A review of amendments to the DMA by Parliament and the Council

Prepared for the Computer and Communications Industry Association

10 January 2022

www.oxera.com

oxera
compelling economics

Contents

Figures and tables

About Oxera

Oxera has provided a leading voice in competition and regulatory policy across a range of sectors for over 30 years. In the digital space, we are an active participant in the debate that is unfolding around Europe, having hosted roundtable discussions between regulators, policymakers, firms and academics in Berlin, Brussels, London and Paris.

Oxera works with many large and small platforms, as well as consumer bodies and regulators, to build a robust and widespread understanding of the economic and social impact that technology has on its users and markets. We also advise and act as experts on antitrust cases, mergers, damages, and other disputes in the digital sector.

Through this experience, we have developed a deep understanding of the business models employed by online platforms, how they are used by consumers and businesses, and the effects—both positive and negative—that various policy and regulatory proposals are likely to have on consumer behaviour, commercial incentives, and market outcomes.

We also work closely with leading academic experts and former regulators, many of whom work with us as Oxera Associates or Project Advisers.

Executive summary

On 15 December 2020, the European Commission published a draft Digital Markets Act ('DMA'), proposing new rules for the largest online platforms. A year later, on 15 December 2021, the European Parliament ('Parliament') adopted the final amendments that it will take into the trilogue negotiations. In parallel, the European Council ('the Council') reviewed the DMA and adopted a 'General Approach' text on 26 November 2021.

While many of the amendments provide more protection for business users, they often overlook the negative impact on end-users. In light of this, the Computer & Communications Industry Association ('CCIA') asked Oxera to review the three texts, focusing on the **unintended consequences** for consumers that could result from proposed changes to: (i) data separation; (ii) product and services integration; (iii) interoperability and interconnection; and (iv) business model choice.

We found some amendments by Parliament and the Council that **improve the balance** of the proposed obligations. For example, amendments to Articles 5(a), 6.1(c) and 6.1(f) would add exemptions to the obligations around data processing and interoperability, allowing platforms to **continue protecting** platform integrity, end-user data protection, and cyber security. This would **benefit consumers** by enabling innovative safety and security features such as Microsoft's Defender suite, which combines data from across its ecosystem to isolate threats.

At the same time, a number of amendments introduced by Parliament risk **worsened outcomes** for consumers over the long term.

First, amendments to recital 46 make an unrealistic demand of platforms by requiring that the 'less personalised' alternative is of the same quality as the personalised service, resulting in all users receiving the 'less personalised alternative'. This will **degrade the consumer experience** if, for example, Amazon cannot personalise its service based on a user's search history, related offers, and product reviews from across its ecosystem—even if that user has agreed to their data being combined.

Second, amendments to the scope of Article 6.1(d) and restrictions on product integrations in recital 48 would **hamper product improvement and reliability** while worsening the 'out-of-the-box' experience for users. For example, Google Search draws on data and functionalities from other Google services (such as Maps or News) to offer users an improved interface and more accurate results.

Third, extending the scope of Articles 6.1(f) and 6.1(c) to include access to more platform functions for third parties would **increase governance risks** by preventing platforms from balancing the degree of interoperability and access granted to third parties in ways that optimise security, quality and trust. For example, Apple's restrictions on the use of Mobile Device Management tools in consumer-facing apps helps preserve user privacy while still offering contestability through APIs.

Fourth, amendments to recital 49, requiring all services to be commercially viable on a standalone basis, would **undermine cross-subsidisation** by platforms and jeopardise ad-funded businesses. For example, Facebook's ad-funded business model cross-subsidises the introduction of new functionalities on the consumer side. Uncertainty over whether changes to services will be considered improvements to a core platform or new services that must be viable on a standalone basis could **inhibit innovation** and the deployment of new features.

Fifth, mandating free interoperability in Article 6.1(f) would **reduce innovation incentives**, meaning fewer features and functionalities for consumers. Innovators must be permitted to share in the value of their innovations if they are to have an incentive to incur the costs and risks required to develop them. Undermining this will ultimately reduce choices of products and services for consumers in the future.

Finally, light amendments to Articles 5(c) and 5(e) maintain the obligation to allow business users to steer end-users off-platform, which puts the viability of **commission-based business models at risk**. If this is replaced with a less efficient alternative, consumers could end up worse off.

Applying all of these restrictions to every gatekeeper platform as a one-size-fits-all solution would **undermine many platform business models**, forcing changes that could lead to increased prices for both businesses and consumers.

We recommend that throughout the trilogue process policymakers seek out **the most flexible** approach possible, maximising the scope for enforcers to make a **holistic assessment** of the market context in which obligations apply, and to assess the impact of those obligations on consumers and businesses.

Amendments that increase the possibility for **regulatory dialogue** will also help reduce legal uncertainty and minimise the risk of future litigation. At the same time, by recognising that some **obligations must be tailored** to a platform's specific economic context, the DMA can avoid the unintended consequences that would worsen outcomes for consumers.

1 Introduction

In December 2020, the European Commission ('the Commission') tabled proposals for a Digital Markets Act ('DMA') that will impose ex ante regulation on a number of 'core platform services' (CPSs) to increase contestability and fairness in Europe's digital economy.[1] The Commission's proposals include 18 obligations and prohibitions that, if enacted, would change the way that CPSs are designed and presented to users.

Since then, the European Parliament's Committee on the Internal Market and Consumer protection ('IMCO') has taken the lead on proposing amendments for Parliament to debate. On 22 November 2021, IMCO published its approved compromise text.[2] On 15 December, the European Parliament ('Parliament') adopted the final amendments ('Parliament's amendments') which will be taken into the trilogue process.[3]

The European Council ('the Council') has reviewed the Commission's proposals concurrently, and on 26 November it agreed on amendments ('the Council's amendments') to take into the trilogue.[4]

In light of this, the Computer and Communications Industry Association ('CCIA') asked Oxera to consider the relative risks and merits of the competing proposals in relation to:

1. data separation;
2. the integration of products and services;
3. interoperability and interconnection;
4. business model choice.

Our review covers eight key articles—2(23b), 5(a), 5(c), 5(e), 6.1(b), 6.1(d), 6.1(c) and 6.1(f)—and three related recitals—36, 48 and 49—with a focus on their potential unintended consequences for consumers. Throughout this report, we highlight where the amendments proposed by Parliament or the Council improve on the Commission's original text, as well as where they introduce new risks to the quality and choice of services for consumers in the long run.

Section 2 highlights the value of exemptions proposed to the data separation provisions, which would allow for safety and security benefits. We also explain why Parliament's amendments would prevent gatekeepers from offering personalised products and services to *any* user, given how platforms use personal data to enhance user experiences.

Section 3 explains how limitations on the preferential or embedded display of services could amount to a prohibition on product integration, worsening

[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. Henceforth referred to as 'Commission proposal'.
[2] European Parliament IMCO Committee (2021), 'Compromise Amendments', Andreas Schwab version of 18 November 2021 ('the IMCO compromise amendments').
[3] European Parliament (2021), 'Amendments adopted by the European Parliament on 15 December 2021 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD))(1)', 15 December.
[4] Council of the European Union (2021), 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) - General approach', Permanent Representatives Committee (Part 1), version of 16 November, voted on 26 November 2021 ('the Council General Approach').

outcomes for consumers. Moreover, the catch-all approach adopted in the proposals prevents users from opting in to a more integrated experience.

Section 4 considers the governance risks that stem from interoperability and interconnection provisions with increased scope. We also consider the importance of limitations or exemptions to interoperability for platform integrity, while highlighting that good governance goes beyond just 'hardcore' security.

Finally, section 5 examines how several amendments could put certain platform business models at risk, thereby reducing consumer choice: the functional separation of gatekeeper services undermines cross-subsidisation; free of charge access and interoperability has an adverse effect on innovation; and obligations to allow off-platform steering and services integration restrict commission-based models. We end by considering the need for a holistic review of the DMA obligations to ensure the full effect on platform businesses and their users is fully understood.

Section 6 concludes with a summary of our findings, highlighting where the amendments introduce more balance to the obligations and where they could have unintended consequences that impact negatively on consumers. We also propose a list of recommendations for the legislators to take into account during the trilogue negotiations.

Overall, we recommend that the trilogue seeks to adopt the most flexible and tailored approach possible for the enforcement of DMA obligations, to preserve quality and choice for consumers in the EU.

2 Data separation

Both Parliament and the Council have proposed amendments to Article 5(a) that reinforce the obligation to obtain user consent before combining personal data (see Table 2.1).

Table 2.1 Amendments to Article 5(a)

The Parliament's amendments	The Council amendments
refrain from combining **and cross using** personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice **in a** *[sic]* **explicit and clear manner,** and **has** provided consent in the sense of Regulation (EU) 2016/679.	~~refrain from combining~~ **not combine** personal data sourced from **any of** these core platform services with personal data from any ~~other~~ **further core platform service or further** services offered by the gatekeeper or with personal data from third-party services, and ~~from signing~~ **not sign** in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of **Article 6(1) point (a) of** Regulation (EU) 2016/679. **The gatekeeper may also rely on the legal basis included under Article 6(1) points (c), (d) and (e) of Regulation (EU) 2016/679, where applicable;**

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

Parliament's proposals focus on the need for consent to be explicit and clear, while also clarifying that the scope of the obligation includes the '*cross using*' (as well as the combination) of personal data between different services. In contrast, the Council stresses that the scope of the restriction includes data from other CPSs, while proposing a closer alignment of the DMA with the existing obligations—and certain exemptions—set out in the General Data Protection Regulation (GDPR).[5]

As discussed in section 2.1, platforms can cross-use data to better safeguard their ecosystems and users. This highlights the value of the exemptions to the consent requirements added by the Council, as they would enable a continuation of these innovative safety and security features.

Furthermore, both Parliament and the Council have proposed amendments to recital 36, which clarifies the intention of the data separation provisions as a means of preventing data advantages among designated gatekeepers (see Table 2.2).

[5] General Data Protection Regulation (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)', Official Journal of the European Union.

Table 2.2 Amendments to Recital 36

Parliament's amendments	Council General Approach
[…]	[…]
To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised **but equivalent** alternative. **The less personalized alternative should not be different or of degraded quality compared to the service offered to the end users who provide consent to the combining of their personal data**.	To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised **but equivalent** alternative, **and without making the core platform service or certain functionalities thereof conditional upon the end user's consent in the sense of Article 6(1) point (a) of Regulation (EU) 2016/679**.
[…]	[…]
	The less personalized alternative should not be different or of degraded quality compared to the service offered to the end users who provide consent to the combining of their personal data, unless the initial quality of the service provided precisely depends on the combination of such data.
	[…]
	At the time of giving consent, the user should be informed that a refusal may lead to a less personalized offer, but that otherwise the core platform service will remain unchanged and that no functionalities will be suppressed.
	[…]

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

These amendments would both require platforms to offer users a 'less personalised but equivalent service'. However, Parliament's proposals make an unrealistic demand of platform operators by stipulating that the less personalised alternative must not be 'different or of degraded quality'. In contrast, the Council acknowledges that some aspects of service quality can *depend on* platforms combining personal data, and these cannot be replicated in the less personalised alternative. The Council nevertheless clarifies that access to the core platform service must not be conditional on users consenting to such personalisation.

In section 2.2, we explain that Parliament's approach misunderstands how platforms use personal data to create value for consumers and would, in effect, mean that *all* users receive the 'less personalised alternative'.

2.1 Security and integrity exemptions benefit consumers

Whereas Parliament's amendments seek to strengthen consumer choice by requiring that consent be obtained in an 'explicit and clear manner', the Council calls for a closer alignment with the existing personal data provisions set out in the GDPR.

In particular, the Council recognises the benefit of including certain exemptions to the consent requirements. Article 6(1) points (c), (d) and (e) of the GDPR—as referred to explicitly in the Council's amendments to the DMA—allow for the processing of personal data *without* explicit user consent if:

> […]
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> […]

As these GDPR provisions recognise, access to cross-service personal data can help platforms to improve the quality, security and integrity of their ecosystems. For example, Microsoft combines personal data from across its product suite to better identify and isolate cyber threats and protect its users (see Box 2.1).

Box 2.1 Case study: Microsoft threat detection

With an increasing array of devices and services operating online, consumers and businesses face a greater risk of cyberattack. This gives rise to a growing demand for security features that can help users to efficiently identify and mitigate cyber-security risks.

Modern threats often develop as an 'attack chain', comprising several related attacks on different users or services within a network. While these attacks may be tackled by an array of individual defence mechanisms, the threat can be more efficiently mitigated by gathering and merging information from across the different points in the chain.

Microsoft 365 Defender combines security insights from across the Microsoft ecosystem to better identify indicators of an attack and generate alerts. The Defender suite includes 'Defender for Endpoint', providing preventative protection and post-breach detection, and 'Defender for Office 365', safeguarding emails, links and other collaboration tools. It provides tools for detection, prevention and response across multiple users, devices and applications.

To do this, Microsoft needs to access a variety of business and personal data from different digital services, including emails, documents, browsers, operating systems and cloud services. For example, if Defender for Endpoint identifies a malicious file, it coordinates with Defender for Office 365 to scan and remove the file from emails and block the file across the network.

Finally, users benefit from cross-service data analytics as these enable coordinated detection of risks and display of unified alerts and solutions from across the Microsoft ecosystem, removing the need to navigate multiple security platforms to detect and resolve a threat.

Source: Microsoft (2021), 'Microsoft 365 Defender', February; Microsoft (2021), 'Microsoft Defender for Endpoint data storage and privacy', June; Microsoft (2021), 'Privacy, security, and transparency', June.

If an individual's choices can limit a platform's ability to gather the data it needs to improve safety, security and integrity, it reduces the protection offered to *all* users—not just those who withhold their consent for personal data to be cross-used and combined.

First, less secure users can pose a threat to the wider ecosystem if their behaviour makes them more susceptible to being hacked. Second, 'bad actors' within the ecosystem are the least likely to consent to their data to be combined, as it would aid in the detection of their activities.

The amendments by the Council recognise the interconnectedness of users in a platform ecosystem and better protect the positive externality on consumers arising from safety and security features that rely on cross-service data analytics.

2.2 Product personalisation requires differentiated services

Parliament's changes to recital 36 make an unrealistic demand of platform operators by requiring that the same quality of service be offered to all users, irrespective of whether they allow their personal data to be combined. This belies a misunderstanding of how platforms use data to create value for consumers by offering higher quality and more personalised products, services and content.

The cross-use or combining of data supports improved product development in two broad ways:[6]

1. *within-user learning*: where data is used to improve the services for an individual, based on their preferences and prior usage;
2. *across-users learning*: where a product or service is improved based on aggregated data insights from across all users.

Importantly, while service improvements based on *across-users* learning may be applied to all users (irrespective of whether or not they consent to their data being combined), those quality improvements that relate to *within-user* learning are specific to the individual and can *only* be offered to users who consent to the cross-use and combination of their personal data. For example, Amazon uses data on a consumer's searches, related offers, and product reviews from across its ecosystem to improve its product and service recommendations to consumers (see Box 2.2).[7]

[6] Hagiu, A. and Wright, J. (2021), 'Data-enabled learning, network effects and competitive advantage', May; Parker, G., Petropoulos, G. and Van Alstyne, M.W. (2021), 'Platform mergers and antitrust', January.
[7] Bernard Marr & Co. (2021), 'Amazon: Using Big Data to understand customers', 23 July; Lineate (2019), '3 Ways Amazon Uses AI to Make Product Recommendations', 16 December.

Box 2.2 Case study: Amazon product personalisation

Amazon is one of the largest online retailers, offering products from more than 200,000 sellers in Europe. However, this means that a user searching for a product on Amazon can receive a large number of similar results; for example, a simple search for 'laptops' returns over 1,000 offers.

To help users find their best options in this long list of potential matches, Amazon uses an algorithm called 'item-based collaborative filtering', which delivers a personalised store experience to each user. This algorithm is informed by data on a consumer's previous searches, their browsing history, related offers, and product reviews from across Amazon's ecosystem (including Marketplace, the Alexa voice assistant, and Amazon Go).

While some data can be used to improve the selection process for all consumers (e.g. alerting them to faulty products coming from a specific seller), other information—specific to the user conducting the search—can lead to more personalised results and a better match for the consumer.

Moreover, better product personalisation can benefit businesses that list their products on Amazon's Marketplace. The share of third-party units sold on Amazon has increased over the last decade to a new peak of 55% in the first quarter of 2021. Better matching based on personal data helps these vendors to be more easily discovered by potential consumers, which highlights how platforms enable third parties to offer their goods and services more efficiently.

Source: Bernard Marr & Co. (2021), 'Amazon: Using Big Data to understand customers', 23 July; Lineate (2019), '3 Ways Amazon Uses AI to Make Product Recommendations', 16 December; Search of the term 'laptops' on amazon.co.uk on 1 December 2021; Statista (2021), 'Share of paid units sold by third-party sellers on Amazon platform as of 2nd quarter 2021', July; Teece, D.J. (2018), 'Business models and dynamic capabilities', *Long Range Planning*, **51**:1, pp. 40–49; Parker, G., Alstyne, M.V. and Jiang, X. (2017), 'Platform ecosystems: how developers invert the firm', *MIS Quarterly*, **41**:1, pp. 255–66; Statista (2019), 'Number of active Amazon marketplace sellers in 2019, by country', December.

Other user experience improvements *require* access to combined personal data in order to function. For example, Google users can view and update their personal information and privacy settings for all their services and devices (such as Gmail, YouTube, Maps and Android phones) via a single Google Account dashboard,[8] while Apple users can access customer support for all their devices via Apple's 'My Support' facility. While these centralised services offer greater clarity and convenience to consumers, they necessarily require platforms to combine a variety of data (including personal data) from across their ecosystems.

Under Article 5(a) of the DMA, platforms would only be able to offer these kinds of personalisation improvements to users who had explicitly consented to having their personal data combined. However, the Parliament's amendments would mean that platforms could *not* offer a less personalised alternative that is of 'a different or degraded quality'.

Since personalisation is an important dimension of quality, the only way that platforms could comply with this obligation would be to offer the 'less personalised alternative' to *all* users—even those who consented to having their personal data combined. This would have a direct effect on Europe's platform users (including both consumers and businesses) by removing their choice to opt in to a more personalised ecosystem.

In contrast, the Council amendments recognise these technical constraints and allow for differences in quality between the personalised and less

[8] See Google Accounts help page, 'Get a summary of data in your Google Account', available at: https://support.google.com/accounts/answer/162744?hl=en&ref_topic=7188671, accessed 16 November 2021.

personalised services, while still stipulating that the access to the core platform services must not be conditional upon the user consenting to their data being combined.

Finally, both Parliament's and the Council's amendments appear to assume that platform business models will continue to be based around zero-priced data. It is ambiguous whether designated gatekeepers can introduce charges for users who do not consent to their data being combined, or, equivalently, make payments to consumers who *do* consent. The text could be improved by making clear that these options *are* available to platform operators, helping to future-proof the DMA against the evolution of online business models.

3 Product and services integration

Article 6.1(d) of the Commission's proposal includes restrictions on how platforms can treat their own products and services in rankings. Parliament's amendments extend the scope of these provisions to include 'other settings'; in contrast, the Council's amendments maintain the Commission's focus on rankings while taking third-party entities belonging to the gatekeeper out of scope (see Table 3.1 below).

Table 3.1 Amendments to Article 6.1(d)

Parliament's amendments	Council General Approach
[…] ~~refrain from treating~~ **not treat more favourably** in ranking **or other settings**, services and products offered by the gatekeeper itself or by any third party belonging to the same undertaking compared to similar services or products of third party and apply **transparent,** fair and non-discriminatory conditions to such **third party services or products** ~~ranking~~; […]	[…] refrain from treating more favourably in ranking services and products offered by the gatekeeper itself ~~or by any third party belonging to the same undertaking~~ compared to similar services or products of third party and apply fair and non-discriminatory conditions to such ranking; […]

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

Furthermore, Parliament proposes amendments to recital 48, stipulating that the *'*preferential or embedded display of a separate online intermediation service shall constitute a favouring*'* (see Table 3.2 below).

Table 3.2 Amendments to recital 48

Parliament's amendments
[…] When offering [its own] products or services on the core platform service, gatekeepers can reserve a better position to their own offering, in terms of ranking, as opposed to the products of third parties also operating on that core platform service. This can occur for instance with products or services, including other core platform services, which are ranked in the results communicated by online search engines, or which are partly or entirely embedded in online search engines results, groups of results specialised in a certain topic, displayed along with the results of an online search engine, which are considered or used by certain end users as a service distinct or additional to the online search engine. **Such preferential or embedded display of a separate online intermediation service shall constitute a favouring irrespective of whether the information or results within the favoured groups of specialised results may also be provided by competing services and are as such ranked in a non-discriminatory way.** […]

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments.

As discussed in sections 3.2 and 4.2 of our May 2021 report, the economic effects of self-preferencing practices are context-specific.[9] That report goes on to explain how blanket prohibitions on self-preferencing—such as those that Parliament proposes in relation to embedded services—fail to account for the benefits that these practices can bring.

[9] Oxera (2021), 'How platforms create value for their users: implications for the Digital Markets Act', prepared for the Computer and Communications Industry Association, May.

At the same time, the Commission's own impact assessment for the DMA provides four criteria that should be met before a regulatory intervention is justified for a given business practice:[10]

(a) There should be sufficient experience with the harmful effects of the identified unfair practices;
(b) Such experience should point to the egregious nature of the unfair practices in question, which would justify the clear identification of obligations related to them;
(c) To the extent possible, these obligations should be directly applicable; and
(d) The unfair practices should be identified in a clear and unambiguous manner to provide the necessary legal certainty for gatekeepers who would need to comply with them, as well as for business users or consumers that may avail themselves of the choices provided for them.

However, a catch-all prohibition on self-preferencing falls foul of these criteria. In particular, a practice cannot be considered to be of an 'egregious nature' (criteria b) if it can also bring benefit to consumers, while the context-specificity of the concerns makes them difficult to identify in a 'clear and unambiguous manner' (criteria d).

In section 3.1, we explain how Parliament's amendments to Article 6.1(d) and recital 48 could limit the ability of platforms to integrate complementary services, reducing the quality and reliability of their offerings, as well as hampering innovation by third parties on the platform.

In section 3.2, we discuss how the catch-all approach to self-preferencing prohibitions reduces choice, as it does not allow users to opt in to a more integrated service from designated gatekeepers.

3.1 Limiting integration degrades service quality

An important benefit of platform ecosystems is the integration of various features and services to deliver additional value to users. In particular, platform operators can improve a consumer's experience by tailoring the services they offer according to a number of contextual and individual-specific factors.

For example, Google's general search service draws on functionalities and data from across Google's product suite to offer users an improved interface and more accurate results.[11] In some cases, this means displaying information or interfaces from one or more of Google's complementary products within the search results (such as locations on a Google Map, news items from Google News, or travel details from Google Flights). By relying on its own services for these additional inputs, Google offers users an improved interface and greater confidence in the accuracy of its results (see Box 3.1).

[10] See European Commission (2020), 'Executive summary of the impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector', staff working document, 15 December, box at para. 153.
[11] Baldwin, Y.C. and Woodard, C.J. (2009), 'The Architecture of Platforms: A Unified View', in Gawer, A. (ed.), *Platforms, Markets and Innovation*, Edward Elgar Publishing, pp. 19–44.

Box 3.1 Case study: Google product integration

Consumers benefit from a richer user experience through the integration of additional Google products into the Google Search page. Google's Search layout aims to simplify the user experience by presenting results in the most accessible manner possible. Similarly, Google personalises and optimises its services by re-using data from across multiple services in its ecosystem.

For example, Google Maps may be used to make suggestions based on a combination of a user's location, their location histories, and real-time traffic updates, as well as live information on arrival times and delays from public transport authorities. Furthermore, location descriptions and user reviews in maps reduce information asymmetries between businesses and potential consumers, lowering transaction costs and improving quality for consumers.

In the context of the 2016 case *Streetmap.eu Ltd vs Google Inc. & Ors*, the UK High Court found that other mapping providers were lagging behind Google Maps in terms of their quality, given (for example) Google's ability to interpret natural language to identify geographical locations. Furthermore, the integration of third-party mapping services was found to cause delays to the display of search results and a higher risk of inaccuracy. Overall, the Court found that the integration of Google Maps within Google Search was a legitimate means of ensuring the accuracy of the service which improved the quality of the user experience.

Sources: Google (2021), 'Privacy Policy – Why Google collects data'; Google (2021), 'How Search algorithms work – Context and settings'; Oxera (2021), 'How platforms create value for their users: implications for the Digital Markets Act', prepared for the Computer and Communications Industry Association, May; UK High Court (2016), *Streetmap.eu Ltd vs Google Inc. & Ors*, 18 October.

Prohibiting integrations like these—as proposed by Parliament under its amendment to recital 48—could worsen the consumer experience. This would particularly be the case where a designated gatekeeper's services are of a superior quality to the third-party alternatives, or where consumers prefer a more integrated experience 'out of the box'. Furthermore, it is difficult to define clear performance metrics for third-party collaborators when consumers value aspects of experience that are not easily quantifiable (such as convenience and trust). In this context, limiting platforms' control over the features and services included in their interfaces could lead to consumers experiencing lower-quality products.

Additionally, extending the scope of these self-preferencing restrictions to include 'other settings'—as proposed in Parliament's amendments to Article 6.1(d)—could have a detrimental effect on the quality and security of innovations by third-party developers and ancillary service providers.

On the one hand, these third parties need to know that core system features will work seamlessly on the platform when designing their products or services, and CPS settings can be an important way for platforms to ensure this. For example, bundling Google's geolocation services with Android supports *innovation on the platform* by ensuring that third-party apps can rely on this system-wide resource.[12]

On the other hand, platforms may need to restrict third-party access to certain settings—or advise users if they *are* accessed—in order to maintain the security and integrity of their ecosystem. For example, while Apple has allowed users to install third-party keyboards on the iPhone since iOS 8, users *must* use the standard iOS keyboard to enter passwords. This helps to protect

[12] Oxera (2018), 'Android in Europe: Benefits to consumers and business', prepared for Google, October, section 2.1.

user security and promote trust in Apple's platform by ensuring that passwords cannot be tracked by third-party keyboard providers.

Similarly, third-party keyboards are installed without network access by default, limiting the functionality that they can provide. Users can grant the keyboard 'full access' in their device settings to enable enhancements such as better predictive typing, or personalised suggestions for names and locations. However, they will first be presented with a confirmation screen asking them to allow their keystroke data to be shared with the third party.[13]

Overall, the combined effect of Parliament's amendments to recital 48 and Article 6.1(d) will be to prevent platforms from integrating their own complementary services, while also reducing the scope for good governance over third-party integrations. This risks diminishing the consumer experience by introducing complexity where many consumers value simplicity. In contrast, the Council's amendments maintain a focus on the key issue of fairness in rankings, which promotes contestability for third parties while avoiding these unintended consequences for end-users.

3.2 A catch-all approach to self-preferencing limits user choice

The issues around limiting integration (as discussed in section 3.1) are compounded by the fact that consumers would be prevented from opting in to a more integrated service if they so wished, limiting their choice. Many users expect new products and services to be ready to use straight 'out of the box'.[14] To deliver this, firms integrate services, pre-install apps, and preconfigure settings, enabling users to experience the full range of functionality they expect when using an app or device for the first time.

For example, Apple's macOS and iOS, are both designed for an intuitive user experience and seamless interaction.[15] When purchasing a new device, consumers expect it to fulfil key functions such as internet browsing, making phone calls, and finding and download apps.[16] Many of the functionalities of Apple products come from the pre-installation and integration of default apps and settings, which are key to meeting these consumer expectations.[17] At the same time, Apple has allowed users to remove the majority of pre-installed apps since the release of iOS 11 in 2017, and it has allowed users to change their iPhone's default web browser and email app since iOS 14 in 2020.[18]

As with the pre-installation of apps, allowing platforms to integrate services can help to ensure a more seamless user experience. However, there is a stark difference between the DMA's approach to pre-installed apps in Article 6.1(b) and Parliament's amendments to Article 6.1(d) and recital 48 relating to the integration of services. In particular, the provisions set out by the Commission in Article 6.1(b) require only that consumers can *remove* pre-installed apps. While both Parliament and the Council have amended this obligation, stipulating that users must also be allowed (or even prompted – e.g. through 'choice screens') to switch defaults, there is no suggestion that the pre-installation of apps or the setting of defaults should be prohibited (see

[13] Welch, C. (2019), 'Apple warns that third-party keyboards on iOS 13 and iPadOS can send data to internet without permission', The Verge, 24 September.
[14] For example, a consumer survey for Application Developers Alliance found that 70% of respondents would prefer to buy an Android device with basic apps pre-installed. See Sterling, G. (2016), 'European survey finds 70 percent of Android owners want pre-installed apps',18 November.
[15] Saxena, H. (2021), 'UX at Apple: the simple principle behind intuitive designs', Bootcamp, 24 November
[16] Sterling, G. (2016), 'European survey finds 70 percent of Android owners want pre-installed apps', Martech, 18 November
[17] Manjoo, F. (2014), 'Apple Strengthens Pull of Its Orbit With Each Device', *New York Times*, 22 October.
[18] Khan, S.H. (2020), 'What Do People Mean When They Say That an iPhone 'Just Works?'', Medium, July.

Table 3.3). Furthermore, we note that while choice screens have been used as competition remedies in the past, there has been much debate as to their efficacy and potential drawbacks for consumers and businesses—highlighting the need for particular care in the design of any such provisions.

Table 3.3 Amendments to pre-installation

Parliament's amendments **Article 5 (g a)**	**Council General Approach** **Article 6.1(b)**
from the moment of end users' first use of any pre-installed core platform service on an operating system, prompt end-users to change the default settings for that core platform service to another option from among a list of the main third-party services available, and allow **and technically enable** end users to uninstall pre-installed software applications on ~~its~~ **a** core platform service ~~operating system~~ **at any stage** without prejudice to the possibility for a gatekeeper to restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third-parties;	[…] allow **and technically enable** end users to un-install any ~~pre-installed~~ software applications on ~~its core platform service~~ **an** operating system **that the gatekeeper provides or effectively controls as easily as any software application installed by end users at any stage, and to change default settings on an operating system that direct or steer end users to services or products offered by the gatekeeper**, without prejudice to the possibility for a gatekeeper to restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third-parties;

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

Indeed, the Commission's own DMA impact assessment acknowledges that this approach is more proportionate than an outright ban on pre-installation:[19]

> Other practices considered and frequently proposed in the literature – like for example banning the pre-installation of software – were replaced by more proportionate obligations – in this case, the possibility to give customers the possibility to always un-install applications […]

At the same time, Article 6.1(b) includes an exemption that allows platforms to restrict the uninstallation of apps that are essential for the functioning of the operating system or device. This helps ensure that consumers can always access the full range of a device's functionality, such as making calls, messaging, health tracking or geolocation—while also guaranteeing that app developers can rely on those functionalities when designing their apps.

In contrast, Parliament's amendments to recital 48, copied in Table 3.2 above, would instil a blanket prohibition on the integration of separate online intermediation services, such as Google Shopping, Google Maps or Google Flights within Google Search. While this may be intended as a means to increase contestability, it has the effect of preventing users from opting in to more integrated services, reducing choice and worsening the experience of consumers who would prefer this.

Finally, we note that Parliament's amendments move Article 6.1(b) (as well as Article 6.1(a)) into Article 5. As Article 5 does not allow for the further specification of the obligations, this reduces the scope for regulatory discussion between the Commission and platforms. Such dialogue is

[19] See European Commission (2020), 'Executive summary of the impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector', staff working document, 15 December, para. 156.

important where there is a degree of subjectivity over an obligation—as is the case here, given the exemption for apps that are ‘essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third-parties’.

4 Interoperability and interconnection

Parliament's proposed addition at Article 2(23b) would introduce a wide definition of interoperability, limiting the ability of platforms to govern access to their ecosystem through the use of APIs and other access technologies (see Table 4.1).

Table 4.1 New Article 23(b)

Parliament's amendments
'Interoperability' means the ability to exchange information and mutually use the information which has been exchanged so that all elements of hardware or software relevant for a given service and used by its provider effectively work with hardware or software relevant for a given services provided by third party providers different from the elements through which the information concerned is originally provided. This shall include the ability to access such information without having to use an application software or other technologies for conversion.

Note: New amendments marked in blue.

Source: Parliament's amendments.

This definition would apply to both Article 6.1(c)—as amended by the Council—and Article 6.1(f) of the Commission's proposals, which require gatekeepers to make it easier for third-party app developers and service providers to interoperate with their platforms. Both Parliament and the Council have put forward substantial amendments to these Articles (see Table 4.2).

Table 4.2 Amendments to Article 6.1(c) and Article 6.1(f)

Parliament's amendments	Council General Approach
(c) allow **and technically enable** the installation and effective use of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the **relevant** core platform services of that gatekeeper. The gatekeeper shall**, where relevant, ask the end users to decide whether they want to make the downloaded application or application store their default setting. The gatekeeper shall** not be prevented from taking **measures that are both necessary and** proportionate ~~measures~~ to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper **or undermine end user data protection or cyber security provided that such necessary and proportionate measures are duly justified by the gatekeeper**;	(c) allow and **technically enable** the installation and effective use **and interoperability** of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the **relevant** core platform services of that gatekeeper. The gatekeeper shall not be prevented from taking **to the extent strictly necessary and** proportionate measures to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper**;** ~~,~~ **provided that such proportionate measures are duly justified by the gatekeeper. The gatekeeper shall furthermore not be prevented from taking to the extent strictly necessary and proportionate measures enabling end users to protect security in relation to third party software applications or software application stores**;

Parliament's amendments	Council General Approach
(f) allow business users, ~~and~~ providers of services **and providers of hardware** ~~ancillary~~ **free of charge** access to and interoperability with the same **hardware and software features accessed or controlled via an** operating system,~~ hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services~~ **provided the operating system is identified pursuant to Article 3(7), that are available to services or hardware provided by the gatekeeper; Providers of ancillary services shall further be allowed access to and interoperability with the same operating system, hardware or software features, regardless of whether the latter are part of an operating system, that are available to ancillary services provided by a gatekeeper. The gatekeeper shall not be prevented from taking indispensable measures to ensure that interoperability does not compromise the integrity of the operating system, hardware or software features provided by the gatekeeper or undermine end-user data protection or cyber security provided that such indispensable measures are duly justified by the gatekeeper.**	(f) allow business users and ~~providers of~~ **undertakings providing** ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services**. In these cases, access and interoperability conditions shall be fair, reasonable and non-discriminatory. The gatekeeper shall not degrade the conditions or quality of access and interoperability provided to business users or undertakings providing ancillary services. The gatekeeper shall not be prevented from taking to the extent strictly necessary and proportionate measures to ensure that third party ancillary services do not endanger the integrity of the operating system, hardware or software features provided by the gatekeeper, provided that such proportionate measures are duly justified by the gatekeeper;**

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

In contrast with the Council, Parliament extends the scope of the interoperability requirements within Article 6.1(f) to include access to core operating system features for 'providers of hardware', as well as broader access to non-operating system features for 'ancillary service providers'. In addition, both Parliament and the Council's amendments to Articles 6.1(c) and 6.1(f) recognise that certain limitations or exemptions to the interoperability requirements can be necessary to protect the integrity and security of platforms.

Finally, Parliament also adds two related articles, 6.1(f a) and 6.1(f b), imposing interconnectivity requirements on providers of a 'number independent interpersonal communication services' (messaging services) and 'social network services' (see Table 4.3).

Table 4.3 New articles 6.1(f a) and 6.1(f b)

Parliament's amendments
(f a) allow any providers of number independent interpersonal communication services upon their request and free of charge to interconnect with the gatekeepers number independent interpersonal communication services identified pursuant to Article 3(7). Interconnection shall be provided under objectively the same conditions and quality that are used by the gatekeeper, its subsidiaries or its partners, thus allowing for a functional interaction with these services, while guaranteeing a high level of security and personal data protection.
(f b) allow any providers of social network services upon their request and free of charge to interconnect with the gatekeepers social network services identified pursuant to Article 3(7). Interconnection shall be provided under objectively the same conditions and quality that are used by the gatekeeper, its subsidiaries or its partners, thus allowing for a functional interaction with these services, while guaranteeing a high level of security and personal data protection. The implementation of this obligation is subjected to the Commission's specification under Article 10 (2) b.

Note: New amendments marked in blue.

Source: Parliament's amendments.

Together, this suite of amendments requires gatekeepers to provide interoperability far more broadly, beyond just the features required for ancillary services. In effect, this imposes an open business model on all designated gatekeepers.

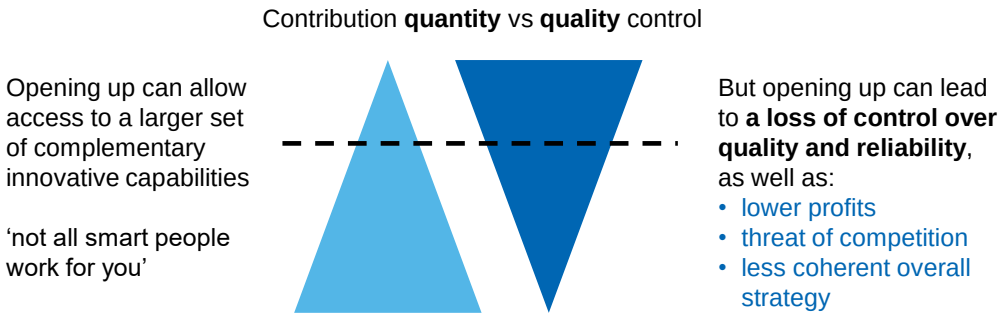
Section 4.1 explains how this mandated openness may introduce new governance risks by inhibiting the ability of gatekeepers to identify, assess and respond to the competing needs of different user groups, including both businesses and consumers.

In section 4.2, we consider whether the important exemptions that Parliament and the Council add to the Commission's original text go far enough. In particular, we highlight that platform governors must also protect quality of service if they are to maximise the value of ecosystems for all parties.

4.1 Mandated openness raises governance risks

Platforms have an inherent incentive to protect quality for users on all sides of the platform.[20] This requires a careful balance between access (to foster third-party innovation on the platform) and control (to protect the overall ecosystem and its users). Platforms adapt their level of openness to provide the most benefit to their users (see Figure 4.1 below).[21] However, the scope extensions proposed by Parliament and Council amendments will, in effect, force platforms to operate more open business models across a wider range of their core platform features and services. This will inherently reduce consumer choice by eliminating the possibility of selecting more-closed platform models. It will also raise governance risks in several ways, increasing the risk of a worsened consumer experience.

Figure 4.1 The open-platform/closed-platform trade-off



Source: Oxera.

First, the broad definition of interoperability that Parliament puts forward in its new Article 2(23b) precludes the use of 'application software or other technologies for conversion'. Instead, it demands a deep level of access for third parties, such that they may seamlessly 'exchange information and mutually use the information which has been exchanged'. This prescription of how designated gatekeepers should provide interoperability may grant more access to proprietary technology than is strictly required to promote contestability, raising questions of proportionality. Putting those concerns

[20] Evans, P. and Gawer, A. (2016), 'The Rise of the Platform Enterprise: A Global Survey', The Center for Global Enterprise Emerging Platform Economy Series, January.
[21] Evans, P. and Gawer, A. (2016), 'The Rise of the Platform Enterprise: A Global Survey', The Center for Global Enterprise Emerging Platform Economy Series, January; Oxera (2021), 'How platforms create value for their users: implications for the Digital Markets Act', prepared for CCIA, May.

aside, it also overlooks the complexities involved in granting access to third parties, including the careful consideration of what functionalities can be made available and the testing of that access to ensure security and reliability. Preventing the use of software or other technologies (such as programming libraries or APIs) would limit the ability of platforms to offer more closely managed services that balance access and control within their ecosystems.

Second, requiring that '[a] gatekeeper shall not degrade the conditions or quality of access and interoperability provided'—as per the Council's amendment to 6.1(f)—fails to acknowledge that while platforms will naturally internalise the effect of an action on other ecosystem participants, third parties do not have this incentive.[22]

Without appropriate governance by platform operators, excessive access to CPSs can result in third parties degrading user experiences and eroding consumer trust. In these circumstances, a tightening of access conditions (which might otherwise be perceived as a 'degradation of access') may be necessary to protect the security, integrity or quality of the entire ecosystem. This is especially important when consumers are unable to easily distinguish the quality of different products being offered over the platform. For example, Apple removed several parental control apps from the App Store and tightened its policies in response to a series of privacy and security risks posed by the underlying technology within these apps (see Box 4.1).

Box 4.1 Case study: Apple Mobile Device Management

Through Mobile Device Management (MDM) technologies, third parties can gain control of a user's devices and access sensitive information, such as location data, app usage and browsing histories. MDM serves a legitimate purpose in business environments, giving companies greater control over their proprietary data and hardware. However, in 2017, Apple began investigating the potential risks of app developers using MDM technology in the context of private, consumer-focused apps.

This investigation found that MDM could give app developers access to sensitive data that put user privacy at risk, while also making devices more vulnerable to hackers. In light of this, Apple updated its App Store guidelines in 2017 to better protect consumers and maintain the integrity of the App Store.

In April 2019, Apple discovered that a number of parental control apps were violating the revised App Store policies around the use of MDM. Having given the developers 30 days to update their apps, Apple removed the apps from the App Store. Apple later began offering 'Screen Time' APIs, enabling third parties to continue to build parental control tools without putting the privacy of children at risk. In doing so, Apple was able to protect the privacy of children while still fostering a competitive app market, providing access to appropriate data through managed APIs.

Source: Apple (2019), 'The facts about parental control apps', April; Perez, S. (2021), 'Apple finally launches a Screen Time API for app developers', TechCrunch, June.

A similar risk of externality effects is raised by the openness and interoperability obligations of Article 6.1(c)—particularly given the broad definition of interoperability proposed by Parliament. The distribution of apps through third-party app stores or direct downloads (sideloading) reduces a platform's ability to identify and manage security threats. This can have wide-

[22] Hagiu, A. (2015), 'Strategic decisions for multisided platforms', Top 10 Lessons on Strategy, *MIT Sloan Management Review*, summer, pp. 4–13.

reaching impacts, as malware introduced through an unsafe app can go on to affect other apps and users.[23]

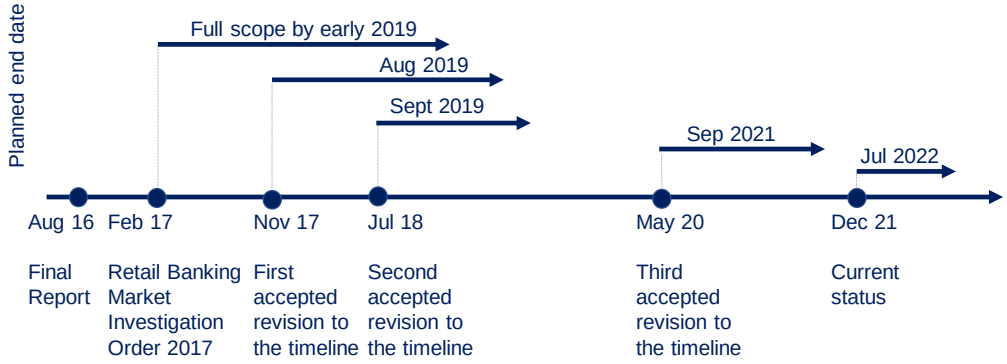
In addition, Parliament's new articles 6.1(f a) and 6.1(f b) mandate that platforms provide interconnectivity to third parties under 'objectively the same conditions and quality' as their own services. Not only will this reduce the ability of platforms to offer differentiated services, but also further hamper platforms' roles as ecosystem governors. For example, WhatsApp guarantees its users privacy by applying end-to-end encryption to all of its messages; however, it would not be able to guarantee this for messages arriving from or being delivered to third-party services.

Properly mitigating the increased governance risks caused by mandated open access would require both additional regulatory oversight—which is not provided for in the DMA—and a substantial investment of time and capital. For example, the UK's Open Banking initiative was introduced in 2017 to increase competition between the major high-street banks and third-party fintechs where access to sensitive financial data was necessary.[24] This required the implementation of a complex governance structure, with secure approval protocols around well-defined information types, to ensure the safety and control of the ecosystem for its users.[25] Moreover, significant costs and numerous regulatory frameworks are needed to make Open Banking functional.[26] It should be noted that the amendments to the DMA require deeper interoperability than simply the sharing of data, and so should be expected to require more complex governance to manage this properly and safely.

However, none of the amendments to the DMA texts account for this necessary oversight. At the same time, Article 39.2 would mean that these interoperability obligations need to be implemented within six months of the regulation coming into force. This is a very short period of time given the case-specific complexity involved with generalising third-party access—as highlighted by the Open Banking example.[27] Despite the fact that the underlying data and services were more standardised in Open Banking, the implementation of those, more limited, interoperability requirements is ongoing five years after the Competition and Markets Authority (CMA) imposed the remedy. The end date for the implementation of Open Banking was initially set for Q1 2019; however, as can be seen in Figure 4.2, this timeline was revised multiple times to address various issues such as inability to deliver, gaps in available functionality, and API performance.

[23] Apple (2021), 'Building a Trusted Ecosystem for Millions of Apps: a threat analysis of sideloading', October.
[24] For more information on the scheme, see the Open Banking homepage.
[25] For more details see the 'Secure by design' information on the Open banking website.
[26] For example, Revised Payment Service Directive (PSD2), The Payment Services Regulations 2017 (PSRs), Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication (RTS-SCA), UK regulatory technical standards for strong customer authentication and secure communication (UK-RTS), Electronic Money Regulations 2011, FCA Approach to final Regulatory Technical Standards, the European Banking Authority opinion on regulatory technical standards implementation on SCA and CSC, EBA report on conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC). See the regulatory section on the Open Banking webpage.
[27] The Centre on Regulation in Europe also recommends that access obligations be specified on a case-by-case basis. See de Streel, A., Feasey, R., Krämer, J. and Monti, G. (2021), 'Making the Digital Markets Act more resilient and effective: recommendations paper', May, section 2.3.3.

Figure 4.2 Open banking implementation timeline



Source: Oxera, based on CMA (2021), 'Retail banking market investigation: Timetable'.

4.2 Access limitations help to protect platform ecosystems

Both the Parliament and Council amendments to Articles 6.1(c) and 6.1(f) introduce valuable limitations to the interoperability obligations. While the wording differs slightly, they both allow platforms to take measures to protect *'the integrity of the operating system, hardware or software features'* that they provide. Notably, Parliament's amendments also allow exemptions on the grounds of end-user data protection or cyber security.[28]

These additional exemptions address an important gap in the initial DMA proposal. The ability to take measures to protect users and the ecosystem begins to restore the ability of platforms to play the governance role discussed in section 4.1. Moreover, these protective measures help the DMA to better align with other legislation—such as the Commission's proposed Digital Services Act (DSA)—that calls on platforms to play a more active role in the safety of users online and the protection of fundamental rights, such data security and privacy.[29]

There is a further subtle but important difference to the approaches proposed by Parliament and Council with respect to Article 6.1(c). Parliament's text would allow *platforms* to take necessary and proportionate actions to prevent third parties from undermining end-user data protection or cyber security. However the Council's text would only allow platforms to enable *end-users* to protect *their own* security. Given that end users are frequently identified as the weak link in digital security, the proactive approach offered by the Parliament may be more appropriate to guarantee security of *all users*.[30]

However, the narrow scope of application for these exemptions fails to recognise that effective platform governance goes beyond just 'hardcore' security and integrity threats. To maintain value for all users, platforms must also promote confidence and trust in their ecosystems. To do this, they must retain a 'bouncer's right' to exclude third parties that compromise the quality of the platform—irrespective of whether that is by compromising the *'integrity of the operating system, hardware or software features'* or through less critical means. For example, the problematic actions of third-party videogame developers in the 1980s were enabled by their wide access to console

[28] Similar exemptions are also included in Parliament's amendments to Article 6.1(f a), 6.1(f b) and 5(c a).
[29] European Commission (2020), 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC', 15 December.
[30] In 2020, almost a third of cybersecurity breaches incorporated social engineering techniques that involve manipulating human psychology for criminal goals. See Gurinaviciute, J. (2021), '5 biggest cybersecurity threats', Security Magazine, February.

technology and ecosystems. This prompted console providers to rebalance the degree of interoperability granted to software developers on their platforms, enabling them to better protect the quality of the consumer experience and integrity of the overall ecosystem (see Box 4.2).

Box 4.2 Case study: promoting trust and quality in game consoles

The 'Atari shock' was a severe crisis within the videogame industry in the early 1980s. Atari popularised video games in the 1970s, but later faced a rapid increase in the number of independent game developers that did not need authorisation from the console providers to bring games to market. Low entry barriers for these developers lead to the market being saturated with games of substandard quality, and since consumers could not distinguish between the quality of the games before purchasing them, the games market became a 'market for lemons'. This resulted in decreased consumer confidence and a rapid decline in the entire console market.

Following the launch of its first console in 1983 (in Japan at first, and the USA in 1985), Nintendo sought to combat these market conditions by enforcing a certain degree of quality control—imposing restrictions on the number of games that developers could publish each year. Furthermore, Nintendo required games to be verified and approved before release in order to keep quality high and boost consumer trust in its ecosystem.

By introducing its 'Seal of Quality', Nintendo provided incentives to developers to release better-designed, high-quality games that were less prone to bugs. This approach to quality control renewed consumer confidence in the console market and protected the experiences of gamers. Such practices continue to the present day, with online stores such as Steam, the Nintendo eShop, and the PlayStation Store reviewing developers' games before publishing them online, and both the Google Play Store and the Apple App Store featuring a review process that app developers need to follow before publishing and distributing their apps to end-users.

Source: Ernkvist, M. (2008), 'Down Many Times, But Still Playing the Game: Creative Destruction and Industry Crashes in the Early Video Game Industry 1971-1986', *History of Insolvency and Bankruptcy*, January; Ward, C. (2019), 'Science Behind the Fiction: How Nintendo Saved and Redefined the Game Industry', *SyFyWire*, 5 June; Cennamo, C. and Santaló, J. (2015), 'How to Avoid Platform Traps', *MIT Sloan Management Review*, **57**, pp. 12–15; McFerran, D. (2019), 'Talking Point: What Does The Nintendo Seal Of Quality Mean In 2019?', *Nintendolife*, 6 February; Boudreau, K.J. and Hagiu, A. (2008), 'Platform Rules: Multi-Sided Platforms as Regulators' in Gawer, A., *Platforms, markets and innovation*, Edward Elgar Publishing, pp. 163–91; Nintendo (2021), 'The process'; Steam (2021), 'Joining The Steamworks Distribution Program'; PlayStation (2021), 'PlayStation for Partners'; Apple (2021), 'Building a trusted ecosystem for millions of apps', June.

Finally, Parliament implicitly acknowledges the complexity around interconnection conditions for social network services in its new Article 6.1(f b), where it states:

> […] The implementation of this obligation is subjected to the Commission's specification under Article 10 (2) b.

In turn, Article 10 (2) b of the DMA specifies that:

> A practice […] shall be considered to be unfair or limit the contestability of core platform services where:
>
> (a) […]
>
> (b) the contestability of markets is weakened as a consequence of such a practice engaged in by gatekeepers.

That is to say, before implementing the obligations for a social media service, the Commission should confirm that **'**the contestability of markets is weakened' by a lack of interconnectivity. This approach would ensure a closer examination of the context in which the obligation would be imposed, reducing the risk of inappropriate interventions, as set out in sections 4.1 and 4.2.

As such, the DMA would benefit from adopting this effects-based approach more widely throughout the obligations defined in articles 5 and 6.

5 Business model choice

The DMA impact assessment found that users will be unaffected by changes in platforms' business models, in part because:[31]

> […] the foreseen interventions will neither ban specific monetisation models (such as ad-based models) nor prevent the uptake of new services by gatekeepers […]

However, we find that a number of the amendments now proposed by Parliament and the Council are at odds with this assessment—particularly when applied in combination across all gatekeeper platforms.

In section 5.1, we explain how Parliament's amendments to recital 49 would undermine cross-subsidies and ad-funded business models, leading to higher prices and lower-quality services for consumers. We also consider the impact on ad-funded business models and the uptake of new features and services by platform operators.

In section 5.2, we examine how Parliament's requirement in Articles 6.1(f), 6.1(f a) and 6.1(f b) to provide access and interoperability free of charge would undermine licensing business models whereby a platform might charge access seekers for access to its CPS. In contrast, the Council stipulates that interoperability conditions should be offered on a '*fair, reasonable and non-discriminatory*' (FRAND) basis, which would help to protect investment incentives for platforms.

In section 5.3, we consider the impact of the obligations in Article 5(c) and Article 5(e) on commission-based business models, particularly in light of the amendments proposed by the Council.

In section 5.4, we consider the combined effect of these obligations on the choice of business models available to platform operators, highlighting how they can lead to higher prices, reduced digital inclusiveness and less innovative products.

5.1 Undermining cross-subsidisation and ad-funding

In addition to the amendments to Article 6.1(d) discussed in section 3, Parliament also proposes changes to the recital on self-preferencing (recital 49) that would require designated gatekeepers to treat each of their products and services as separate commercial entities (see Table 5.1).

[31] See European Commission (2020), 'Executive summary of the impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector', staff working document, 15 December, Annex 3: Who is affected and how?, p. 48.

Table 5.1 Amendments to recital 49

Parliament's amendments

In such situations, the gatekeeper should not engage in any form of differentiated or preferential treatment in ranking on the core platform service, whether through legal, commercial or technical means, in favour of products or services it offers itself or through a business user which it controls. To ensure that this obligation is effective, it should also be ensured that the conditions that apply to such ranking are also generally fair. Ranking should in this context cover all forms of relative prominence, including display, rating, linking or voice results. To ensure that this obligation is effective and cannot be circumvented it should also apply to any measure that may have an equivalent effect to the differentiated or preferential treatment in ranking. **In addition, to avoid any conflicts of interest, gatekeepers should be required to treat its own product or services, as a separate commercial entity that is commercially viable as a stand-alone service.** The guidelines adopted pursuant to Article 5 of Regulation (EU) 2019/1150 should also facilitate the implementation and enforcement of this obligation

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments.

In particular, Parliament stipulates that each individual service should be *'commercially viable as a stand-alone service'*, effectively calling for the functional separation of the different services offered by a gatekeeper—with substantial consequences for the types of business models that these platforms can adopt. This stands in stark contrast to both the Commission and Council texts, which enforce the unbiased treatment of third parties by platform intermediaries without demanding the structural separation of gatekeepers.

Requiring services be commercially viable on a standalone basis also represents a de facto ban on the cross-subsidisation of ancillary services. Many platforms bundle non-revenue generating services (such as news aggregation, email services, or online calendars) alongside revenue-generating services as a means of maximising ecosystem value. Prohibiting this cross-subsidisation could lead to increased prices for consumers, which in turn could have a negative impact on digital inclusion.

For example, through the Mobile Application Distribution Agreement, Google offered original equipment manufacturers (OEMs) the Android OS for free, along with a selection of apps such as Play Store, Google Search, and Gmail.[32] This was made possible as Google cross-subsidised the cost of developing and maintaining these apps from the revenues generated by its Search and Play Store services. Google's dual role as a platform operator and app provider allowed it to unlock the benefits that these free apps and services would generate for the wider Android ecosystem.[33]

For OEMs, the free Android OS enables them to avoid the cost of purchasing or developing an operating system. For consumers, this means lower-priced smartphones running an extensive, well-maintained mobile OS with access to a wide range of apps. However, requiring the Android OS to be viable on a standalone basis would require a new business model, likely involving a fee for OEMs. This would reduce the availability of high-quality, low-priced phones, with a particular effect on lower-income consumers. A 2018 Oxera

[32] In addition, OEMs have the option to receive additional remuneration if Google Search and Chrome are set as non-exclusive defaults.
[33] Following the European Commission decision in the Android Case, Google made changes to how it licenses its proprietary apps. However, it is still providing the Android OS for free. See Google Blog (2018), 'Complying with the EC's Android decision', 16 October.

study estimated that 21m (18%) more mobile devices were sold in Europe in 2017 as a result of the price advantage offered by the free Android OS.[34]

Furthermore, cross-subsidising organic content and features with ad-funded services is a core feature of many online platforms. The academic literature explains how this can be an efficient way to finance services that orchestrate a large number of low-value interactions, which would be dwarfed by transaction costs if contracted on an individual basis.[35] In many cases, platforms harness this value through data-driven advertising services, which they then use to cross-subsidise their consumer services. Requiring services that are normally funded by advertising to become standalone services would undo the benefits of this cross-subsidy arrangement.

For example, in the case of search, the value to consumers of any individual query is generally small, making it difficult to charge for this on a transactional basis.[36] At the same time, the accumulated value of many queries by many users adds up to a considerable social benefit. As such, it is more practical and efficient to offer search services to consumers for free, with the high fixed costs of providing them being paid for by charging advertisers for sponsored results.

Similarly, there are beneficial spill-overs from network effects when a social media platform has more users, as this means a greater diversity of content shared and more connections being available. While it may be possible to change the funding model to a subscription or 'freemium' service (for example, Microsoft's LinkedIn is supplied through a mixture of ad-funding and some subscribers paying more for additional access), this could have negative consequences for digital inclusion if, for example, poorer consumers were unable to pay the subscription costs. Given the inherent network effects of social media, this would also reduce the value for all remaining users.

Moreover, ad-funded business models can help to facilitate investments by platform operators in the quality of their ecosystems. These platforms are incentivised to maintain user engagement by continually improving and updating their services to remain relevant.[37] New services or functionalities can be cross-subsidised with ad revenues, meaning that users across the ecosystem benefit from better products and services without being charged. However, Parliament's requirement to treat all services as standalone products could inhibit these innovation incentives. Platforms introducing incremental changes could face uncertainty around whether these changes count as improvements to the core platform service, or whether they are new services that must be assessed in isolation.

For example, throughout its development, Facebook's ad-funded business model has cross-subsidised the introduction of new functionality on the consumer side (see Box 5.1). Although none of Facebook's features began as separate products, Parliament's amendment raises the risk that authorities (or courts) might consider them to be separate entities, and then require them to be commercially viable on a standalone basis. This kind of uncertainty could cause platforms to be more cautious about introducing experimental services

[34] Oxera (2018), 'Android in Europe: Benefits to consumers and business', prepared for Google, October, section 2.5.
[35] Anderson, C. (2008), *The Long Tail: The Revised and Updated Edition: Why the Future of Business is Selling Less of More*, New York: Hyperion.
[37] Zhou, Z., Zhang, L. and Van Alstyne, M. (2020), 'How Users Drive Value: Platform Investments that Matter',12 June.

and features around their CPSs, meaning less innovation and reduced quality for users.

Box 5.1 Case study: Facebook's evolution

What began as a photo directory for Harvard students in 2004 has grown into a global social network platform, bringing together close to 2bn users daily. Over the course of its development, Facebook has added an increasing array of features and services, increasing convenience for users and promoting social interactions. Its current offering includes the News Feed, Photos, Messenger, Events, Groups, Watch, Jobs, Dating, and Marketplace.

Facebook combined features to enhance and enrich its overall ecosystem by adapting to changing consumer tastes over time. For example, it first introduced dedicated Buy-and-Sell Groups—and, later, Facebook Marketplace and Facebook Shops—when it noticed that users were increasingly using standard groups to exchange second-hand goods.

By integrating new features, Facebook takes full advantage of its inherent network effects to serve the needs of a wide number of consumers better than if its features were provided separately. For example, messaging features are more valuable to consumers as part of a bundled social media offering than as a standalone product, because this bundle builds upon a pre-existing network of friends; this means that users can reach someone without the need for additional contact details.

The cross-subsidisation of consumer-facing innovations with advertising revenue is behind Facebook's ability to provide this wide variety of functionalities and services. The quality of the experience that it offers to users cannot be understood in isolation.

Sources: Oxera (2021), 'How platforms create value for their users: implications for the Digital Markets Act', prepared for the Computer and Communications Industry Association, section 3.3, May; Facebook (2016), 'Introducing Marketplace: Buy and Sell With Your Local Community', October; Facebook (2018), 'Marketplace Turns Two: Introducing New AI Features and More', October; Statista (2021), 'Number of daily active Facebook users worldwide as of 3rd quarter 2021', October.

5.2 Free access undermines a licensing business model

As set out in Table 4.2, Parliament's amendments to Article 6.1(f), 6.1(f a) and 6.1(f b) would require designated gatekeepers to provide access and interoperability, as well as interconnectivity, 'free of charge'. The ability to charge third parties for the use of a platform can be a significant revenue stream for some operators, and therefore an important means of recovering their investments.[38] As such, if platforms are unable to charge access seekers for use of their core features, there will be lower incentives to develop them in the first place, while restrictions on charging business users may lead to the introduction of pricing on the consumer side.

This is likely to have an adverse effect on platform incentives, which would be detrimental to the overall consumer experience in the long run. Importantly, the Commission's DMA impact assessment assumed that gatekeeper innovation incentives would remain largely unchanged.[39] This assumption is unlikely to be borne out if platforms must offer interoperability free of charge, meaning the gains to third parties have not been properly weighed against the costs to consumers of lost innovation and investment by gatekeepers.[40]

[38] Tiwana, A. (2013), *Platform ecosystems: Aligning Architecture, Governance and Strategy*, Elsevier; Parker, G., Van Alstyne, M. and Choudary, S. (2016), *Platform Revolution*, W.W. Norton & Company.
[39] See European Commission (2020), 'Impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector', Part 1/2, para 303 and Part 2/2, pp. 46–48.
[40] See European Commission (2020), 'Executive summary of the impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector', staff working document, 15 December.

First, mandating access to platform features free of charge could reduce innovation incentives for platforms that have already been designated as gatekeepers, or weaken their incentives to maintain their platform infrastructure. For example, a platform may spot an opportunity to provide an innovative ancillary service on its platform, with the service enabled by some alteration or change to the CPS. However, the platform might be hesitant to make this change if it was forced to provide free of charge access to the new feature, hindering its ability to recover development costs. As the leading platform operators have historically spent large amounts on technology R&D—for example, Amazon spending $42.74bn in 2020, Alphabet $27.57bn, Microsoft $19.27bn, Apple $18.75bn, Facebook $18.45bn, and Oracle $6.07bn—this could have a substantial chilling effect on innovation.[41]

Second, limiting how platforms can share in the value they create will reduce incentives to develop new services that might end up designated as a CPS. Innovators must be permitted to capture some of the value of their innovation if they are to have any incentive to incur the high upfront costs required to develop them in the first place, with the rewards needing to cover the cost of their overall portfolio of innovations—including those that are unsuccessful.

Parliament's amendment would mean that a share of the value that a designated gatekeeper creates from its investments could be expropriated by its rivals, while reducing the gatekeeper's ability to monetise those investments. In contrast, the Council's amendments require that access and interoperability be granted on FRAND terms. This approach better preserves the incentives of gatekeepers to invest and innovate, while still ensuring contestability and fairness for business users. This is, in effect, the same trade-off between static and dynamic efficiency that is encapsulated in intellectual property protection (i.e. patents). However, it does still introduce a degree of legal uncertainty for both firms and authorities, as there is no ex ante understanding of what a FRAND price should be, let alone what FRAND access conditions would be for the diversity of CPSs to which this obligation will apply.

Moreover, platforms are also enablers of innovation by providing opportunities for third parties to *innovate on* the platform. Changes to the platforms' incentives can have a negative downstream effect. For example, if a platform reduces the number of features it develops (e.g. mapping functionalities, design APIs, general purpose AI or coding libraries) or the speed of their roll-out, this affects the products and services offered by third parties when they take these functionalities and build on them.

5.3 Restrictions on commission-based models

While both Parliament and the Council have proposed a number of clarifying amendments to Article 5(c) (including splitting the Article into two sub-parts), the effect of the obligation remains the same, which is to enable business users to steer users off-platform to complete transactions (see Table 5.2).

[41] Nasdaq (2021), 'Which Companies Spend the Most in Research and Development (R&D)?', June; Microsoft (2020), 'Annual Report'; Oracle (2020), 'Form 10-K: Annual report'.

Table 5.2 Amendments to Article 5(c)

Parliament's amendments	Council General Approach
(c) allow business users to ***communicate and*** promote offers ***including under different purchasing conditions*** to end users acquired via the core platform service ***or through other channels***, and to conclude contracts with these end users ***or receive payments for services provided*** regardless of whether ***they use*** for that purpose ~~they use~~ the core platform services of the gatekeeper ~~or not, and allow end users to access and use, through the core platform services of the gatekeeper, content, subscriptions, features or other items by using the software application of a business user, where these items have been acquired by the end users from the relevant business user without using the core platform services of the gatekeeper;~~	(c) allow business users to communicate and promote offers including under different conditions to end users acquired via the core platform service or through other channels, and to conclude contracts with these end users regardless of whether for that purpose they use the core platform services of the gatekeeper or not~~, and allow end users to access and use, through the core platform services of the gatekeeper, content, subscriptions, features or other items by using the software application of a business user, where these items have been acquired by the end users from the relevant business user without using the core platform services of the gatekeeper;~~
(ca) allow end users to access and use, through the core platform services of the gatekeeper, content, subscriptions, features or other items by using the software application of a business user, even where these items have been acquired by the end users from the relevant business user without using the core platform services of the gatekeeper, unless the gatekeeper can demonstrate that such access undermines end users data protection or cybersecurity.	**(ca) allow end users to access and use, through the core platform services of the gatekeeper, content, subscriptions, features or other items by using the software application of a business user, where these items have been acquired by the end users from the relevant business user without using the core platform services of the gatekeeper;**

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

At the same time, Parliament's amendments to Article 5(e) would also prevent platforms requiring third parties to use their ancillary services (including payment services) as a means of charging a value-based commission.

Table 5.3 Amendments to Article 5(e)

Parliament's amendments	Council General Approach
(e) refrain from requiring business users to use, offer or interoperate with an identification service ***or any other ancillary service*** of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;	(e) refrain from requiring business users **or end users** to use, **and in the case of business users, also to** offer or interoperate with, an identification **or payment** service of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;

Note: Amendments as compared with the Commission's proposals marked in blue.

Source: Parliament's amendments and Council General Approach.

Taken together, Articles 5(c) and 5(e)—as amended—would limit the extent to which platforms can rely on commission-based business models. The impact of this for online travel agents (OTAs) is discussed in section 5.1 of our previous report.[42] We explain that if hotels and transport providers can circumvent the OTA at the time of booking (e.g. by offering discounts for booking direct) it will undermine the platform's revenue stream.

The same logic can extend to any commission-based sales model, such as app stores, marketplaces, or recommendation services. This introduces the

[42] Oxera (2021), 'How platforms create value for their users: implications for the Digital Markets Act', prepared for the Computer and Communications Industry Association, May, section 5.1.

risk of free-riding by a platforms' business users, who can benefit from the scale and promotion offered by the platform without contributing to the costs.

5.4 Combined effect of the obligations

Each of the obligations discussed above is designed to address contestability concerns within one type of business model. However, applying these as a one-size-fits-all solution to every gatekeeper platform has the unintended consequence of significantly restricting their choice of business model.

This has the potential to be detrimental to consumers, as it may lead to higher prices and lower digital inclusiveness. For example, with limitations on cross-subsidies, ad-funding, licensing and commission-based business models, platforms may be pushed towards introducing listing fees for businesses, membership fees for end-users, or some combination of the two. This would be necessary in order to cover the development costs that are no longer recoverable via existing business models.

Such a change in business model also has the potential to affect the balance of risk and the type of business users that are attracted to particular platforms, which could mean less innovative products being made available on platforms. For example, if businesses need to incur the costs of listing new products and services on a platform (such as apps on an app store) before knowing how successful their product will be, the added risk will discourage some businesses from entering the market. This would particularly affect those with novel ideas that are as yet untested in the market.

The combined effect of these obligations can also create a regulatory 'cliff-edge' for growing digital platforms. For example, an online travel agency or other online marketplace that grows quickly with a commission-based business model would see its core revenue stream put at risk if it grows large enough to be designated as a gatekeeper. This is likely to limit the appetite for growth and investment past a certain point, and may also have negative consequences for businesses or consumers if they are 'delisted' in order to keep the platform under the threshold levels.

This would be further compounded by Parliament's amendment to recital 14a that stipulates '*ancillary services should also be subject to the obligations applicable to core platform services*'. With this change, the DMA would further reduce gatekeepers' choices of how to deliver services and products to users and increase the incentives to keep all platform services below 'gatekeeper' scale.

Overall, this illustrates the critical need to step back and consider the impact of the proposed regulations as a whole—rather than focusing on each obligation in isolation—if policymakers are to avoid inadvertently amplifying the scope and scale of any unintended consequences for end-users.

6 Conclusion

In this report, we have reviewed the amendments proposed to selected articles and recitals by Parliament and the Council relating to issues of: (i) data separation; (ii) product and services integration; (iii) interoperability and interconnection; and (iv) business model choice. Throughout, we have focused on the unintended consequences that these provisions could have for consumers.

6.1 Summary of our conclusions

In some cases, we found that the amendments introduce a better balance to the obligations proposed by the Commission, which we anticipate would have a positive impact on consumers. In particular:

- the Council's amendments to Article 5(a) would better align with GDPR and add important exemptions to the user consent requirements, allowing platforms to better protect the security and integrity of their ecosystems;
- both Parliament and the Council proposed amendments to Articles 6.1(c) and 6.1(f) to allow gatekeepers to take proportionate measures to protect the integrity and security of their OS, hardware or software features;
- moreover, Parliament's additional provisions in Articles 5(c), 6.1(c) and 6.1(f) allow gatekeepers to better protect end-user data and cyber security, further enabling platforms to manage risks for their users.

In other cases, the amendments make clarifications to the Commission's DMA text to help both platforms and authorities to better understand its expectations and requirements. However, we also identified a number of amendments that risk worsened outcomes for consumers over the long term.

- Parliament's amendments to recital 46 make an unrealistic demand of platforms by requiring that the 'less personalised' alternative be of the same quality as the personalised service, resulting in *all* users receiving the 'less personalised alternative'.
- Parliament's amendments to the scope of Article 6.1(d) and restriction on product integrations in recital 48 would hamper product improvement and reliability while worsening the 'out-of-the-box' experience for users.
- Parliament's extension to the scope of Article 6.1(c) and Article 6.1(f)—to include access to more platform functions for third parties—would raise governance risks that degrade the overall consumer experience.
- Parliament's amendments to recital 49 (requiring all gatekeeper services to be commercially viable on a standalone basis) and Article 6.1(f) (requiring free of charge interoperability) together with the obligations in Articles 5(c) and 5(e) impose business model restrictions that do not leave many alternatives for monetisation. As these changes undermine ad-funded, licensing, and commission-based business models, the alternatives include listing fees and end-user charges that will lead to higher prices, reduced digital inclusiveness, and fewer new features and functionalities for users.

Throughout the Commission's proposed DMA, there is an implicit assumption that consumer interest will automatically be advanced by improving fairness and contestability for business users. For example, Article 10.2(a) describes unfairness and limitations to contestability while only referencing businesses,

and without mentioning impacts on consumers.[43] However, this short-run focus could inhibit dynamic competition in the long run.[44] To address this tension between outcomes for business users and outcomes for consumers, we outline a number of recommendations for the final DMA text.

6.2 Recommendations

Well-designed regulation should first identify the market failure that it is trying to fix, and then test whether the proposed intervention is likely to produce better or worse outcomes. This is particularly important when the practices being regulated could lead to positive consumer outcomes as well as negative ones.

In our previous report, we discussed how the DMA's current 'catch-all' and 'per se' approach to prohibiting value-creating behaviours risks stifling the growth of Europe's digital economy and ultimately harming consumers.[45] Throughout the trilogue process, we recommend adopting the most flexible language possible, leaving room for the most holistic assessment of market features and tailoring of interventions when enforcing the DMA's obligations.

Building on the recommendation of our previous report, we propose the following key principles.

- Allow gatekeepers to adopt clear safeguards beyond just 'hardcore' security measures. Platforms should also be able to take action to preserve the quality and integrity of their ecosystem, and to protect end-user data.
- Allow gatekeepers the option of integrating their complementary services in order to provide a holistic 'out-of-the-box' experience.
- Avoid a catch-all approach to access, interoperability and integration obligations, instead targeting interventions at the specific data and functionalities required for contestability and fairness.
- Ensure the obligations preserve investment and innovation incentives for platforms by allowing them to share in the value they create. In particular, avoid mandating 'free of charge' access or interoperability where the benefit to end-users depends on active participation and ongoing investment by the platform operator.
- Adopt longer timelines for the implementation of access and interoperability obligations (as well as similar obligations related to the portability of data) in order to minimise governance risks. The proposed interventions should be carefully tested before being widely implemented and remain open to change in the event of unintended consequences for users.
- Avoid applying 'one-size-fits-all' obligations to all platforms. While each obligation may promote contestability in certain circumstances, taking them together and applying them to all platforms can effectively prohibit certain platform business models.

[43] DMA Article 10.2(a) reads: 'A practice […] shall be considered to be unfair or limit the contestability of core platform services where: (a) there is an imbalance of rights and obligations on business users and the gatekeeper is obtaining an advantage from business users that is disproportionate to the service provided by the gatekeeper to business users;'.
[44] Also acknowledged by an Parliament report commissioned from Dr Jules Stuyck: Stuyk, J. (2011), 'Briefing Paper addressing unfair commercial practices in business-to-business relations in the internal market'—which states that 'A too generous application of the fairness test in unfair competition law inhibits dynamic competition', p. 16.
[45] Oxera (2021), 'How platforms create value for their users: implications for the Digital Markets Act', prepared for the Computer and Communications Industry Association, May, section 5.

The trilogue will be most successful if it properly recognises that some obligations must be tailored to a platform's specific circumstances. It must also consider the effect of those obligations in the economic context in which they will be applied. This will help to avoid inadvertently banning behaviours that benefit consumers and business users. In addition, amendments that increase the possibility for regulatory dialogue will help reduce legal uncertainty and minimise the risk of costly and time-consuming litigation in the future.

www.oxera.com

oxera
compelling economics