Data Act proposals: potentially adverse effects on consumers and innovation in the EU

An economic review of the European Commission's proposal

Prepared for
Google

28 November 2022

Final: public

www.oxera.com

oxera
compelling economics

Contents

Figures and tables

About Oxera and our clients

Oxera is an international economics consultancy with 40 years of experience across sectors, geographies and jurisdictions. We have a deep understanding of the digital sector, having been actively engaged in the debate around the future of digital regulation.

We regularly publish on this topic, contribute to public consultations, and advise policymakers, regulators and businesses on digital and creative issues.

The report was commissioned by Google. Any errors or omissions remain our own.

1 Introduction

1.1 About this report

This report considers the potential unintended consequences for consumers, innovators and the broader data ecosystem of the European Commission's current proposal for the Data Act. In particular, the report assesses the economic implications and resulting policy issues around three core aspects:

- the broad scope of 'relevant data' and 'related services' outlined within Chapters 2 and 3 of the Data Act (see section 2);
- the exclusion of Digital Markets Act (DMA)-designated Gatekeepers outlined in Article 5.2 (see section 3);
- the fair reasonable and non-discriminatory (FRAND) access obligations outlined in Articles 8 and 9 (see section 4).

We conclude with a summary of the policy tensions arising both *within* the Data Act and *between* the Data Act and other digital legislation (see section 5).

The remainder of this section gives an overview of the objectives of the Data Act, including some core economic characteristics of data that drive the implications of the proposals.

1.2 Objectives of the Data Act

The Data Act is primarily intended to unlock the value of data held on the wide range of Internet of Things (IoT) devices used in the EU, by increasing the extent of sharing and promoting its use as an economic input. Importantly, this aim is to be achieved while maintaining incentives to invest in the raw data generation that lies at the root of the data economy (see Box 2.1).

Box 1.1 Stated aims and objectives of the Data Act

In its press release accompanying the publication of the proposal for a Data Act, the Commission explained that the Data Act: 'aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation.'

Source: European Commission (2022), 'Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data', 23 February.

More specifically, the Data Act aims to improve competition and fairness in data markets, while ensuring that users' data privacy is maintained, by:

- removing barriers to the development of the European data economy;[1]
- ensuring greater balance in the distribution of value from non-personal industrial data and the new wave of IoT devices;[2]
- overcoming perceived inequities between large data holders (including Gatekeepers) and small and medium-sized enterprises (SMEs);[3]
- facilitating access to, and the use of, data by consumers and businesses, while preserving incentives to invest in new ways to create value from data.[4]

In effect, these policies seek to promote aftermarket services by mandating access to IoT device data for users or authorised third parties—although

certain firms are excluded from the data-sharing provisions, and when sharing does take place it will typically include compensation on FRAND terms.

1.3 Key characteristics of data

Data sharing can unlock social value by enabling more firms to develop innovative products and services, removing bottlenecks to competition, and levelling the bargaining power of actors across the sector.

With the growth of the digital economy, data has often been called the 'new oil'. However, if one firm uses a barrel of oil, that same oil cannot be used by another firm. It is a depletable and rivalrous resource. In contrast, data is:

- **non-depletable**: i.e. it is not 'used up' when it is put to use and so can be re-used to create further value;
- **non-rivalrous**: it is easily reproduced and so can be used by several firms, or for different purposes, simultaneously.

In addition, much of the data being collected is not unique. The collection or generation of data by one firm does not prevent another firm from creating the same data. For example, information about a user's location can be—and often is—collected through a multitude of devices and services at the same time (e.g. mapping apps, weather apps, connected cars, wearables).

A core rationale for unlocking social value through data sharing is that using consumer data for one purpose does not, in most cases, diminish its use for another purpose. Therefore, the non-depletable and non-rivalrous aspects of data mean that it can be shared to generate further value.

2 Scope of the Data Act

There are at least two ways in which an excessive requirement to share broad datasets from devices, as well as additional data from a wide range of related services, could endanger the data ecosystem:

- first, it could reduce incentives to invest in data creation by eroding data holders' ability to share in the value created by these risky investments;
- second, it could reduce participation in the ecosystem by eroding user trust if data holders are unable to effectively manage third parties' data access.

In this section, we first discuss the proposed scope of the Data Act in terms of the data and services to be included (section 2.1), before expanding on the mechanisms that can drive these two unintended consequences (section 2.2 and 2.3).

2.1 What does the Data Act say about scope?

The Data Act focuses on data collected by 'tangible products' and their 'related services', including virtual assistants (see Box 2.1).

'Tangible products' include a wide range of IoT devices, such as vehicles, smart-home equipment and consumer goods, medical and health devices, and agricultural and industrial machinery. These devices are all within the scope of the Data Act. These kinds of IoT device are developed and produced by firms of differing sizes, and produce both personal and non-personal datasets.

'Related services' are any services fulfilling a function that the device is sold with the ability to perform. As such, a device could involve many discrete related services, such as payment services, location services, search services, or music services. This means that a broad range of data—that is only tangentially connected to the underlying IoT device—could also fall within the scope of the Data Act.

Box 2.1 Scope of the Data Act

- **Tangible products:** Article 2(2) specifies the products covered by the Data Act as follows: ''product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data.'
- **Related services:** Article 2(3) defines the services related to those products, which also fall within the scope of the Data Act, as follows: ''related service' means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions.'
- **Virtual assistants:** Article 7(2) explicitly specifies that: 'Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service.'
- **Definitions of data:** Recital 17 specifies the data that is in scope: 'Data generated by the use of a product or related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off.'

Source: European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, pp. 38–39.

Under the Data Act, this data is to be shared with the device's user or third parties acting on their behalf. The Data Act specifies that this obligation applies to:[5]

- data recorded intentionally by the user;
- data generated as a by-product of the user's action, such as diagnostics data;
- data without any action by the user, such as when the product is in standby mode and data recorded during periods when the product is switched off.

Data that results from any software process that calculates derivative data—for example, any data that is transformed, altered, aggregated—is excluded as it is subject to IP rights. Furthermore, the Data Act allows for third-party firms—with the permission of the device's user—to request access to the data produced by an IoT device and to use this as an input to their products and services. However, the Act specifies that the data should not be used to create a product that directly competes with the core functioning of the original IoT device—with the effect of protecting innovation incentives for the device maker.

2.2 Impact on investment incentives

The Commission has previously noted the transformative effects that the proliferation of IoT devices can have on the economy.[6] It is estimated that both the number of devices and the revenue they generate is growing by around 10% annually,[7] indicating a steady growth in the applications and use cases of IoT.[8]

To fulfil the Data Act's goals of facilitating the generation and use of data,[9] it is crucial that this development and production of IoT devices is maintained. One of the principal aims of the Act is to improve dynamic competition and innovation in this market, both of which rely on two important economic features:[10]

- **appropriability**: the ability of the innovator to share in the value of their innovation and recoup R&D investment;
- **contestability**: the ability of a challenger to enter a market and compete with incumbent products or services.

However, data access regulation that is designed to increase the *contestability* of markets can reduce the *appropriability* of value by potential innovators for data generation. This creates an acute policy trade-off, which will require a careful balance that fosters both short-term competition and long-run innovation.[11]

Importantly, much of the data that is created is *not* simply a free by-product. It is costly to acquire, and sharing data on terms that do not compensate the data generator for those costs will reduce incentives to innovate in data creation. Furthermore, the costs of data collection may be largely intangible and may vary greatly. For example, the collection (or production) of data can require dedicated expenditure and effort, such as defining the nature of the desired data and designing a set-up to generate it;[12] while the risks associated with this uncertain development must also be compensated.

Furthermore, once data has been acquired there is a substantial investment made into the functioning of the device that can deliver commercial insights or consumer services. Once again, firms make considerable investment in the

tools and algorithms that enable effective processing, with many of these algorithms representing significant trade secrets. It is important, therefore, that the scope of data remains sufficiently limited to ensure that these algorithms cannot be 'reverse-engineered' by data access seekers. Therefore, in order not to discourage innovation, the Data Act must ensure that no data outputs are shared that allow firms receiving the data access to trade secrets.

These tensions between investment incentives that foster long-run dynamic competition and access conditions that promote static competition to avoid market power have also arisen in other sectors. For example, in telecoms regulation, wholesale access to certain network capacity must balance the short-run needs of retail access seekers with the long-run benefits of investment by the network operator. In addition to highlighting the tension between investment and access incentives, this example highlights the complexity in assessing what return on investment would be sufficient to achieve the objective of the regulation (see Box 2.2).

Box 2.2 Case study: access mandates, appropriability and investment incentives in the telecoms sector

The importance of appropriability and its impact on incentives to invest is demonstrated in the telecoms sector. In the EU, owners of an essential section of very-high-capacity telecoms networks (VHCN) were mandated to offer access to some capacity of the network. The European Commission mandated that access would be given on non-discriminatory terms, which outlined a cost-based charging principle.[1]

It was found that, while this mandatory access pricing allowed for increased competition in the broadband market, it came at the cost of reducing incentives to invest, and slowed the roll-out of the next generation network. This is because the rate of return on the asset—that is, the compensation from other firms wishing to purchase some of the capacity—would be highly uncertain given that demand from firms at that stage would be unknown. If strict cost pricing were mandated, the rate of return would allow firms to recover only the direct costs of the investment, without compensating them for the significant downside risks around demand for the asset, even if those downside scenarios did not materialise. Pricing flexibility, especially in an initial transition phase, can allow firms to adjust their compensation in light of the revealed demand for capacity from other firms, and ensure that they are compensated for both the costs of the investment and the risk that they have taken on.

The impact of cost-based mandates on investment incentives in the telecoms sector was large. In 2009, it was estimated that the increase in regulation had resulted in a €16bn reduction in investment in telecoms infrastructure stock, representing around 23% of the total stock.While regulations encouraged increased investment from entrants, this was not enough to offset the larger decrease in investment by incumbents.[2] Further studies note that the regulatory model was better at promoting static competition than stimulating long-term dynamic competition (such as new network investments).[3]

As a result, more recent regulations, such as the European Electronic Communications Code (EECC), recognise and aim to mitigate this issue of investment incentives. The EECC states: 'Due to uncertainty regarding the rate of materialisation of demand for the provision of next-generation broadband services, it is important in order to promote efficient investment and innovation to allow those operators investing in new or upgraded networks a certain degree of pricing flexibility.'[4]

Note: [1] European Commission (2010), 'Commission Recommendation on regulated access to Next Generation Access Networks (NGA)', 25 September. [2] Grajek, M. and Roller, L.H. (2009), 'Regulation and Investment in Network Industries: Evidence from European Telecoms', *ESMT Working Paper*, 15 June, p. 16. [3] Cave, M., Genakos, C. and Valletti, T. (2019), 'The European framework for regulating telecommunications: a 25-year appraisal', *Review of Industrial Organization*, **55**:1, pp. 47–62. [4] European Commission (2018), 'Directive (EU) 2018/1972 of the European Parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code', 17 December, recital 193. This is sometimes referred to as the 'fair bet principle', and has regulatory precedent in the telecoms sector; see Oxera (2017), 'Does Ofcom's approach in the WLA market review honour the fair bet principle?', 16 June.

In the context of the Data Act, markets for data must similarly balance competing private incentives and social objectives. To foster new innovation in data generation and services, the returns to the investment must be appropriable. This will depend to some extent on how firms can monetise the data that they create, such as using it directly to gain a competitive advantage in a product or service, or selling it to third-party service providers. However, in its current formulation, the Data Act risks undermining appropriability in three ways.

First, there could be disincentives to invest in designing and manufacturing IoT devices if it is not possible to recoup the costs of the investment through the sale of the device. This would be a risk when trade secrets around the functioning of the device, in particular the algorithms used for processing the data, can be reverse-engineered through the data shared. This would also be a risk if the Data Act fails to ensure compliance with the intended purpose of the data sharing, which explicitly excludes using the data for a competing product.

Second, there could be disincentives to invest in the collection of data if the costs cannot be recovered through aftermarket services. Data collection relies on the design choices of IoT manufacturers, such as the inclusion of sensors, which will necessarily come at a cost. Such sensors may be subsidised by the aftermarket services that can be offered using the data that they generate. If firms are less able to monetise these innovations, they may be less willing to invest in the first place.[13] This could mean increased prices for IoT devices, or reduced functionality at the same price point. In either case, less data would be generated as a result of reduced investment incentives.

This point can be illustrated by considering the incentives for Tesla to install sensors within its cars to enable self-driving.[14] These sensors allow drivers to subscribe to Tesla's self-driving software, but the investment in installing these is undermined if another company can provide competing self-driving software using the data. Given that the instalment of the self-driving functionality in the car is not charged for separately, a reduction in the ability to charge for the related services would undermine the incentives of Tesla to invest in these sensors.

Third, the creation of usable device data is often the culmination of many layers of R&D and investment into a network of data collection, processing and security measures that are not easily separable and allocable to individual users. These characteristics mean that charging for data only on the basis of the costs of the extraction and transmission would be insufficient to maintain the incentives on firms to continue to invest in products that will generate and collect data. If the compensation for making data available to SMEs cannot exceed the directly related costs (i.e. if investments made in the data collection and production cannot be considered to calculate the compensation), this removes any profit opportunity,[15] giving companies less incentive to collect data in the first place.

Both the incentives around data generation, and the format in which the data must be provided, underpin the need for the Data Act to ensure the appropriability of data-generating devices. If these incentives are not sufficiently accounted for, the market for data generation could be compromised, and the amount of data generated might be reduced, with a knock-on reduction in the social and economic benefits that it could bring.

Differences in investment incentives can also be highlighted with reference to the objectives of the General Data Protection Regulation (GDPR) and the Data

Act, as set out in Box 2.3. Whereas the Data Act must maintain incentives for the production of data as a commercial input, the GDPR solely focuses on giving people control over personal data that was collected, rather than generated, by a firm.

Box 2.3 Key differences between the GDPR and the Data Act

There are important differences in the data that is covered by the GDPR and the Data Act, as well as the way in which that data must be provided.

Type of data
The GDPR covers only personal data, and the data subject may request for that data to be provided to them or another data controller in an appropriate format.[1] The Data Act covers both personal and non-personal data produced by IoT devices, where this data is used primarily as an input into related services for the user.[2]

Scope of data
The difference in the scope of data that is covered by the respective regulations is important, as it underpins the need for the compensation of the input data covered by the Data Act. Whereas the GDPR covers personal data only, which is not specific to any particular method of data generation, much of the data covered by the Data Act is specific and dependent on the device on which the data was generated. Given that data covered under the Data Act is to a greater extent dependent on the commercial appropriability of that data generation, there should be appropriate compensation for data sharing in order to maintain data generation incentives. The GDPR does, however, have exceptions whereby the costs of providing data may be compensated, but only 'where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character'.[3]

Data format
Furthermore, the GDPR and the Data Act require data to be provided in different formats. Whereas the GDPR requires that data be provided as a single copy of machine-readable data, the Data Act requires that the third party has access to data continuously and in real time. The costs of this latter form of data transfer are likely to be higher, with the need to develop industry standards and application programming interfaces (APIs) for interfacing between companies.[4] Additionally, continuous data is used primarily as an input into the provision of related services, and may thus be considered more of a commercial input than the property of an individual consumer.

Note / Source: [1] European Commission (2016), 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', p. 13. [2] European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, p. 20. [3] European Commission (2016), 'General Data Protection Regulation', p. 40. [4] The GDPR does, however, have exceptions whereby the costs of providing data may be compensated, but only 'where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character'. [5] The need for interfacing and the use of APIs between companies is similar to the kind of data sharing that has been seen in the financial sector through the open banking reforms. This is explored further in section 4.

In summary, it is necessary to take investment incentives into account when setting the compensation for access to a new asset, and for these to sufficiently compensate both the direct costs and risks of an investment. This is particularly applicable in the case of investments in data generation, as there will be significant uncertainty over demand for newly generated data, as the products and services that will use this data might be developed only once the data starts being generated.

2.3 Impact on trust and participation

The Data Act requires data holders to make the relevant data available to a third party upon the request of the user. However, it does not set out any criteria for a third party to be eligible to receive a user's data.[16] In particular, third parties have no requirement to demonstrate that they have the necessary

infrastructure in place to keep secure the data they receive. The Data Act also does not allow any third parties to be excluded from data access due to previous failings in relation to security and privacy. This risks data ending up in the hands of 'bad actors', unless the data-sharing obligations come with clear security and privacy criteria for the data recipient. This is even more relevant considering that users will not be in a position to review and evaluate the nature of the data they would share with the third-party data recipient. This is of particular concern given that the development of a digital economy is dependent on the creation of trust.[17]

Trust is a key criterion in order for consumers and firms to participate in the data ecosystem. As such, the effective functioning of an ecosystem is based on the perceived security of the system, which is the key driver of user trust. A recent survey on online trust in Europe and the rest of the world by Frost & Sullivan shows that consumers' online spending habits depend heavily on their level of 'digital trust', and that nearly half of consumers stopped using an online service after a data breach disclosure.[18]

Trust can be ensured through good governance of the ecosystem. The effectiveness of good governance will depend on platforms' ability to 'leverage advances in information and communication technologies while maintaining the trust and security of digital transactions',[19] and this good governance ensures participation and the ability to generate and use data.[20] Therefore, in order to attract participation, along with the value of the services provided, ecosystems compete with each other on the quality of the security of their infrastructure. Research has found that almost a third of ecosystem orchestrators attributed their failure to trust-related issues.[21] Surveys of consumer attitudes toward IoT devices showed that security concerns are the biggest barrier to growth in IoT device take-up.[22] A global survey conducted by Ipsos Mori found that 75% of respondents distrust the way data from IoT devices is shared. [23] In all countries except Japan, security concerns were as big a factor in the decision not to buy an IoT device as price.

To provide a secure environment, data ecosystems have governance regimes ranging from the rudimentary to the sophisticated, including rules, standards, detection mechanisms and penalties designed to deal with the bad behaviour of some platform users that harms other users.[24] In particular, they can aim to limit or restrict admission of low-quality access-seekers in order to uphold the reputation of their ecosystem and increase the long-term benefits to both business users and consumers. Platforms can achieve this in a variety of ways.

First, they can set ecosystem rules that govern what third parties can and cannot do. The platform may take an active role in moderating actors that violate these rules, but this rests on having the ability to penalise and ultimately exclude bad actors from the community.[25] This is particularly important when consumers are unable to distinguish between the quality of services of different participants.

While consumers have a preference for greater security and privacy, they often find it difficult to differentiate between products that are more or less secure.[26] Users often fail to understand what data on them is being collected, and how this data is used.[27]

Second, ecosystem orchestrators can regulate the levels of access that third parties have to their data. On the one hand, this can mean restricting third-party access to specific types of data—for example, an operating system may

prevent third-party developers from directly accessing specific pieces of hardware (e.g. a fingerprint scanner). On the other hand, data holders may need to restrict data access to certain third parties in case they are not able to ensure responsible use of the data.

These practices ensure that responsible sharing and use of data are already available through industry initiatives, such as Matter. Specifically, Matter has set up frameworks that allow safe data sharing and ensure interoperability between IoT devices in a secure manner—this requires devices to undergo certification processes to participate.[28] Similarly, in its decision regarding the acquisition of Fitbit by Google, the Commission approved the merger conditional on a commitment package that included access to users' health and fitness data, as long as those seeking access met a number of Privacy and Security Requirements. [29] These Requirements included third parties needing to handle data securely in accordance with industry standard security practices, including by undergoing standardised security assessments.

If data holders are required to give full data access to *any* third party that asks for it—potentially including insecure actors that the data holder would ordinarily have weeded out—this system of trust will now be undermined. In this case, the burden will be on consumers, who will need to distinguish between safe and dangerous data holders. The governance role has been eroded and competition between ecosystems on security and quality is undermined. To overcome such issues, data holders must be able to ensure that third parties with access to data take the necessary measures to avoid data breaches or misuses.

An example of the effects of unsuccessful platform governance by Meta is shown in Box 2.4.

Box 2.4 Case study: the role of platform ecosystems

Data ecosystems apply a range of different policies and incentives to maintain the security and integrity of their platforms. Until recently, Facebook relied on a set of policies that app developers that use the Facebook Platform APIs must follow in order to restrict the way in which they can use users' data extracted from the platform. After a series of policy breaches and user data leaks, Facebook decided to update its policies to ensure a safer environment for users' data.

The main example of these breaches was the Cambridge Analytica breach in 2018, in which third-party developers collected data from Facebook users and sold it to Cambridge Analytica, which used the data in violation of Facebook's terms of service.[1]

Facebook then changed its procedures and implemented a strict review to maintain app developers' access to Facebook Platform APIs. Specifically, app developers were required to verify their business and sign supplemental term contracts, which introduced additional security requirements. Developers that operated as third-party providers to other businesses were required to sign an additional contract that restricted the usage of data.[3] Additionally, Facebook ran an investigation of apps that had access to large amounts of data.[4] Developers that did not go through this audit were banned from Facebook. A couple of months after starting this process, Facebook suspended around 200 apps while a more detailed investigation was done.[5]

It is likely that the main incentive for Facebook to update its data security policies was the fact that users care about their data being protected. A 2017 survey by The Verge showed that around 60% of participants did not use Facebook because they did not trust it.[6] In the 2021 versions of the same survey, that statistic went down to c. 45%.[7] The SlickText 2019 survey showed that the Cambridge Analytica breach made over 70% of participants worried about how their information was being used.[8]

Source: [1] Confessore, N. (2018), 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far', *The New York Times*, April. [2] 'Facebook (2018), 'Enhanced Developer App Review and Graph API 3.0 Now Live'. [3] Facebook (2018), 'An Update on Facebook App

Review'. [4] Facebook (2018), 'An Update on Our App Investigation and Audit'. [5] The Verge (2017), 'Tech Survey'. [6] The Verge (2021), 'Tech Survey'. [7] SlickText (2019), 'One Year After Cambridge Analytica, Survey Reveals Strong Consumer Privacy Fears Remain'.

Ecosystems' orchestrators aim to minimise bad behaviour that might harm participants. In their governance role, they ensure that data sharing takes place when informed consent is granted by a user, and when the user's—or broader ecosystem's—security is not compromised in the process. This is particularly important when consumers in general are not careful with the data that they share.[30] As a result, ecosystem participants—in this case, third-party data access seekers—must be incentivised to invest in improved security in order to be able to partake in the ecosystem and gain access to data.[31]

Another important principle for building trust is seen in the GDPR, where data collectors must operate under the data minimisation principle. The aim of this principle is to make sure that only data that is relevant and necessary to accomplish a specific purpose is collected. Box 2.5 draws similarities between the Data Act and the GDPR, and sets out why data sharing should operate under the same data principle of data minimisation: only data that is necessary for a specific purpose should be made available to third parties, and it should be used only for that purpose. In particular, the Data Act should not discourage data minimisation and privacy-preserving practices. Data that is encrypted, anonymised, pseudonymised, aggregated, or kept private on-device should not be within the scope of the Data Act. Re-associating such data with a user should be impossible, and would disincentivise such privacy-preserving techniques to begin with.

The Commission recognises these principles in the recitals, highlighting that 'only the data stemming from the interaction between the user and product through the virtual assistant falls within the scope of this Regulation. Data produced by the virtual assistant unrelated to the use of a product is not the object of this Regulation'.[32] However, this is not well translated into the proposals on scope, which require data relating to service-to-service interactions to be shared as well. A similar concern would arise if 'standby data' were to be within the scope of the Data Act. Virtual assistants intentionally wait in standby mode until they detect an activation method (e.g. 'Hey Google' or 'Alexa'). The detection of activity happens on-device, where it is frequently overwritten. While the device is in standby mode, data is not leaving the device. Companies have invested in data minimisation technologies like 'on-device processing' with the goal of limiting user data retention and increasing user trust. Depending on the service, requirements to log on-device data permanently would risk undermining user trust. Data holders should therefore be able to apply the data minimisation principle in order to avoid third parties abusing data sharing requirements in the Data Act.

Box 2.5 Reflections on the GDPR and trust

The GDPR is about guaranteeing the protection of the fundamental right to privacy, which needs to be preserved under the Data Act. The GDPR highlights the need for a 'coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.'

The GDPR includes a number of principles outlining how data is managed and stored, one of which is data minimisation. Data minimisation means, for example, that 'the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.' Data minimisation also implies limiting the number of natural persons within an organisation who have access to the data. This is a key principle of the GDPR, especially in the face of a significant rise in the scale of the collection and sharing of personal data.

In order to preserve trust in data ecosystems, the relevant scope of data covered under the Data Act needs to be minimised to include only the data that is needed to provide the service requested by the user, so that the risk of disincentivising participation by erosion of trust is minimised. Therefore, the practice of data minimisation needs to be incorporated to protect the trust and continued participation of the data subject.

Source: European Commission (2016), 'General Data Protection Regulation', 4 May; European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February.

Therefore, core to the functioning of the Data Act is the need to maintain trust in the devices and services that businesses and customers are using, in order to maintain their participation. If the Data Act does not maintain this trust, users are likely to cease to participate in the market, with a knock-on dampening effect on business investment, and possibly a reduction in consumer choice. The tensions identified in the Data Act are further discussed in section 5.

3 Exclusion of DMA Gatekeepers

3.1 New and existing rules for designated Gatekeepers

Building on definitions outlined in the DMA, the Data Act excludes Gatekeepers from using the provisions of the Data Act to obtain device data—even if that data is requested by the device user (see Box 3.1).

Box 3.1 Gatekeepers in the Data Act

Gatekeepers may not request data as a third party:

Article 5(2): Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper, pursuant to Article […] of [Regulation XXX on contestable and fair markets in the digital sector (Digital Markets Act)], shall not be an eligible third party under this Article and therefore shall not:

a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1);

b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;

c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).

Gatekeepers may not receive data from third parties:

Article 6(2): The third party shall not:

[…]

c) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article […] of [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)];

Source: European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, pp. 41–43.

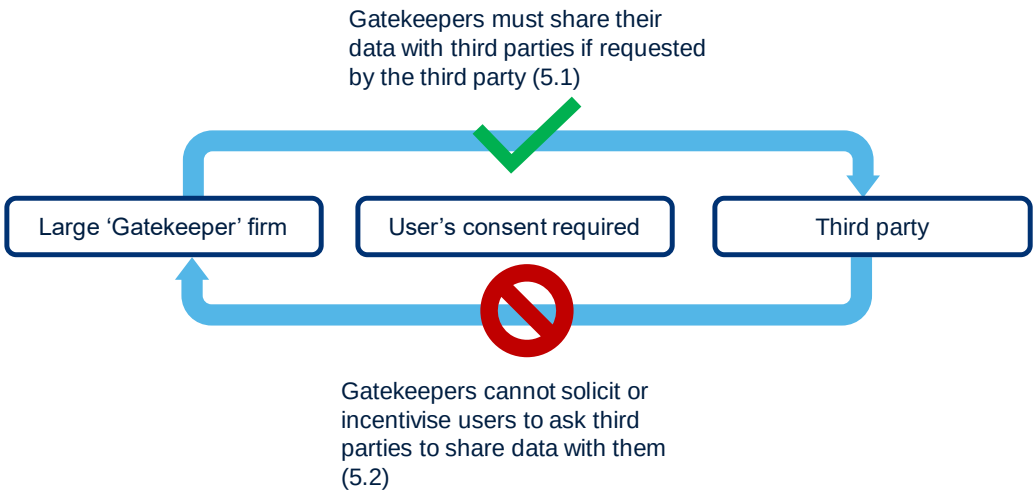
These articles mean that:

- **Gatekeepers may not request data**: Gatekeepers cannot request data from a data holder as a third party acting on behalf of a device user (an Article 5 request);
- **Gatekeepers may not receive data**: Gatekeepers cannot receive data from a user who requested data from a data holder (an Article 4 request) and actively wants to share data with a Gatekeeper's products, and may not incentivise this from a data subject.[33] Similarly, any other third party receiving data under Article 4 or 5 cannot make that data available to a Gatekeeper.[34]

The Data Act cites the 'unrivalled' ability of Gatekeepers to access data as the reason for excluding them from the data access rights outlined in Article 5.1.[35] However, this overlooks the adverse effect that reduced access to Gatekeeper services might have on competition in the IoT product market and consumer choice, and fails to take account of the potential benefits of symmetric sharing.

The asymmetry of this flow of data is outlined in Figure 3.1 below.

Figure 3.1 Mandated flow of Gatekeeper data under the Data Act (Article 5)



Source: Oxera.

Additionally, there is a question around whether the Data Act needs to address any competition concerns with Gatekeepers, given the parallel legislation in the DMA that seeks to address market power issues (see Box 3.2). If the DMA achieves its goals of safeguarding fairness and contestability in the digital sector then additional market-power-oriented policies in the Data Act would be unnecessary and disproportionate.

Box 3.2 The DMA and Gatekeepers' obligations

The DMA outlines measures to promote competition in the digital sector of the EU economy.[1] In particular, these measures are aimed at resolving issues arising from having considerable economic power and safeguarding the fairness and contestability of core platform services.

The measures include a number of obligations that apply to providers that have a significant impact in the internal market and an entrenched and durable position, now or in the near future. These obligations should apply *only* to those services that constitute an important gateway for business users to reach end-users.

For a service to be defined as a gateway, it needs to have more than 45m monthly active end-users in the internal market and more than 10,000 active business users.[2]

The obligations set out in the DMA already include some provisions aimed at requiring firms to share more data. Specifically, these relate to businesses, or third parties operating on behalf of businesses, being able to access the data that they generate when operating on a large core platform. The data that is subject to access obligations is data that is 'provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users', and is therefore relevant only to the core platform service of the Gatekeeper.[3]

Source: [1] European Commission (2020), 'Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)', 15 December. [2] Ibid., pp. 36–37. [3] Ibid., p. 27, para. 54; Ibid., Article 6 1(i), pp. 40–41.

It is also important to note that under the DMA, Gatekeepers are obliged to share only the data related to a user generated through the core platform service.[36] The DMA does not impose obligations on Gatekeepers as a whole, but only to their products and services in digital markets where they have significant market power.

The exclusion of Gatekeepers presumes significant market power by Gatekeepers in the market for IoT-generated data, which the Impact

Assessment of the Data Act has not assessed.[37] Firms with significant economic power relating to data covered in the Data Act are likely to be those firms whose sources of data generation are not replicable, and form an important input to the provision of goods or services of other businesses. For example, it is estimated that a Boeing airliner could produce 40TB of data over one hour in flight.[38] This serves as valuable information to an airline operating the plane in the context of optimising its flying style to reduce fuel use, or to competitors to Boeing in terms of improving maintenance services. Boeing may therefore exert significant market power on some business customers through its control of industrial data from IoT devices, but is not a designated Gatekeeper under the DMA.

3.2 Impact on consumer choice

The principles of asymmetric access result in reduced access to Gatekeeper services. This gives rise to concerns relating to the uptake of non-Gatekeeper devices and the availability of innovative services of some of the largest service providers.

Customers using a Gatekeeper product can request that their data is shared with any third party in order to make use of that third party's services. Customers who have a non-Gatekeeper product are limited to sharing their data (and potentially using services) with non-Gatekeepers only.

Even if data can still be accessed on commercial terms, consumers face uncertainty around the ability to transfer their data between their smart devices and Gatekeeper services. That is to say, they are dependent on commercial agreements being sought and maintained, rather than having a guarantee that the data can be transferred into their chosen services under the Data Act. It is currently not clear that Gatekeepers will continue to be able to access data from third parties on commercial terms.[39]

In a high-level opinion on the Data Act, the Body of European Regulators for Electronic Communications has asked that it be duly considered whether the provisions do not, in an indirect way, restrict users' choice of data and services usage, potentially leading to lock-in effects.[40]

Given the uncertainty around being able to transfer non-Gatekeeper device data to a Gatekeeper-provided service, consumers will have a greater incentive to use Gatekeeper IoT devices, as this gives them a wider choice of service providers. Asymmetric data access may therefore have an unintended adverse effect on the ability of non-Gatekeepers to compete in the market for IoT devices.

The exception of data-sharing rights for Gatekeepers also means that customers using a Gatekeeper device cannot share their data with another Gatekeeper's service. This means that customers would need to switch to the other Gatekeepers device in order to be able to use their device data as input for that Gatekeeper's service. This limits the extent to which services provided by Gatekeepers are able to compete with each other. Asymmetric access to data might also have an impact on the availability of Gatekeepers' innovative services. First, an asymmetric data-sharing obligation will directly restrict a user's access to new and innovative Gatekeeper services, which is likely to hinder innovation and competition between Gatekeepers. In addition to disincentives to invest in innovation due to a reduced ability to obtain appropriate returns as a result of the data-sharing obligation, Gatekeepers will have disincentives to invest due to a reduced ability to market their services. This is especially important since firms that are able to successfully innovate

are more likely to become Gatekeepers and then have their ability to innovate restricted.[41]

In some markets, Gatekeepers will be potential *entrants*, rather than incumbent operators. Importantly, the academic literature finds that entrants often bring 'drastic' or transformative technologies or innovations to new markets.[42] Thus, restrictions on adjacent market entry by global platforms may deprive consumers of significant benefits from innovation.

In this respect, the data access obligation could provide an opportunity for increased competition between Gatekeepers. Gatekeepers are often important innovators, and sharing data *between* their ecosystems is an important driver of continued inter-ecosystem competition. The benefits of symmetric sharing are illustrated in Box 3.3, where we explore the impact on innovation of the Payment Services Directive in the European financial services sector.

Box 3.3 Case study: the Payment Services Directive and the benefits of symmetry of data access

Open banking refers to the changes enacted in the wake of the Commission's Payment Services Directive, which outlined the need for data sharing between large incumbent banks and new entrants.[1] The aim of these changes was to allow for greater competition by facilitating customer switching both between and away from large incumbent banks. Additionally, data sharing was intended to facilitate innovation in the services offered around consumer banking, even within the incumbent's services.[2]

The regulation was designed to be symmetric—data could be shared between all market actors in both directions, including incumbents and new entrants. For example, users could view their balance across different bank accounts within one bank's app, whether that bank was an incumbent or a new entrant. As a result, innovation was exhibited by both market entrants, which offered new insights and financial products to consumers, and the incumbent banks, which offered more streamlined banking apps where consumers could see information from multiple accounts in one place, even where those accounts were with different banks.

Two examples of new and improved services offered as a result of the symmetric Open Banking regulations are set out below.

- **BNP Paribas and Token's 'Instanea'**:[3] Instanea is a service developed in a joint venture between BNP Paribas and Token, an open banking platform, that allows for faster and more secure account-to-account payments across Europe. It integrates with previous online shopping payments services, and allows for functions such as consumers approving payments in their online banking app. The economies of scale and wide consumer reach of BNP Paribas have enabled a larger number of consumers to benefit from Instanea's innovative services.
- **Tink**:[4] this start-up FinTech was founded to develop services across a range of open banking areas, such as data sharing and analysis, faster payments services, and faster and more accurate lending decisions. Tink has partnered with both incumbents and new entrants to improve their service offering and ultimately lead to faster banking services for consumers.

These examples highlight the need for symmetry of data-sharing obligations in order for innovations to take place across the market. At one end of the market, innovations were coming from Europe's third-largest bank, a firm that had been dominant for decades; while at the other end, they were coming from Tink, a firm that is less than ten years old.

Note: [1] Alongside this, the UK Competition and Markets Authority enhanced the provisions outlined in the Payment Services Directive and oversaw its implementation under the Open Banking Implementation Entity, which undertook the development of industry standards for the data-sharing APIs.

Source: [1] European Commission (2015), 'Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)', 23 December. [2] European Commission (2019), 'Frequently Asked Questions: Making electronic payments and online banking safer and easier for consumers', 13 September. [3] BNP Paribas (2021), 'BNP Paribas

Partners with Token to launch “Instanea” an instant payment initiative for its merchants customers across Europe’, 9 March. [4] For more information, see the Tink website.

Lastly, these adverse effects of reduced access to Gatekeeper services demonstrate that, while the Data Act aims to achieve its objective of achieving increased data sharing to unlock the full potential of data, the exclusion of DMA-designated Gatekeepers risks inhibiting the functioning of the data ecosystem.

In other words, there is a tension within the Data Act between aiming to increase data sharing and trying to ensure that that data sharing is on fair terms. The policy aims to achieve this fairness by inhibiting the scope of data sharing, namely with Gatekeepers.

It is clear that asymmetric data sharing will implicitly distort the market for data, by inhibiting the ability of some actors to unlock the value of data from external sources. The current Data Act proposals do not recognise the benefits of symmetric data sharing and the innovations that can arise on both sides of the market when this is imposed.

4 FRAND obligations

The Data Act sets out the broad conditions under which data holders are to make data available to third parties. In particular, it states that data holders should make data available on FRAND terms. This is intended to protect firms against unfair contractual terms in data sharing by large enterprises.[43]

This section describes the nature of FRAND terms, as applied in the Data Act and elsewhere, and explores the possible risks associated with these and what questions will need to be answered to mitigate them.

4.1 What does the Data Act say about compensation for data access?

The Data Act is addressing a number of aims under its FRAND mandate. First, it is addressing a perceived unfairness in the contractual terms for data sharing.[44] Additionally, it is aiming to mitigate the difficulties currently faced by SMEs in acquiring data from other parties, due to market power imbalances between them and other actors, and as a result of the costs of acquiring data.[45] Finally, the FRAND terms sit within the overarching aim of the Data Act, which seeks to ensure a fair allocation of value between actors in the market for IoT data.[46]

Box 4.1 Data provided under FRAND terms in most cases

The Data Act outlines the following provisions relating to FRAND, outlining where the terms should be applied and providing clarification on how the FRAND mandate should be interpreted.

Article 8: 'Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner.'

Recital 41: 'It is not unlawful discrimination, where a data holder uses different contractual terms for making data available or different compensation, if those differences are justified by objective reasons.'

Recital 44: 'To protect micro, small or medium-sized enterprises […] the compensation for making data available to be paid by them should not exceed the direct cost of making the data available and be non-discriminatory.'

Recital 46: 'It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company.'

Source: European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, pp. 41–42.

The articles relating to compensation for data sharing, as set out in Box 4.1, imply that FRAND access will be relevant only in a subset of cases. For example, these terms do not strictly apply when:

- a small data holder is making data available to a large data recipient;
- data is being shared between two large firms.

The Data Act is also more specific in the case of data sharing to SMEs, proposing that SMEs should be able to access data on cost-based terms.

4.2 Determining compensation for data access

FRAND access terms are normally applied to products that are an important input for a downstream market. Examples of such terms are standard essential

patents (SEPs) and wholesale access to telecoms networks with significant market power.

FRAND is designed to provide a reasonable return in order to preserve incentives for providers to operate their input and continue innovating, while at the same time preventing these providers from unreasonably profiting from the removal of competition by foreclosing access with higher prices.[47] FRAND terms thus need to take account of two balancing objectives:

- access to the essential input;
- continued provision of that input.

If a certain piece of data is vital to offering a service, can be obtained from only one place, and cannot be easily replicated, it may be considered appropriate to impose access on FRAND terms in order to ensure that downstream competitors can gain access to the data.

However, the benefits from access to data can be reaped only if there are sufficient incentives to collect the data in the first place, which implies that the terms under which data access is regulated are of crucial importance.

FRAND is a well-established but complex concept, and a variety of valuation tools can be used to assess what constitutes a FRAND price for data. Given the specific circumstances of the data and the objectives of the party valuing the data, one or more of these methods will be appropriate, as follows.

- **Cost-based**: this method examines the costs associated with creating, storing, processing and sharing the data. It will require a full allocation of the costs associated with providing the good or service, including investments and common costs. This is particularly challenging in the case of high fixed-cost, low marginal-cost goods. This method of valuation is not appropriate when the input can be replicated elsewhere or obtained from another source, and where innovation or incentivising future investment is important.
- **Benchmark- or market-based**: this method looks at the prices at which data is traded between willing buyers and willing sellers. if there is a concern about the fairness of the price of access then this price can be benchmarked against those of equivalent goods. However, this is challenging for highly bespoke products, or products where there is no comparable market.
- **Income-based**: this method involves a bottom-up estimation of future revenues according to each business activity that employs the data. A challenge with this approach is that the data holder will need access to significant amounts of data from the access seeker.
- **Externalities-based**: this method looks at the broader impact of data. If the prime objective is to maximise the value to society of the available data, an externalities-based approach can be used to ensure that prices paid allow for the optimal use of the asset to ensure certain market outcomes. This approach is likely to be time- and cost-intensive, as assessing the value of data to society is not straightforward and usually involves surveys and/or natural experiments.

An appropriate valuation methodology is crucial in ensuring that both sides of the market are supported in line with the policy's aims. Indeed, there are

myriad risks to the success of the data ecosystems if an inappropriate pricing methodology is applied.

First, it is important to note that FRAND prices must be context-dependent. This means that FRAND prices must take into account the precise characteristics of the data collected. In particular, they should take account of:

- how the data was collected—was it volunteered, derived or inferred?
- the type of data collected—does it involve activity or behavioural data (e.g. what people buy), user-generated content (e.g. communications), social data, locational data, demographic data, or biometric data?

These characteristics of the data will determine the cost of data collection as well as the time over which the data remains relevant. As part of the policy goal is to foster greater innovation and investment in data collection, an access price that takes account of the 'value to the owner' (i.e. compensates the access-giver for the risk of investing in the asset and loss of exclusivity) may be more appropriate.[48]

Second, differentiated pricing may be necessary to reflect the differing uses of data by the acquiring party. The value of data can differ greatly depending on the context in which it will be used, and setting an equivalent price—on the grounds of non-discrimination—could lead to either some firms being priced out of the market, or the inadvertent subsidisation of other firms at the expense of data generation.

Prices can be considered to be non-discriminatory even when different fees are charged to different users, as long as 'similarly situated' data recipients have access on the same terms. There are examples of differentiated pricing in other regulated sectors, such as the EU's financial Benchmarks Regulation, in which firms are grouped based on the characteristics of the input that they wish to purchase (see Box 4.2).

Box 4.2 Case study: FRAND pricing for benchmark data access—the need for flexibility

One market in which FRAND terms have been applied is in access to financial benchmarks, as outlined in Article 22 of the EU's Benchmarks Regulation.[1] Some benchmarks, such as the LIBOR rate or market indices, are widely used across the financial sector as inputs to services. These benchmarks are often produced by one firm, where a purchaser would not be able to buy access to an equivalent benchmark from another firm, and as such the producer of the benchmark enjoys monopoly power. As a result, the Regulation mandates that these benchmarks are purchased on FRAND terms to ensure that they are accessible to a wide range of market participants and to stop the producer of the benchmark abusing its position.

It is important to note, however, that despite the non-discriminatory terms outlined in the Benchmarks Regulation, there is scope for vendors of benchmarks and information relating to benchmarks to differentiate the prices charged for data access, but only 'where objectively justified, such as in terms of the quantity, scope or field of use demanded and applied in a proportionate manner.'[2] This is applied in particular to where benchmark data is used by a central counterparty clearing house (CCP).

Furthermore, the Regulation requires that 'different categories and the criteria defining the various categories of CCPs and trading venues should be made publicly available.'[3] This means that the burden is on the vendor of the benchmark to define objectively reasonable and proportional categories of purchaser and to state these definitions publicly.

Source: [1] European Commission (2016), 'Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014', 29 June.
[2] European Commission (2016), 'Commission Delegated Regulation (EU) 2016/2021 of 2 June

2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council on markets in financial instruments with regard to regulatory technical standards on access in respect of benchmarks', 2 June.

There are parallels between the implementation of the EU's Benchmarks Regulation and the implementation of the Data Act, as there may be reasonable grounds for differentiated pricing of data depending on the firm purchasing it, and how that data will be used in aftermarket services. Allowing for a reflection of the use of data in the price charged for it can both protect investment incentives and allow for cheaper data provision for the most innovative products that do not directly compete with the original device's aftermarket services.

Third, a strict direct cost-based method is not likely be appropriate, as it would undermine the incentives to invest in data-generating products. This is particularly salient where SMEs are purchasing data, as it is currently proposed that this will be on cost-based terms.[49] As SMEs could make up a large proportion of the new entrants offering new aftermarket services, the relationship between a cost-based charging principle and the incentives for incumbents to develop data-generating devices will need to be accounted for.

Moreover, treating SMEs[50] differently may not be appropriate for firms in the digital sector, where staff headcount and revenues can be low for a long time while the company scales and monetises its product. These firms may be small in terms of turnover and headcount, but may be able to supply products and accumulate large quantities of data, and thus be able to operate as competitive actors within the market for IoT data. For example, a few months before Nest, a smart thermostat and smoke-detector manufacturer, was acquired by Google for US$3.2bn, the brand had only around 200 employees.[51]

Finally, it is worth noting that a large amount of data sharing can also take place under commercial negotiation, as shown by the fact that the market for IoT devices and data generation has expanded significantly in recent years, even in the absence of the Data Act (as noted previously). We understand that the Data Act aims to further facilitate this growth, and ensure that the data generated is used more widely in new aftermarket applications. As much data sharing has already taken place under commercial terms, this evidence points to the use of either a benchmark- or externality-based valuation methodology, as this would ensure that the incentives that are already present in an expanding market are maintained and potentially extended.

In summary, FRAND terms are a complex issue and must be assessed alongside a specific policy objective. The FRAND obligations within the Data Act should seek to address the trade-off between maintaining incentives for investment in innovative devices, allowing for contestability in the market for related services, and offsetting possible competition concerns by ensuring fair contractual terms. This highlights the tension between the Data Act's aims to grow the market for IoT devices and data generation, and its aim to fully unlock the value of that data. Full account must be taken of these competing aims to ensure that the compensation paid for access to data, under the FRAND terms, achieves a balance. The tension is between the fairness that is appropriate to data generators and providers of services, and is discussed further in section 5.

5 Conclusions and recommendations

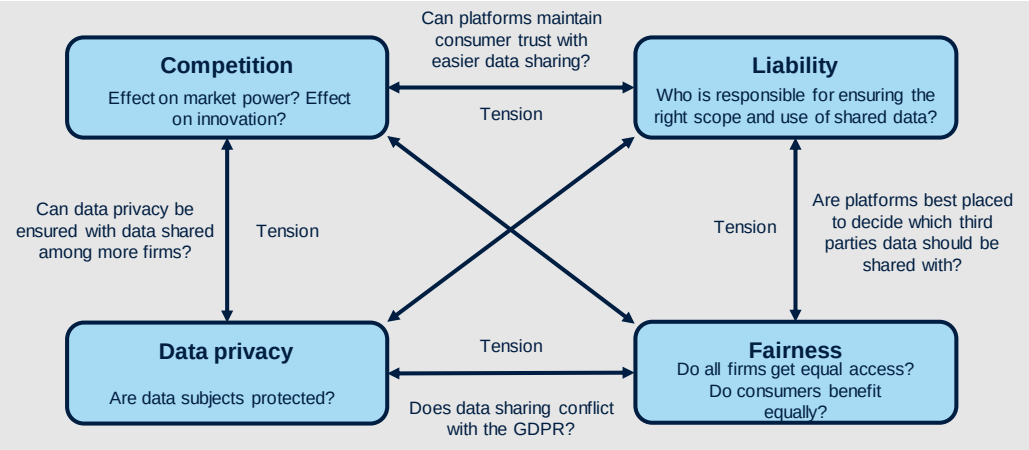
The Data Act highlights tensions between conflicting policy objectives. In this report we have identified a number of these tensions, both between the competing objectives of the Data Act and between the Data Act and other existing or proposed regulations.

5.1 Tensions within the Data Act

Some of the key objectives of regulation in digital markets can be categorised into four broad pillars (see Figure 5.1):

- **competition and innovation**: requiring contestability of the market to foster static competition, while maintaining investment incentives for innovation by incumbent firms;
- **data protection and privacy**: ensuring that data is handled securely and consumers are able to exercise meaningful choice over who can use their private data and how;
- **liability**: ensuring an appropriate balance of responsibilities for data security between data ecosystems and their users;
- **fairness**: overcoming perceived inequities between large data holders and small firms that require access to data.

Figure 5.1 Categorising the Data Act's internal and external tensions



Source: Oxera.

Tensions exist within and between these various objectives, as proposed obligations in the Data Act may have the desired effect on one objective but the opposite effect on another. For example:

- while contestability requires more access to key data ecosystems, the wide scope of access may undermine investment and user privacy objectives;
- there is a tension between the objective of fair access to data for all firms, and ensuring the security of a data ecosystem;
- tensions between liability and data privacy may be captured in the question of whether data subjects or the data holders are considered key actors for ensuring the privacy and security of the subject's data. For example, does the Data Act expect users to verify that the firm getting access to data is trustworthy and has the right infrastructure in place to treat data securely?

5.2 Recommendations

As policymakers continue to debate and amend the Data Act, a number of key principles may help to ensure that they find a balance between the tensions considered in this report.

- **Keep the scope of the data limited to its purpose**: in keeping with the data minimisation principle of the GDPR, maintaining a narrow scope of data and related services (to cover only data that is transmissible, accessible to the data holder, can be verifiably linked to a user, is required for the primary functioning of the product, and has not been processed) will help to ensure that both the investment incentives, and security and trust of the underlying data ecosystem are not undermined and that fundamental rights to privacy are protected.
- **Ensure that the scope avoids revealing business-sensitive data**: requiring companies to share data that could give third parties access to trade secrets would discourage investment in data collection.
- **Avoid asymmetries**: with parallel legislation—such as the DMA—tackling issues of market power, the Data Act would ideally focus on promoting data sharing across the digital economy, without asymmetries between participants. Otherwise it will restrict user choice regarding the data and services usage, potentially leading to lock-in effects that would be contrary to the aims of the Data Act and the DMA. Ultimately, this may risk limiting the user's right to use a product or service of their choice and, in some cases, hinder innovation.
- **Appropriate application of FRAND terms**: compensation for data sharing must reflect the high fixed costs of data generation, rather than focusing on the low costs of sharing data that have already been generated, if it is to encourage investment and dynamic competition. To ensure this, the Data Act should remain flexible in its pricing methodology and avoid being too prescriptive, to allow recognition of different data types and usage.

[1] European Commission (2022), 'Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data', 23 February, p. 1.
[2] Ibid., p. 1.
[3] Ibid., p. 2.
[4] Ibid., p. 3.
[5] Ibid., p. 20.
[6] Ibid., p. 17.
[7] Transforma Insights (2020), 'Internet of Things (IoT) total annual revenue worldwide from 2019 to 2030 (in billion U.S. dollars)', December; Transforma Insights (2020), 'Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical', December.
[8] Hunke, N., Yusuf, Z., Rüßmann, M., Schmieg, F., Bhatia, A. and Kalra, N. (2017), 'Winning in IoT-It's all about the business processes', *bcg.perspectives*.
[9] European Commission (2022), 'Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data', 23 February, p. 3.
[10] European Commission (2021), 'European Council meeting (21 and 22 October 2021) – Conclusions', 22 October, p. 2; Shapiro, C. (2012), 'Competition and Innovation: Did Arrow Hit the Bull's Eye?', in J. Lerner and S. Stern (eds), *The Rate and Direction of Inventive Activity Revisited*, University of Chicago Press, pp. 361–410.
[11] Segal, I. and Whinston, M.D. (2007), 'Antitrust in innovative industries', *American Economic Review*, **97**:5, pp. 1703–1730.
[12] Research for the Dutch Ministry of Economic Affairs and Climate Policy (2020), 'Exploring data sharing obligations in the technology sector', 30 November, p. 25.
[13] Evans, D.S. and Schmalensee, R. (2002), 'Some economic aspects of antitrust analysis in dynamically competitive industries', *Innovation Policy and the Economy*, **2**, pp. 1–49.
[14] All Tesla vehicles are fitted with the sensors needed to enable autopilot or some self-driving capabilities, but the use of these services is dependent on a subscription to software from Tesla; see Tesla website, 'Support: Autopilot and Full Self-Driving Capability', accessed on 16 August 2022.

[15] BEREC (2022), 'BEREC High-Level Opinion on the European Commission's proposal for a Data Act', p. 12.
[16] Other than the exclusion of Gatekeepers, which is further explored in section 2.3.
[17] European Commission (2016), 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', recital 7.
[18] Frost & Sullivan (2018), 'The Global State of Online Digital Trust', pp. 7–9.
[19] Kretschmer, T., Leiponen, A., Schilling, M. and Vasudeva, G. (2022), 'Platform ecosystems as meta-organizations: Implications for platform strategies', *Strategic Management Journal*, **43**:3, pp. 405–424.
[20] Ibid.
[21] BCG (2021), 'Building Trust in Business Ecosystems', February.
[22] Consumer International and Internet Society (2019), 'The trust opportunity: exploring consumers' attitudes to the internet of things'.
[23] Ibid.
[24] Ibid.
[25] Kretschmer, T., Leiponen, A., Schilling, M. and Vasudeva, G. (2022), 'Platform ecosystems as meta-organizations: Implications for platform strategies', *Strategic Management Journal*, **43**:3, pp. 405–424.
[26] BullGuard (2016), 'Despite fast adoption of Internet of Things, a shocking 72 per cent of consumers don't know how to secure their connected devices', press release.
[27] Mazzetti, M., Perlroth, N. and Bergman, R. (2019), 'It Seemed Like a Popular Chat App. It's Secretly a Spy Tool.', *The New York Times*, 22 December.
[28] For example, see the Connectivity Standards Alliance website for more detail on the initiative.
[29] European Commission (2020), 'Case M.9660-Google/Fitbit commitments to the European Commission', 17 December, p. 16.
[30] Even though consumers show concerns over data collection and platform security, they do not take available actions to avoid private data collection. For example, only 14% of consumers encrypt their online communications, with around 30% changing their password regularly. McKinsey (2020), 'The consumer-data opportunity and the privacy imperative', April.
[31] Mukhopadhyay, S., de Reuver, M. and Bouwman, H. (2016), 'Effectiveness of control mechanisms in mobile platform ecosystem', *Telematics and Informatics*, **33**:3, pp. 848–859.
[32] European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, recital 22.
[33] European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, pp. 41–42.
[34] Ibid., p. 43.
[35] Ibid., p. 26.
[36] European Commission (2020), 'Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)', 15 December, pp. 40–41.
[37] European Commission (2021), ' Inception Impact Assessment', 21 May.
[38] Tech monitor (2015), '10 of the biggest IoT data generators'.
[39] Body of European Regulators for Electronic Communications (2022), 'BEREC High-Level Opinion on the European Commission's proposal for a Data Act', p. 8.
[40] Ibid., p. 8.
[41] BCG (2020), 'The Serial Innovation Imperative - the most innovative companies 2020'; Forbes (2018), 'The world's most innovative companies'.
[42] Cabral, L. (2018), 'Standing on the Shoulders of Dwarfs: Dominant Firms and Innovation Incentives', *CEPR*, Discussion Paper No. DP13115; Acemoglu, D. and Cao, D. (2015), 'Innovation by entrants and incumbents', *Journal of Economic Theory*, **157**, pp. 255–294.
[43] European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, p. 13.
[44] Ibid., pp. 47–48.
[45] Ibid., p. 26.
[46] Ibid., p. 2.
[47] Marshall, N., Jenkins, H. and Niels, G. (2008), 'The Price of Intellectual Property: What is FRAND?', in *Global Competition Review*, 'The Handbook of Competition Economics: A Global Competition Review Special Report'.
[48] Oxera (2021), 'If data is so valuable, how much should you pay to access it?', *Today's Agenda*, 4 February.
[49] European Commission (2022), 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 23 February, p. 44.
[50] Defined by the EU as an enterprise that employs fewer than 250 people and which has an annual turnover not exceeding €50m, and/or an annual balance sheet total not exceeding €43m. See European Commission (2003), 'Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422)', 6 May, Article 2.
[51] Andersen, D. (2013), 'From The Garage To 200 Employees In 3 Years: How Nest Thermostats Were Born', *Tech Crunch*, 13 May.

www.oxera.com

oxera
compelling economics