the GDPR, "*including where personal and non-personal data are inextricably linked*". This may trigger a second bifurcation in the data-access pricing regime, with personal (and mixed) data still subject to the GDPR's free-of-charge data transfer to third parties. This suggests that the type of data, rather than economic reasoning, matters to determine the third-party access pricing rule.

4 The prohibition on porting data to DMA gatekeepers

DA Art 5(2) would prohibit data transfers to very large third-party platforms that have been designated as 'gatekeepers', or very large, hard-to-avoid platforms, under the DMA. In practice, this implies that it is unlikely that data can be transferred to platforms operated by companies such as Apple, Google, Amazon, Microsoft or Meta. This prohibition is presented as a pro-competitive measure. From a competition perspective, gatekeepers already collect huge data pools that reinforce their market power (Crémer *et al*, 2019). The prohibition would prevent a further increase in that data-driven market power. This section argues that this is a one-sided view that ignores the competition-enhancing effects of platforms and the welfare-increasing benefits of network effects in platforms. It explores the transmission mechanisms for the potential welfare-reducing and anti-competitive impact of this prohibition. These negative welfare effects occur particularly when gatekeepers play an intermediary role that reduces transaction costs in services markets and economies of scope in the aggregation of market information (Carballa-Smichowski *et al*, 2022).

Two examples, from the automotive and smart home services sectors, illustrate how this prohibition creates data-portability bottlenecks that reduce users' choices, competition in downstream services markets and network benefits that users could derive from their internet-of-things devices.

In modern cars, Apple's CarPlay and Alphabet's Android Auto are the dominant in-car operating systems (OS) that potentially enable users to install a variety of aftermarket car services apps. Users are familiar with these OS outside the car. They facilitate seamless synchronisation with other mobile and home consumer devices. The OS retrieve data directly inside the car through an interface that converts the specific data format of the car brand and model to a standard format so that app developers do not have to re-write their apps for every car model. The OS in principle enables users to install an alternative navigation app to replace the manufacturer's default navigation service, or maintenance apps from their preferred independent maintenance service provider, or price comparison apps to assist them in the selection of the cheapest maintenance provider. Intermediary service providers, such as car rental and fleet management companies, could implement their own car services in these OS without the agreement of the manufacturer. That would put the Apple and Android OS in competition with the car manufacturer's own OS that has exclusive access to mechanical and navigation data. Manufacturers' OS offer few apps, selected by the manufacturer and designed to direct users towards the manufacturer's own aftermarket services or preferred service providers. Some manufacturers operate app stores. But they do not allow apps from competing service providers. For

the time being, car manufacturers apply technical protection measures to preserve their exclusive access to mechanical and navigation data. As a result, Apple and Android OS are limited to media and entertainment services that are not based on car data.

The DA's data access and portability rules would apply to cars and would eliminate car manufacturers' exclusive access to car data (Gill, 2022). However, the prohibition against transferring data to core platform services offered by DMA gatekeepers, such as app stores and operating systems, effectively prevents any change in that situation. This reduces competition in data-driven services because drivers' choices would be limited to services and apps offered by the car manufacturer. It also prevents seamless integration of car data services across applications in cars, home devices, smartphones and other digital devices. Car manufacturers will benefit from these restrictions in competition; car users will lose.

In principle, the DA opens up possibilities for independent service providers to circumvent these restrictions and develop their own apps outside the Apple and Android ecosystems. In practice, there are many obstacles on this alternative route. The DA does not impose an obligation on car manufacturers to open an app store within their own OS, or to open the app store to apps from competing service providers. Independent service providers could also put their apps in the Apple and Android stores and ask users to download them to their smartphones instead of directly into their cars. App developers would then have to transfer car data from a central server operated by the car manufacturer to the smartphone. This may create latency problems for time-critical apps. Inside the car, small smartphone screens would compete for attention with the manufacturer's larger screen¹¹. App developers would incur higher app development costs because apps would have to be adapted to the data and formats of each car brand and model. Manufacturers would charge independent service providers a third-party access price for the data, and users would probably have to pay for at least part of these charges.

A similar situation occurs in smart home services where Google and Amazon have developed strong market positions with their standardised operating systems that connect seamlessly with many smart home devices from a wide range of smaller producers. That gives these producers access to a wide market. It also benefits users who can integrate a wide variety of brands and models of smart fridges, heating systems, security devices, etc, into their Google or Amazon-operated home systems. The DA's prohibition on porting data to these gatekeeper platforms would prevent that. As a result, consumers will face a very fragmented market with many hurdles to integrate devices from different

¹¹ Smartphone and car screen mirroring technology could partly overcome that problem.

manufacturers into a single home network. Producers of smart home devices will have to develop their own home systems. A common and open data interoperability standard could overcome these hurdles. There is no incentive for the largest players in this market to design an open standard when users are not allowed to port their data to platforms that use that standard.

Complications occur because of ambiguity around devices that would fall under the prohibition in DA Art 5(2). It is not clear if that prohibition would apply only to smart home devices not produced by gatekeepers, or also to devices produced by these firms. In the former case, it may have an adverse effect on competition because it would push consumers to buy only Google and Amazon smart home devices and thereby strengthen the market position of these big players. In the latter case, it would effectively disrupt vertical integration of home applications inside these firms.

There is an additional ambiguity in the interpretation of this prohibition with regard to the recipients of data transfers. The DMA definition of core platform services includes OS such as Android and Apple iOS. However, apps or app developers within these OS are not gatekeepers according to the DMA. As such, they do not fall under the DA prohibition on transferring data to gatekeepers. However, when the app has access to the data, the OS will usually have access as well, at least to part of the data. Most if not all apps contain code that enables the OS operator to monitor activity and data flows within the app. This raises the question of whether the gatekeeper's OS would be considered the recipient of the data transfers, or should the services app within the OS be considered the recipient? In the former case, the DA prohibition would prevent any transfer; in the latter case not. The DA rapporteur in the European Parliament (2022) proposed an amendment to Recital 14 that seeks to overcome this ambiguity. It mentions OS explicitly as falling under the data access rule of the DA. If that amendment were accepted in the final version, it would endorse the former interpretation. The same ambiguity applies to data transfer pricing. If the operating system provider, as a large firm, is the recipient, the DA's marginal-cost-plus-markup rule applies; if the app is the recipient, with many app developers qualifying as SMEs, the marginal-cost-only rule would apply. Similarly, would all app-based services qualify as "*comparable recipients*" under the DA, resulting in a prohibition of price discrimination, or can they be price-discriminated depending on the type of service they offer?

There is no need for a DA lock on data transfers to DMA gatekeepers because the DMA already contains a data unlocking mechanism. DMA Arts 6(7) and 6(9) impose data-sharing obligations on gatekeepers precisely to avoid strengthening their market position. DMA Art 6(1) unlocks gatekeepers' exclusive control over their data and prohibits privileged use of this data for gatekeepers' vertically integrated services, unless they are publicly available or shared with competitors. Moreover, data-sharing

conditions imposed on gatekeepers in the DMA are more favourable to users than in the DA. Contrary to marginal cost pricing in the DA, DMA gatekeepers should share data free of charge and via API tools that ensure real-time effective interoperability at the operating system, hardware and software level.

Last but not least, the prohibition on data transfers to DMA gatekeeper platforms makes it very difficult to generate network externalities with product data. It limits welfare gains for users as well as producers from network effects. Product manufacturers can try to create their own data platforms, but their network effects will inevitably be very limited because they only reach their own products and users, not an entire market of users and competing and complementary products. It fragments market information into narrow silos of inefficient use of that information. The DA does not mention data-driven network effects. Even the DMA only looks at the anti-competitive side of network effects and does not consider the positive welfare effects of these network effects for platform users. Gatekeeper platforms achieve strong market positions precisely because they offer strong network benefits to users. These network externalities generate user welfare: users get more benefits than what they pay for.

Weakening these network effects is considered to be pro-competitive and therefore welfare enhancing. The DA has inherited this one-sided perspective on platforms. As a result, the ostensibly pro-competitive provision that prohibits data transfers to monopolistic DMA gatekeeper platforms is likely to have an anti-competitive and innovation-reducing impact in downstream services markets for IoT products. Cabral *et al* (2021) suggest that policymakers should tread a fine line in the balance between the negative welfare effects of reduced competition by dominant platforms, and the positive welfare effects of network externalities. That advice has been ignored in the DA.

5 The prohibition on using data for competition purposes

A particularly striking anti-competitive feature of the DA are the prohibitions it imposes on use by data holders, users and third-party data recipients of product data to compete with each other in product or related services markets (DA Arts 4(6), 5(5) and 6(2)). Users may use the data to develop new and innovative products, or related services, but not if these products or services compete directly with the product or service from which the data originates. Data holders should not use data in a way that could affect the commercial position of the user or a third-party, unless they have consented to such use of the data. This reduces the scope of legitimate data-driven innovations to not-too-close substitute products. Who will decide whether a data-driven insight or service innovation undermines or improves the economic position of users and third-parties? Does the use of data for targeted advertising, price

and service quality discrimination, and more generally the use of data for service innovation in accordance with the preferences of users and the commercial strategies of service producers, undermine or strengthen the economic position of users and providers? These provisions effectively reduce competition in data-driven services and product markets. They suggest that the *status quo ante* in the private welfare of product manufacturers, data holders, users and third parties is preferable to innovation. Non-use of information seems to be preferable to efficiency and welfare-enhancing economic use.

The DA offers no meaningful economic arguments to support these anti-competitive provisions. The provisions may have been included to enhance trust in the DA because access to data cannot be used against the interests of any of the parties involved. As other authors have noted (Metzger and Schweitzer, 2022; Picht, 2022; Schweitzer *et al*, 2022), this reflects a negative prejudice against competition and a misguided approach to regulatory policy as a tool to preserve the private interests of stakeholders, rather than to boost the social welfare of society.

A possible rationale for these provisions may have been the protection of intellectual property rights and trade secrets of product manufacturers and data holders. Traditional IPR strengthens the static monopoly right but also boosts dynamic innovation incentives by allowing the development of substitutes that do not interfere with the scope of the patented or copyrighted product features. However, manufacturers and data holders can apply traditional IPR instruments, such as patents and copyright, to protect their hardware, embedded software and designs against direct competition. The scope of these IPR rights is well-defined in law and does not prevent competition from innovative products that are partial substitutes for the original product, but differ in some important technical characteristics that are not covered by IP rights. The DA introduces additional IP protection by prohibiting the use of data by third-parties for developing competing products with the manufacturer, or preventing the manufacturer from developing competing services with the third-party data recipient. There is no need for these data-related prohibitions as an additional layer of protection on top of IP law.

The main objective of the DA is to address monopolistic market failures in vertical integration between upstream product markets and downstream data-driven services. It overlooks however that data adds another aspect to the traditional vertical integration arguments: economies of scope in the re-use of data. Since data is non-rival, re-use in competing and non-competing services can be social-welfare enhancing. The DA provisions address this concern by opening user access to data. That breaks any attempt at vertical restraints or vertical integration between upstream and downstream markets. However, the prohibition on competing with the original product or related service producers restricts

the re-use of data to innovation in non-competing products and services. This erodes a considerable part of the social value of data.

6 Filling the gaps: towards mutual exhaustion of rights

The previous sections discussed anti-competitive provisions in the DA that create obstacles to the proper functioning of data markets and data-driven services markets. In this section, we focus on two market obstacles that the DA ignores – data rights for producers and data-driven network effects – and propose to solve these issues with the introduction of the principle of mutual exhaustion of rights between all parties.

The DA grants an asymmetric data access right to product users but remains silent on producer rights to access and use the data. It assumes implicitly that producers have *de-facto* access to the data. That assumption is not necessarily true. Users may be businesses that have market power and do not want producers to access the data generated through business usage of a product or service. Data-access bottlenecks may also occur in production chains that involve many producers of data-generating components. Producers may sell parts and components to other producers who assemble them into new products. Parts producers do not necessarily have access to the data generated by the use of these parts in an assembled product or in a production chain.

Data is usually co-produced or co-generated between at least two – and often many – parties: the producer and the users of a product or service. The data would not exist without collaboration between these parties. As a result, these parties may have a material interest in, and claim access to, the co-generated data¹². The optimal social-welfare maximising allocation of access rights between the co-generating parties, including possible compensation mechanisms, is a complex exercise that cannot be achieved with a few general legal clauses. The DA short-cuts this complex process by separating data access rights and the right to monetise data, and by allocating the former to users and the latter to product manufacturers. This standard solution may at least partly address competition and vertical integration (between pre- and aftermarket services) issues. However, it is unlikely to be sufficient when considered from a horizontal data integration or data-network effects perspective.

¹² This mutual claim of producers and users distinguishes the economics of data from the economics of IPR. IPR-protected innovations are produced unilaterally by an innovator. Users of an innovative service or product do not contribute to the innovation and cannot claim rights on that innovation, except for the rights granted to them by a bilateral license contract, or possibly by legal exceptions to IPR.

Data is subject to economies of scale and scope in aggregation: merging a larger number and variety of data into a single pool may generate more economically valuable insights, compared to the insights that can be gained from keeping the data separated (Calzolari *et al*, 2022; Ishitashi, 2022; Carballa-Smichowski *et al*, 2022). Economies of scale and scope are also known under the label of data-driven network effects or externalities that can improve the quality of data-driven services (Prüfer and Schotmuller, 2020; Acemoglu *et al*, 2019; Choi *et al*, 2019). The DA ignores these network effects. Producers often have an advantage over users because they can potentially aggregate data across all the products and services they sell. Users can only access the data from the product they bought and are usually not in a position to generate significant economies of scale and scope in data aggregation, unless they hold a significant market share of producer output. Market forces may work both ways, putting more data aggregation market power into the hands of producers or users of products. The combination of data-access claims from all data co-generators, and the ability to generate data network effects in data aggregation, is a reason to establish a level playing field in terms of data access and use rights between producers and users.

This could be achieved with the introduction of the principle of mutual exhaustion of data access and use rights for producers and users, at the point of sale of a data-driven product or service¹³. Mutual exhaustion implies that neither party can claim any rights or restrictions on what other parties can do with the data generated by a service that they produce or use, beyond the payment and conditions agreed at the point of sale of that product or service. Users have full and unrestricted free access rights to these data. Similarly, users cannot claim any data access and use restrictions on producers, beyond the point of sale of the service. Mutual exhaustion would be subject to restrictions imposed by pre-existing rights, such as those attributed by the GDPR to natural persons, and those attributed to legal persons by IPR and trade secrets law. While the GDPR and IPR are a rather well-defined body of law and jurisprudence, trade secrets are rather poorly defined in terms of digital data.

Mutual exhaustion would apply to all producer-user pairs at every stage in a production process. Its general application would maximise economies of scale and scope in data aggregation and the resulting innovation potential. This may have very far-reaching consequences for the organisation of production processes. It would require further research before it can be turned into a practical application.

¹³ This idea is also discussed in Schweitzer *et al* (2022).

7 Summary of the policy recommendations

Recommended changes to the draft Data Act	Relevant articles and recitals
Drop the definition of 'products' and allow the application of the DA to data generated by the use of all products and services	Delete Recitals 14 and 15. Extend the scope of Art 3 to all products (goods) and services
User data-access and portability rights should cover all data that the manufacturer or data holder has access to.	Covered by the amendment to Art 4 (1) proposed by the European Parliament rapporteur. Delete Recital 17.
Eliminate exclusive data-pricing rights for product manufacturers and data holders in case of data transfers to third parties.	Delete Art 9(1) and extend the compensation provisions of Art 9(2) to all users, irrespective of the size of the firm.
Eliminate restrictions on data transfers to gatekeepers under the DMA	Delete Art 5(2)
Eliminate the restrictions on the use of data for product and services competition	Delete Art 4(4) and Art 4(6)
Create a level playing field between all data co-generators by introducing a mutual exhaustion of data rights at point of sale	Introduce an explicit reference to access rights for users AND producers in Art 3. Revise references to 'users' in other relevant articles accordingly. Introduce the principle of mutual exhaustion of rights at point of sale in Art 3.

References

- Acemoglu D., A. Makhdoumi, A. Malekian and A. Ozdaglar (2019) 'Too much data: prices and inefficiencies in data markets', Working Paper 26296, National Bureau of Economic Research
- Antoine, L. and M. Leistner (2022) *IPR and the use of open data and data sharing initiatives by public and private actors*, study for the European Parliament Policy Department, May
- Cabral, L., J. Haucap, G. Parker, G. Petropoulos, T. Valletti and M. Van Alstyne (2021) *The EU Digital Markets Act: a Report from a Panel of Economic Experts*, Joint Research Centre of the European Commission
- Calzolari, G., A. Cheysson and R. Rovatti (2022) 'Machine Data: market and analytics', mimeo, European University Institute, October
- Colangelo, G. (2022) *The European proposal for a Data Act, a first assessment*, Centre on European Regulation (CERRE), July
- Carballa-Smichowski, B., N. Duch-Brown, S. Höcük, P. Kumar, B. Martens, J. Mulder and P. Prüfer (2022) 'Economies of scope in data aggregation with a case study in health data', mimeo
- Choi J.P., D.-S. Jeon and B.-C. Kim (2019) 'Privacy and personal data collection with information externalities', *Journal of Public Economics* 173: 113-124
- Donewald, C., M. Fenwick, P. Jurcys, M. Lampinen, V. Nekrosius and A. Smaliukas (2020) 'Ownership of user-held data why property law is the right approach', *Harvard Journal of Law and Technology Digest [2021]*
- Drexler, J. (2018) *Data access and control in the era of connected devices*, study on behalf of the European Consumer Organisation (BEUC), Brussels
- Efroni, Z., P. Von Hagen, L. Völzmann, R. Peter and M. Sattorov (2022) 'Position Paper regarding Data Act Proposal of the European Commission', Weizenbaum Institute for the Networked Society, Berlin, June
- European Commission (2017) 'Building a European Data Economy', COM(2017)9, 10 January
- European Commission (2022a) 'Proposal for a Regulation of the European Parliament and Council on harmonised rules on fair access to and use of data (Data Act)', COM(2022)68, 23 February
- European Commission (2022b) 'Proposal for a regulation on the European Health Data System', COM/2022/197 final, 3 May
- Gill, D. (2022) 'The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources', mimeo, May
- Graef, I. and M. Husovec (2022) 'Seven Things to Improve in the Data Act', mimeo, March

- Habich, E. (2022) 'FRAND Access to Data: Perspectives from the FRAND Licensing of Standard Essential Patents for the Data Act Proposal and the Digital Markets Act', mimeo, University of Zurich
- Hoegaerts, L. and B. Schönenberger (2019) *The automotive digital transformation and the economic impacts of existing data access models*, Technical Report for the International Federation of Automobile Service Providers (FIA)
- Kerber, W. (2022) 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives', *GRUR International*, ikac107: 1-16.
- Metzger A. and H. Schweitzer (2022) 'Shaping Markets: A Critical Evaluation of the Draft Data Act', mimeo, September
- Perarnaud, C. and R. Fanni (2022) 'The EU Data Act, Towards a new European data revolution', *CEPS Policy Insights 2022-05*, Centre for European Policy Studies
- Perzanowski, A. and J. Schultz (2016) *The End of Ownership: Personal Property in the Digital Economy*, MIT Press
- Picht, P.G. (2022) 'Caught in the Acts: Framing Mandatory Data Access Transactions Under the Data Act, Further EU Digital Regulation Acts, and Competition Law', *Research Paper No. 22-12*, Max Planck Institute for Innovation & Competition
- Picht, P. and H. Richter (2022) 'The Proposed EU Digital Services Regulation 2020: Data Desiderata', *Research Paper No. 21-21*, Max Planck Institute for Innovation & Competition
- Posner, R. (1978) 'The Chicago School of Antitrust Analysis', *University of Pennsylvania Law Review* 925 (1979): 925-948.
- Prüfer, J. and C. Schotmuller (2020) 'Competing with big data', *The Journal of Industrial Economics* 69(4): 967-1008
- Schweitzer, H., A. Metzger, K. Blind, H. Richter, C. Niebel and F. Gutmann (2022) *Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy*, report for the German ministry of economics and climate, July
- Staaht Gabrielsen, T., B. Johansen and G. Shaffer (2018) 'When is Double Marginalization a Problem?' *Working Papers in Economics 7/18*, University of Bergen, Department of Economics
- Zech, H. (2015) 'Information as property', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 6(3): 192-197



© Bruegel 2022. All rights reserved. Short sections, not to exceed two paragraphs, may be quoted in the original language without explicit permission provided that the source is acknowledged. Opinions expressed in this publication are those of the author(s) alone.

Bruegel, Rue de la Charité 33, B-1210 Brussels
(+32) 2 227 4210
info@bruegel.org
www.bruegel.org