

cerre

Centre on Regulation in Europe

ISSUE PAPER

May 2021


Alexandre de Stree

Richard Feasey

Jan Krämer

Giorgio Monti

**OBLIGATIONS AND
PROHIBITIONS**



As provided for in CERRE's by-laws and the procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which these Issue Papers have been prepared, has received the support and/or input of the following organisations: AGCOM, Apple, ARCEP, BIPT, Booking.Com, COMREG, Deutsche Telekom, Mediaset, Microsoft, OFCOM, Qualcomm, Spotify, and Vodafone. These organisations bear no responsibility for the contents of these Issue Papers.

The Issue Papers were prepared by a team of academics coordinated by CERRE Academic Co-Director, Alexandre de Streel, and including Richard Feasey, Jan Krämer and Giorgio Monti. The academic team also benefited greatly from very useful comments by Amelia Fletcher. The proposals contained in these Issue Papers were intended to promote debate between participants at the four private seminars organised by CERRE between March and April 2021. The views expressed in these Issue Papers are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or to any sponsor or members of CERRE.

© Copyright 2021, Centre on Regulation in Europe (CERRE)

info@cerre.eu

www.cerre.eu

Table of contents

About CERRE	4
About the authors	5
1 Introduction	7
2 The objectives of the obligations	7
2.1 The role of the DMA objectives.....	7
2.2 The DMA objectives of contestability and fairness.....	8
2.3 Recommendations	14
3 The scope of the obligations	15
3.1 The Commission’s proposal.....	15
3.2 Recommendations	17
4 The expected effectiveness of the obligations	18
4.1 Expected effectiveness and practical issues arising	18
4.2 Recommendations	21
5 Risks of unintended harm	22
Annex: Assessment of individual obligations	24

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the academic qualifications and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, the specification of market rules and the improvement of infrastructure management in a rapidly changing social, political, economic and technological environment. The work of CERRE also aims to refine the respective roles of market operators, governments and regulatory bodies, as well as aiming to improve the expertise of the latter, given that - in many Member States - the regulators are relatively new to the role.

About the authors



Alexandre de Stree is Academic Co-Director at CERRE and a professor of European law at the University of Namur and the Research Centre for Information, Law and Society (CRIDS/NADI). He is a Hauser Global Fellow at New York University (NYU) Law School and visiting professor at the European University Institute, SciencesPo Paris and Barcelona Graduate School of Economics, and also assessor at the Belgian Competition Authority. His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence. Recently, he advised the European Commission and the European Parliament on the regulation of online platforms. Previously, Alexandre worked for the Belgian Deputy Prime Minister, the Belgian Permanent Representation to the European Union and the European Commission (DG CNECT). He holds a Ph.D. in Law from the European University Institute and a Master's Degree in Economics from the University of Louvain.



Richard Feasey is a CERRE Senior Adviser, an Inquiry Chair at the UK's Competition and Markets Authority and Member of the National Infrastructure Commission for Wales. He lectures at University College and Kings College London and the Judge Business School. He has previously been an adviser to the UK Payments Systems Regulator, the House of Lords EU Sub-Committee and to various international legal and economic advisory firms. He was Director of Public Policy for Vodafone plc between 2001 and 2013.



Jan Krämer is an Academic Co-Director at CERRE and a Professor at the University of Passau, Germany, where he holds the chair of Internet & Telecommunications Business. Previously, he headed a research group on telecommunications markets at the Karlsruhe Institute of Technology (KIT), where he also obtained a diploma degree in Business and Economics Engineering with a focus on computer science, telematics and operations research, and a Ph.D. in Economics, both with distinction. He is editor and author of several interdisciplinary books on the regulation of telecommunications markets and has published numerous articles in the premier scholarly journals in Information Systems, Economics, Management and Marketing research on issues such as net neutrality, data and platform economy, and the design of electronic markets. Professor Krämer has served as academic consultant for leading firms in the telecommunications and Internet industry, as well as for governmental institutions, such as the German Federal Ministry for Economic Affairs and the European Commission. His current research focuses on the role of data for competition and innovation in online markets and the regulation of online platforms.



Giorgio Monti is Professor of Competition Law at Tilburg Law School. He began his career in the UK (Leicester 1993-2001 and London School of Economics (2001-2010) before taking up the Chair in competition law at the European University Institute in Florence, Italy (2010-2019). While at the EUI he helped establish the Florence Competition Program which carries out research and training for judges and executives. He also served as Head of the Law Department at the EUI. His principal field of research is competition law, a subject he enjoys tackling from an economic and a policy perspective. Together with Damian Chalmers and Gareth Davies he is a co-author of *European Union Law: Text and Materials* (4th ed, Cambridge University Press, 2019), one of the major texts on the subject. He is one of the editors of the *Common Market Law Review*.

1 Introduction

This paper considers in more detail the eighteen proposed obligations and prohibitions in the DMA proposal.

The paper is in five sections: after this introduction, section 2 deals with the objectives of the obligations, why this is important and what each obligation is expected to do for fairness and contestability; section 3 examines the expected scope of each obligation in terms of the Core Platform Services to which it is expected to apply; section 4 examines the expected effectiveness of these obligations, as they currently stand, including key barriers to effectiveness, and areas where there is likely to be a need for further specification; and section 5 examines the risk of unintended harm arising from the obligations.

2 The objectives of the obligations

2.1 The role of the DMA objectives

The general objective of the DMA is set out at Recital 79:

*The objective of this Regulation is to ensure a **contestable** and **fair** digital sector in general and core platform services in particular, with a view to promoting innovation, high quality of digital products and services, fair and competitive prices, as well as a high quality and choice for end users in the digital sector. [emphasis added]*

Thus, the two principal DMA objectives are **contestability** and **fairness**, but these are in turn intended to create good incentives for innovation, high quality and choice, and fair and competitive prices. Between them, the two principal objectives are supposed to underpin all current and future obligations:

- **For existing obligations**, Article 7 states clearly that:

*The measures implemented by the gatekeeper to ensure compliance with the obligations laid down in Articles 5 and 6 shall be **effective in achieving the objective of the relevant obligation**; while*

- **For new obligations**, Article 10 states that:

*The Commission is empowered to adopt delegated acts [...] to update the obligations laid down in Articles 5 and 6 where [...]it has identified the need for new obligations addressing practices that limit the **contestability** of core platform services or are **unfair** in the same way as the practices addressed by the obligations laid down in Articles 5 and 6. [Emphasis added].*

In addition, any implementation of the DMA would be subject to the requirements on proportionality under the EU Treaties, and this too is closely linked to the stated objectives. The DMA recitals (para 33) highlight that:

The obligations laid down in this Regulation are limited to what is necessary and justified to address the unfairness of the identified practices by gatekeepers and to ensure contestability in relation to core platform services provided by gatekeepers.

Article 5 of the Treaty on the European Union (TEU) itself states that:

'the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties'.

In practice, the case-law on proportionality under TEU suggests that assessment involves four elements: (1) an appropriate (or suitable) measure; (2) in pursuit of a legitimate objective; (3)

among the appropriate measures that measure which constitutes the least restrictive measure; and (4) not manifestly disproportionate in terms of costs versus benefits balance.

2.2 The DMA objectives of contestability and fairness

Given this framework, it seems vital that the meanings of the contestability and fairness concepts, as used in the context of the DMA, are clear. There are, however, relatively few details provided about what is meant by the terms 'fairness' and 'contestability'.

Article 10(2), which relates to the use of market investigation to update obligations, sets out that:

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; or*
- b) the **contestability** of markets is weakened as a consequence of such a practice engaged in by gatekeepers.*

The Impact Assessment (at paras 109/110) is more forthcoming (emphasis added):

*[C]ertain digital markets may not be functioning well and delivering competitive outcomes due to their particular features, in particular extreme scale (or scope) economies, and a high degree of vertical integration; direct or indirect network effects; multi-sidedness; data dependency; switching costs; asymmetric and limited information, and related biases in consumer behaviour as well as the conduct of gatekeepers. Therefore, **a specific policy objective is to allow identifying and addressing such market failures in respect of key digital markets to ensure that these markets remain contestable and competitive.** This will contribute to digital markets delivering low prices, better quality, as well as more choice and innovation to the benefit of EU consumers.*

*Gatekeepers' economic strength, their position of intermediaries between businesses and consumers together with market dynamics fuelling gatekeepers' growth lead to an imbalance in power between gatekeepers and their business users. This enables gatekeepers to impose unfair commercial conditions on business users, thus hampering competition on the platform. Such unfair behaviour does also have a negative impact on (the emergence of) alternative platforms since it strengthens consumer lock-in thus preventing multi-homing. In light of this, **a specific policy objective is to lay out a clearly-defined set of rules addressing identified gatekeepers' unfair behaviour, thereby facilitating a more balanced commercial relationship between gatekeepers and their business users, which would be also expected to create the right incentives for multi-homing.***

These various reference points help to discern what is intended by the terms contestability and fairness in the context of the DMA. However, they leave some questions unanswered. At the same time, while the DMA obligations are discussed both in the DMA Recitals and the Impact Assessment, there is no comprehensive discussion of how each obligation is intended to deliver against each objective. Indeed, it is also not clear whether any obligations are meant to deliver against both objectives, as opposed to just one. In assessing the effectiveness of each obligation, this would seem important.

2.2.1 What is meant by fairness? And what obligations does this relate to?

Fairness is a term that can mean many things in different contexts. In the context of the DMA, it is clear that, for a commercial practice to be unfair, it must result from an imbalance of power between gatekeepers and business users and confers a disproportionate advantage on the gatekeeper. This is useful but it is not a very full explanation.

At the same time, when regulating bilateral trading relationships between commercial parties, any fairness concept must be fairly tightly defined. The reason for this is well set out by Tommaso Valletti (then DGComp Chief Economist) in a different, but analogous, context (the debate around unfair trading practices regulations in the food supply chain):

*It is not obvious to determine what is "fair" or "unfair" in bilateral commercial negotiations [...] Commercial transactions between various businesses along the supply chain typically aim both at (i) maximizing the total gains from the transaction (i.e. the size of the pie), and (ii) splitting these total gains between parties (i.e. sharing the pie). Therefore, **identifying efficiency-enhancing commercial practices as unfair trading practices and prohibiting them could very well harm all parties involved [...] by reducing the size of the pie (the total gains from the transaction) to be shared between the trading partners in the first place.**¹ (emphasis added)*

This risk is serious. It is therefore important to ensure that the concept of fairness utilised within the DMA is focused on enhancing overall efficiency. This is in line with Recital 79 cited above. We propose that a good way to do this is to **focus on the fairness of commercial opportunity, rather than focusing on how any resulting surplus is shared out**. If market actors have greater fairness of commercial opportunity, then a fairer sharing of the surplus should emerge anyway, without this being a direct objective. We have identified four possible categories of fairness that link to the idea of commercial opportunity, and how such opportunity might be unfairly limited due to an imbalance of power. Between them, these four categories appear to underpin the vast majority of proposed DMA obligations:

- i. Fair right to access alternative routes to market:** Some of the commercial terms addressed by the proposed Obligations restrict business users' use of alternative platforms or other routes to markets. Examples include Articles 5(b), 5(c), 6(1)(c), 6(1)(d).
- ii. Equitable treatment of third-party business users relative to the gatekeeper's rival services:** Some of the proposed Obligations are designed to ensure non-discriminatory treatment of all business users, irrespective of who owns them. Examples include Articles 5(e), 5(f), 6(1.a), 6(1.b), 6(1.e), 6(1.f), 6(1.i), 6(1.k).
- iii. Fair transparency about the service provided and the terms of those services:** This is addressed in the context of the advertising services by Articles 5(g) and 6(1.g).
- iv. Fair rights of expression to public authorities:** The right to complain to public authorities is addressed by Article 5(d).

These four categories appear well-aligned with an efficiency-focused concept of fairness. We note that only the first is tightly linked with the specific aim of increasing multi-homing which is highlighted at para 110 in the Impact Assessment, cited above, but we find the focus on multi-homing unduly narrow. It is noteworthy that, if one includes all four of these aspects within the DMA concept of fairness, then this concept arguably motivates almost all of the DMA obligations (other

¹ Commission Staff Working Document of 12 April 2018, Impact Assessment on the Proposal for a Directive on unfair trading practices in business-to-business relationships in the food supply chain, SWD(2018) 92: Annex H: Economic Impact. See pp.260-268 at: <https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-92-F1-EN-MAIN-PART-1.PDF>.

than Articles 5(a), 6(1.h) and 6(1)). We also note that all eighteen Obligations are described – at Annex 5.2.2 in the Impact Assessment – as addressing ‘unfair practices’.

It is perhaps not so surprising that **almost all of the Obligations can be justified on fairness grounds, given that there are direct links between unfair commercial practices, as described above, and contestability**. Taking each of the forms of fairness identified above in turn:

- i. **Fair right of access to alternative routes to market:** Commercial practices that restrict business users from accessing rival routes to market inherently limit the entry and expansion of such alternatives to act as a competitive constraint to the gatekeepers’ core platforms. More generally, any barrier to multi-homing can make a service which exhibits network effects more likely to ‘tip’ towards being concentrated. Alternative routes to market could include rival platforms, but could also include direct access to market, or partial platform disintermediation, for example through using alternative ancillary services or using the platform for only part of the service offered by the business user. Such unfair commercial practices directly constrain platform contestability.
- ii. **Equitable treatment of third-party business users relative to the gatekeeper’s rival services:** Discriminatory commercial terms that give the gatekeeper an unfair advantage in related markets inherently enable it to leverage from its core market position into these related markets. In the longer term, such commercial practices may indirectly constrain platform contestability, since the most likely source of entry into a gatekeeper’s core platform service will often be a successful business user of the platform, either through reverse integration into the platform service or through fostering entry by an independent platform.
- iii. **Fair transparency about the service provided and the terms of those services:** Business users can only make informed decisions about the use of alternative platforms if they have a good understanding of the deal they are receiving from the gatekeeper platform. As such, greater transparency should foster contestability.
- iv. **Fair rights of expression to public authorities:** Unless firms have the right to complain to public authorities, the DMA (and also competition authorities) will unlikely be fully effective in driving up contestability.

Indeed, the discussion of the fairness objective in the Impact Assessment (as cited above) emphasises the concern that, due to their economic strength, gatekeepers can impose terms on business users that both distort competition **on** the platform but also, over the longer term, limit contestability **to** the platform.

We note that, **as currently described within the DMA proposal, the concept of fairness relates purely to the treatment of business users**. This might seem odd, given that some of the obligations appear to relate to the fair treatment of end-users, not just fairness to business users. In particular, *Articles 5(a), 5(e), 6(1.b) and 6(1.h)* would seem at least partially motivated by the fairness objective for end-users relating to data protection and data control.

However, it may be that the Commission fears that incorporating fairness to end-users would open up the fairness concept too far, and move too far in the direction of consumer protection. This may be right, and we note that the obligations we identify can also be motivated by other fairness and/or contestability considerations. If the DMA is successful in achieving its core objectives, this should create a fairer situation for end users too, without this needing to be explicitly incorporated within the DMA’s fairness concept.²

² We note that Recital 12 does appear to refer to end-users, but – given the language used elsewhere in the DMA – perhaps this is intended in this indirect way. “*Weak contestability and unfair practices in the digital sector are more frequent and pronounced for certain digital services than for others. [...] These providers of core platform*

2.2.2 What is meant by contestability? And what obligations does this relate to?

As regards the contestability objective itself, the paragraphs cited above are clear that this is intended to relate to the **contestability of regulated Core Platform Services (CPS) only. This is a relatively narrow approach, in that it arguably excludes two important forms of contestability.**

First, it is not clear whether the DMA concept of contestability encompasses **platform disintermediation**. This can take two forms: *either* business users moving to direct supply (as opposed to an alternative platform); *or* partial disintermediation, whereby business users utilise an alternative provider for some – but not all - parts of the CPS service (whether this will be contracting out ancillary services to a third party, or dealing directly with end users). Platform disintermediation may not lead to the entry or expansion of a full-service rival to the gatekeeper but can provide an important competitive constraint on it. We would suggest that platform disintermediation should be recognised as an element of contestability.

Second, it is not clear whether the DMA concept of contestability encompasses **contestability of related markets, and therefore addresses unfair leverage by a gatekeeper from the regulated CPS into related markets**. In this context, we note that the Furman Report (and others) identified two key problems with digital platform markets: first, that they have a tendency to tip to being highly concentrated and hard to contest; and second, that the incumbent platforms then tend to leverage their position into related markets. The current contestability objective encompasses the former concern, but not the latter.

An argument could be made that leverage into related markets does, over the longer term, indirectly limit core platform contestability, since a likely source of entry into a gatekeeper's core platform service will often be a successful business user of that platform service. In this case, a focus on the contestability of regulated CPS only still arguably be used to justify obligations that address leverage. However, it is far from clear from the wording in the DMA proposal that this is intended.

There is an exception, in which the narrow DMA contestability objective, as it stands, does appear to address leverage, but this is the very specific instance where a gatekeeper has multiple regulated CPS, some of which are effectively business users of others. For example, Google Search could be viewed as a 'business user' of the Android OS. In this situation, leverage from one regulated CPS service would directly impact the contestability of another regulated CPS, and this would fall within the narrow formulation of contestability.

However, significant concerns about leverage into related markets extend beyond situations where both CPS already constitute an important gateway for the gatekeeper, in the terms of Art 3(1.b). Moreover, **despite the narrow drawing of the contestability objective to contestability of regulated CPS markets, there are in practice several obligations which appear to reflect concerns about both the leverage into related markets, and barriers to platform disintermediation** as shown in Table 1.

*services have emerged most frequently as gatekeepers for business users and **end users** with far-reaching impacts, gaining the ability to easily set commercial conditions and terms in a unilateral and detrimental manner for their business users and **end users**". (Emphasis added)*

Art.	Summary of the obligation	Promote direct CPS contestability	Promote platform disintermediation	Limit leverage into related markets
5a	No data fusion without user consent	x		x
5b	No wide MFN/parity clauses	x		
5c	No anti-steering	x	x	
5d	No prevention of raising issues with public authorities	x	x	x
5e	No tying to business users from CPS to ID services	x	x	x (into ancillary services)
5f	No tying from CPS to other CPS	x		x (but only into regulated CPS)
5g	Price transparency for ads	x	x	
6.1a	No use of data related to business users to compete against them	x*		x
6.1b	Allow un-installing of apps, unless essential to OS/device	x*		x (into apps)
6.1c	Allow 'side loading' of third-party apps or app stores, unless threatens the integrity	x (app stores)	x	x (into apps)
6.1d	No self-preferencing in rankings	x*	x*	x
6.1e	No technical restriction of switching or multi-homing across apps using OS	x*		x (into apps)
6.1f	Access and interoperability for business users and ancillary services to OS should be as for proprietary ancillary services	x*	x	x (into apps and ancillary services)
6.1g	Performance transparency for ads	x	x	
6.1h	Provide real-time data portability for end-users	x		
6.1i	Provide real-time data sharing for business-users	x		x
6.1j	Data sharing obligation: FRAND access to click and query data	x (Search)		
6.1k	Fair and non-discriminatory terms of access to app stores	x	x	x (apps)

* For these, the CPS contestability narrative only appears to hold in specific instances where the gatekeeper has a regulated CPS in both a platform market and a related business user market

Table 1: Apparent 'contestability' objectives of the obligations

This table sets out our view on the expected impact of each obligation in relation to each of these categories of contestability. We note that:

- While all of the obligations can be viewed as promoting **direct CPS contestability**, there are (at least) five cases where the primary focus appears to be on limiting leverage. An impact on direct CPS contestability only arises for gatekeepers that have at least two regulated CPS and one is a business user of another.
- Around seven of the obligations appear intended to promote **platform disintermediation**, either partial or full. This could in turn facilitate the development of new platforms.

- Around 12 out of the obligations would be expected to limit leverage by the gatekeeper from a regulated CPS into a related market (whether or not it is a regulated CPS in that related market). As discussed above, limiting such leverage would be expected to directly promote the **contestability of the related market**, but only indirectly (if at all) to promote contestability in the core CPS market.

Why do we see a focus on leverage into related markets, even though it is not part of the contestability objective? As was highlighted above, it seems that **leverage concerns are effectively addressed within the DMA via the fairness objective**. If this reading of the DMA proposal is correct, it implies a slightly odd situation, in that a potentially important strand of contestability issues – leverage which harms contestability in related markets - are being addressed under the fairness objective.

Of course, it could be argued that it is appropriate for the DMA to be cautious about limiting leverage by the gatekeepers into related markets, or even that this is not a suitable objective for the DMA. After all, there is a risk that obligations which are designed to limit leverage could have an ambiguous impact on contestability in these markets:

- On the one hand, if regulation were to unduly restrict the ability of gatekeepers to enter and expand in new markets, then this could harm contestability in these related markets, rather than enhancing it.
- On the other hand, if it is unduly easy for gatekeepers to enter and expand in related markets, then this will limit the ability and incentive for independent third parties to do so, reducing contestability in these related markets. In this case, regulation which limits such leverage would enhance contestability in these related markets.

Given this balance to be struck, the **DMA would ideally balance these concerns by not preventing gatekeepers from entering or expanding into related markets, but limiting them from doing so by unfairly leveraging from their position in their regulated core platform services**. But there is a fine line to be drawn here between fair and unfair market entry/expansion. **It could be that this is the line that the Commission is trying to draw when describing obligations which appear to relate to leverage as reflecting the fairness objective**. But if so, it would be useful to be more explicit about it.

Linked to this, another reason for the DMA adopting a relatively narrow concept of contestability may be that there is currently no potential for firms to make an objective justification defence for breaching an obligation. In this situation, it may make more sense to avoid obligations which could have positive or negative implications for contestability, and thus this could lie behind the currently narrow contestability concept. CERRE has previously recommended that objective justification should be possible, albeit on the relatively narrow grounds that compliance would in fact harm fairness and/or contestability, and thus act contrary to the objectives of the regulation.³ **If such an objective justification were to be incorporated within the DMA, this would arguably strengthen the case for a more expansive concept of contestability**, which more fully reflects the competition concerns highlighted by the Furman Report and others.

A final point on contestability. It cannot be expected that the DMA (and certainly not any specific obligation) can be truly effective in ensuring contestability in CPS markets, as the Recitals suggest. Contestable markets – as envisaged by Baumol (1982) – are a theoretical construct. They require extremely strong assumptions, which more or less never hold in reality, and certainly do not hold in markets characterised by strong economies of scale and scope, network externalities, and consumer behavioural biases. **No one seriously expects the DMA to be able to 'ensure' contestable markets. Rather, it is hoped that the regulation will 'enhance' contestability**, in the sense of lowering barriers to entry and expansion and thereby better enabling and incentivising third

³ CERRE DMA First Assessment Paper, January 2021, p.22-23.

parties to compete and innovate.⁴ This concept of contestability is more of a spectrum: a market can exhibit less or more contestability, depending on the size of the barriers to entry and expansion. Does this mean that the wording needs to change?

2.3 Recommendations

It would be useful to spell out more fully within the DMA itself what is meant by the contestability and fairness objectives, how the two interact, and what are the limiting principles in relation to both concepts? However, we have also noted that the contestability objective appears unduly narrow. This leads us to the following recommendations.

- *Recommendation (a): The concept of fairness in the DMA should be clarified*

In terms of fairness, the discussion above suggests that the DMA fairness concept excludes both fairness to end users and the fair sharing of surplus between commercial firms. These may well be indirect benefits of the DMA, but they are not direct objectives. This could usefully be made more explicit. One way of clarifying the precise formulation of fairness would be to add in a **focus on commercial opportunity**. For example, Article 10(2.a) might be reworded:

"There is an imbalance of rights and obligations on business users, which restricts the commercial opportunity open to the business user, and so confers an advantage on the gatekeeper that is disproportionate to the service provided by the gatekeeper to business users"

The Recitals might also usefully set out the four ways we highlight above in which an imbalance of power might feed into unfair commercial terms.

- *Recommendation (b) The concept of contestability in the DMA should be widened*

Serious considerations should be given to **widening the contestability objective to include both platform disintermediation and limiting unfair leverage by gatekeepers into related markets**. It seems inappropriate to introduce obligations which have these objectives under cover of the fairness objective. Such a widening may be less risky if the Commission also accepts the separate CERRE recommendation to introduce a narrow form of objective justification. In the alternative, if the contestability objective is not widened, the DMA should be more explicit about how leverage is addressed by the fairness objective.

Also, given the discussion of contestability above, we would recommend changing the wording around the objectives of the DMA **from 'ensuring' contestability to 'enhancing' contestability**.

- *Recommendation (c): Matching obligations with objectives*

It would also be useful for the DMA to **set out more clearly how each obligation is intended to deliver contestability and/or fairness**. This would better enable the assessment under Article 7 of the effectiveness of each obligation in achieving its objectives. It may also be useful in further clarifying the obligations themselves.

⁴ See CERRE (2020), *The role of data for digital markets contestability: case studies and data access remedies*, <https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/>

3 The scope of the obligations

3.1 The Commission's proposal

Another issue concerning the obligations is that their likely scope, in terms of the Core Platform Services covered, is not always entirely clear. Table 2 below provides an initial assessment on which Obligations apply to which core platform service. The letters used for identifying CPS are based on the Article 2(2).

Our assessment shows:

- 8 of the 18 Obligations are (more or less) **focused on one or two particular CPSs**. Of these, obligation 5b, which restricts wide MFNS and exclusive dealing, is explicitly restricted to online intermediation services, but it is not entirely clear why. The exclusive dealing provisions, in particular, seem likely to be of value in other CPS too.
- A further 4 of the 18 appear to be **targeted to one or two particular CPSs**, but their applicability is ambiguous, and they could in theory apply more widely. Of these, Obligation 6(1)(d) on self-preferencing is theoretically of wide applicability, but in practice may only be relevant to a subset of CPS. But this is ambiguous.
- 4 of the 18 Obligations are effectively ecosystem-wide provisions, in that they relate to gatekeepers with **any type of CPS**. Of these, obligation 5(f), relating to tying between CPS, is also of wide applicability, in that it can apply to any CPS, but only applies between two 'relevant' CPS (i.e. CPS which are themselves 'important gateways').
- App stores are likely subject to the vast majority of Obligations (arguably 14 out of 18). Operating systems and marketplaces are each likely subject to around 9 out of 18. If one combines search engines (b) and their associated advertising services (h), then they are likely subject to 9 out of 18, and on the same basis social networks are subject to 8 out of 18.
- By contrast, some other individual CPS are likely subject to just 4 or 5 Obligations. In particular, this is relevant to number-independent communications services (e) and cloud computing services (g).

Ob.	Summary of the obligation	CPS relevant?	Comments
5a	No data fusion without user consent	All	Effectively ecosystem-wide.
5b	No wide MFN/parity clauses or exclusive dealing	a (app stores and marketplaces)	Clear (NB interesting that scope so narrow)
5c	No anti-steering	a (app stores and possibly marketplaces)	Fairly clear, although could apply more widely in theory
5d	No prevention of raising issues with public authorities	All	Effectively ecosystem-wide
5e	No tying to business users from CPS to ID services	All	Effectively ecosystem-wide
5f	No tying from regulated CPS to other regulated CPS	All, but needs at least two regulated CPS.	Clear (once related CPS have been clearly identified) but will be different for each gatekeeper
5g	Price transparency for ads	h	Clear
6.1a	No use of data related to business users to compete against them	a (app stores and marketplaces)	Ambiguous. Could apply more widely, e.g. to: b and h.
6.1b	Allow un-installing of apps, unless essential to OS/device	a (app stores) and f	Clear
6.1c	Allow 'side loading' of third-party apps or app stores, unless threatens integrity	a (app stores) and f	Clear
6.1d	No self-preferencing in rankings	a, b, c and possibly f	Ambiguous. Could apply more widely in theory.
6.1e	No technical restriction of switching or multi-homing across apps using OS	f (and arguably also a (app stores))	Ambiguous. Could apply more widely in theory.
6.1f	Access and interoperability for business users and ancillary services to OS should be as for proprietary ancillary services	f	Ambiguous. Could apply more widely in theory.
6.1g	Performance transparency for ads	h	Clear
6.1h	Provide real-time data portability for end-users	All	Effectively ecosystem-wide, but probably not h in practice.
6.1i	Provide real-time data sharing for business-users	a (app stores and marketplaces)	Ambiguous. Could apply more widely, e.g. to: b, c, d, g or h.
6.1j	Data sharing obligation: FRAND access to click and query data	b	Clear
6.1k	Fair and non-discriminatory terms of access to app stores	a (app stores)	Clear

Key: a – online intermediation services; b – online search engines; c – online social networking services; d – video-sharing platform services; e – number-independent interpersonal communication services; f – operating systems; g – cloud computing services; and h – advertising services.

Table 2: Likely scope of the obligations

3.2 Recommendations

- *Recommendation (d): Consideration should be given to regulating number-independent communications services and cloud computing services on the same basis as advertising services, that is only if 'provided by a provider of any of the [other] core platform services'.*

Very few obligations apply to number-independent communications services and cloud computing services, and no obligations apply uniquely to them. Where a gatekeeper provides these CPS alongside other CPS (such as Facebook and WhatsApp), it may make sense to include these within the overall regulatory scope. However, for firms which solely provide these services, it is far from obvious that it is proportionate to bring them into the regulatory fold on the basis of such limited regulatory coverage.

As explained in the issues paper on designation, the DMA could provide that **number-independent communications services and cloud computing services would be regulated as CPS only where gatekeepers were designated on the basis of another CPS** – and that they cannot be used for gatekeeper designation in their own right. This is effectively already the case for advertising services which are only categorised as a CPS in their own right if provided by a provider of any of the other core platform services listed.⁵

- *Recommendation (e): The presumption should be that obligations apply to all of the services provided by a gatekeeper within a regulated CPS*

A final recommendation relates to gatekeepers who are designated as having an important gateway CPS for one of the CPS categories, but also have other services within that CPS category. An example might be Apple, which could be designated as an intermediation service for its app store, but which also has e-book and e-music intermediation services. This raises an obvious question: does the regulation relate to all services within this CPS category or just the service which forms the basis of the designation?

Given the potential for services to change their precise nature rapidly in the digital realm, there is certainly an argument for CPS-wide designation. Moreover, it is in the nature of digital ecosystems that market power over a particular service also tends to confer a degree of competitive advantage over nearby services. At the same time, however, it may be disproportionate to impose all obligations on services which are included merely because they fall under the same CPS category.

On balance, the best option might be to **include all services within a designated CPS by default but for the Article 7 specification process to allow for the removal of non-core services from the scope of some or all obligations on grounds of proportionality**. We note, though, that this does not solve the problem for Article 5 obligations, where Article 7 does not apply. This would be solved if the distinction between Articles 5 and 6 were removed. Alternatively, it may be worth allowing for a narrow form of specification – on scope only – for Article 5 obligations.

- *Recommendation (f): Consideration should be given to explicitly narrowing the scope of specific obligations*

In some cases, it does not necessarily matter that the scope of an obligation is wider than the obvious CPS at which it is targeted. If there is no chance of the obligation applying to a particular CPS, then there is no work to be done in meeting the obligation. And if the obligation genuinely has general applicability across all CPS, then there may be a benefit in keeping the scope wide. This might potentially be true of Article 5(c) which prohibits anti-steering, for example, and appears to apply only to online intermediation services but might be a reasonable obligation to impose on any CPS to which it might apply.

⁵ DMA Proposal, art.2(2h).

However, there are other obligations where the potential breadth of applicability, in terms of scope, seems potentially problematic. **Narrowing the scope is likely to be especially merited where the potential applicability of the obligation runs far wider than the core service which provided the original rationale** (see Table 2 in the Impact Assessment). Certainly, it is not obvious that the Commission has considered the proportionality of each obligation in relation to each CPS where it could potentially apply. Where this is true, it would seem appropriate and proportionate to explicitly narrow the scope of applicability.

In the alternative, given that this lack of clarity on scope primarily applies to Article 6 obligations, it should be made explicit that the scope of application can be narrowed through the specification process. Article 6(1h) on end-user data portability may be an example of an obligation where it would make sense to keep the scope of applicability broad in principle, but where it would be proportionate to narrow this through the specification process to specific CPS where data portability will make a real difference to contestability.

- *Recommendation (g): Consideration should be given to widening the scope of Obligation on MFN*

Obligation 5(b) on MFN is arguably more narrowly scoped than could be justified, especially for the element which bans exclusive dealing.

4 The expected effectiveness of the obligations

The eighteen proposed obligations within the DMA are currently not entirely clear, several could be achieved in a variety of different ways, and some involve managing explicit tensions, for example between contestability and privacy. As such, the issue arising for gatekeeper firms is not so much whether or not to comply with the obligations (clearly they must), but rather the manner of compliance.

Table 3 in the Annex sets out, for each of the 18 proposed obligations, some initial thoughts on:

- The likely effectiveness of each, and the factors that might limit this.
- Practical issues likely to arise either upfront, via clarifying the obligation or through the specification process, or in the ongoing assessment of compliance.
- Risk of any unintended harm arising from the Obligations, assuming that they are effective in achieving their primary aim (and excluding any risks that arise purely due to having lower revenues or higher costs, due to the regulation).

It would be useful to receive views at the workshop on the views and factors identified. However, based on this preliminary table, we have drawn the following conclusions.

4.1 Expected effectiveness and practical issues arising

Based on the assessment in Table 3, we identify significant concerns over the effectiveness of several of the eighteen obligations in their current form. There are **at least ten obligations where it would be useful if the DMA could provide additional clarity upfront, either within the Recitals or through reformulation of the objective.** Being as clear as possible upfront does create a risk of drawing the scope of the obligations too narrowly. However, it carries a huge benefit in terms of legal clarity (for both gatekeepers and business users) and in terms of the resources that will be required within the Commission to provide further specifications. In any case, the vast majority of Article 6 obligations are likely to require at least some further specification, at least as currently written.

The main questions and caveats identified fall under the following categories:

A risk that certain obligations may be unduly narrowly drawn and thus limited in its effectiveness. In particular, Article 5(f) prohibits tying **between regulated CPS markets**. This limits leverage between CPS activities where gatekeepers already have gateway power. While this is valuable, it is arguably rather narrow. Drawing from the discussion above about the merits of limiting leverage from core markets into related markets, there may be merit in extending this obligation to tying from regulated CPS markets into any related markets, not just other regulated CPS markets. This would be especially true if there were greater potential for (narrow) objective justification. Also, this obligation appears to be partially influenced by the Google Android case, but it is far from obvious that the obligation would have any effect on agreements between Google and OEMs, unless the latter are classed as 'business users'.

For the core **data-sharing provisions**, there is currently a **lack of specificity** about the requirements which could hamper effectiveness.

- For Article 6(1.h), relating to end user **data portability**, it is good that the provision specifies that data must be continuous and real-time.⁶ However, as currently framed, there is **no explicit requirement on gatekeepers to utilise Open APIs or to provide data in a consistent format over time. Nor any requirement for the direct transfer of data to third parties, rather than via the end user. Nor any requirement for the gatekeeper to keep track of consumer consents, on a readily accessible basis, and enable consent to be re-confirmed or revoked.** The provision does set out that portability needs to be 'effective', so all this may be implicit, but it would usefully be made explicit. The reliance on the definition of data portability under GDPR also means that there is also no clarity as to whether the data to be ported would include observed data, and not just input data. For the provision to have significant contestability benefits, it needs to include both input and observed data.
- Likewise, for Article 6(1.i) relating to **business user data access**, the obligation requires the provision of aggregated **or** non-aggregated data, but it is not clear who decides which. Can the gatekeeper simply decide to provide aggregated data only, or is it constrained to doing so only where there is a GDPR issue and a lack of consumer consent?
- For Article 6(1.j) relating to **search data sharing**, there is likewise no requirement to adopt a consistent or open approach to data-sharing (unless this is implicit with the requirement of FRAND terms), and there is no explicit requirement that data be **real-time or even recent**. Nor is there an explicit requirement to give access to **all** queries, click and view data, as opposed to a subset of such data. Finally, it is not clear how much the usefulness of data will be limited by the required anonymisation process.

There are also risks that **certain obligations are too widely applicable**. For example,

- Article 6(1.f) requires gatekeepers to allow **business users and providers of ancillary services access to and interoperability** with its OS/hardware/software on the same basis as its own services. This obligation appears to be influenced by the payment services market, with business users wishing to utilise alternative payment service providers, and payment service providers seeking to access the mobile payments market. But it is in practice not constrained – indeed, it is not even constrained to ancillary services (whatever they are). This potentially introduces a **very extensive duty to provide access and interoperability across a whole range of different aspects of the gatekeepers' core platform services**. It is not obvious that this breadth of applicability is intentional, it may well not be proportionate, and it may anyway be difficult to make effective.

⁶ See CERRE, *Making data portability more effective for the digital economy*, June 2020: <https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/>

- Articles 6(1.h) and 6(1.i) provide similarly extensive requirements around **data portability**. Experience from the UK Open Banking initiative suggests that it takes years, not months, to implement even a relatively simple data portability provision. Admittedly, the archaic banking infrastructure was part of the problem here, but the ambition here is far greater, and the scope very wide. If it is to be effective (see below), **data portability and sharing are complex and resource-consuming exercises**.⁷ It is far from obvious that it is appropriate to require data portability in all circumstances, with no clear limiting principles. It is unlikely to be effective in enhancing contestability and could reduce the attention given to making data portability work well in those areas where it could make a difference. There may be a serious need for prioritisation of those instances of data-sharing that will have the greatest impact on contestability, rather than trying to do everything at once.

There are **incentive-based risks** around the effectiveness of provisions which seek to ensure **fair-treatment between the gatekeeper's proprietary services and those rival third-party business users**. For example:

- Article 6(1.d) prohibits **self-preferencing in rankings**, but 'self-preferencing' can be **hard to define in practice**. This is especially true in paid-for rankings, where the gatekeeper can always pay more for rankings, given that it keeps the proceeds.⁸ It is also **hard to assess** whether the criteria utilised for ranking are genuinely objective. Moreover, even genuinely objective criteria can potentially be exclusionary – an example being Amazon giving preference in rankings to products which are 'fulfilled by Amazon' because it can be confident in speedy and reliable delivery; or Google giving higher rankings to sites which use Google Accelerated Mobile Pages because it can have confidence that they will load quickly. It is not clear that these examples will be addressed by this obligation.
- Article 6(1.k) requires that gatekeepers apply **fair and non-discriminatory terms of access to app stores**. Similar concerns arise here, especially if app stores charge for prominence (and there is nothing in the DMA that prohibits them from doing so). While Recital 57 provides some details on the benchmarks to be used as a yardstick for assessing the fairness of access conditions, it is **not clear that these benchmarks would fully prevent a gatekeeper from charging an unduly high price to both a third party business and its rival service**.

Consumer behavioural considerations: consumer inertia, consumer trust issues, over-willingness to sign up to unfair privacy consents, susceptibility to influence through choice architecture. Also, the fact that the gatekeeper is typically in control of the interface design will determine the **choice architecture** facing end users and can utilise A/B testing techniques to increase the impact of this choice architecture, potentially in ways that most suits its interests.⁹

A risk that GDPR requirements could limit effectiveness and that this could be exacerbated by gatekeepers acting with excessive caution in respect of GDPR, although this risk is partly addressed by the anti-circumvention provision in Article 11(2). There is also a question as to **what constitutes active consumer consent** in this context. Arguably consumers need to be given more than a 'take it or leave it' option whereby they are denied access to a service unless they give up all control over their data. But it is not clear whether this is required under the relevant obligations (or under the GDPR).

The Commission may face difficulty in assessing the evidence provided in relation to **technical exceptions**, e.g. in assessing the essentiality of apps in relation to obligation 6(1.b) or threat to integrity in relation to obligation 6(1.c).

⁷ CERRE, *Data sharing for digital markets contestability, Towards a governance framework*, September 2020.

⁸ See CERRE (2019), fn. 9.

⁹ CERRE, *Effective remedies for anti-competitive intermediation bias on vertically integrated platforms*, October 2019: <https://cerre.eu/publications/implementing-effective-remedies-anti-competitive-intermediation-bias-vertically/>

There are significant risks that **effective implementation is not likely to be feasible in six months**, and indeed that there could be a trade-off being speed and effectiveness. This is especially true for the interoperability and data-related obligations.

There also significant issues around **how to monitor some of the obligations**, especially around the use of data: breach (or circumvention) may not be apparent to either business users or end users.

Finally, we note that there has been no serious attempt by the Commission to **assess how effectively the group of obligations will work as a package**, and we have also not tried to do this. However, we note that there is no restriction on self-preferencing beyond ranking services/products, and that there are no provisions that ban the purchase, or requirement, of exclusive or preferential positioning. As such, it is not obvious that the obligations, as they stand, would have fully addressed the EC's Google Shopping or Google Android cases.

More generally, there is a question to be addressed about the extent to which – where relevant – the Obligations **apply to current contracts or just new ones**? If current, does this change termination rights – that is, does this mean that contracts can be entirely renegotiated? Would there be any exception for technical issues, for example if it were to prove technically impossible to enable already installed apps to be suddenly capable of being uninstalled?

4.2 Recommendations

The above issues give rise to a variety of recommendations. Note that we have not endeavoured here to propose precise revised wording, but rather to highlight the areas which merit further consideration.

- *Recommendation (h): Clarify or narrow down some obligations*

Given the concerns highlighted above in relation to obligations being too narrowly drawn, some **obligations require greater upfront clarification**, within the Recitals, or even reformulation.

It should be made clear, for instance in the DMA Recitals, that incentivising conduct, for example through offering higher rankings/prominence for firms that behave as desired by the gatekeeper, will be viewed as seriously as specific behavioural requirements.¹⁰

Moreover, as already recommended in section 3, the concerns highlighted above in relation to certainly obligations being too widely applicable, it should be **made explicitly possible for applicability to be refined and narrowed through the Article 7 specification** process.

- *Recommendation (i): In relation to choice architecture for consumer consent and other choices*

There needs to be **regulatory oversight of the choice architecture** put in place by the gatekeepers and overarching **principles for what is expected**. One option would be to require the gatekeepers to design their choice architecture so that it best reflects the decisions that consumers would make if making fully deliberative choices based on complete information. This should be testable via A/B testing. It would be useful to make explicit that the Commission can require gatekeepers to engage in such A/B testing and to provide the results of any such testing to the Commission.¹¹

¹⁰ CERRE, *Effective remedies for anti-competitive intermediation bias on vertically integrated platforms*, October 2019 made the recommendation that a ban of pay-for-prominence is not proportionate, but it may need to come with heightened transparency standards vis a vis the regulator.

¹¹ This recommendation is also made in CERRE, *Effective remedies for anti-competitive intermediation bias on vertically integrated platforms*, October 2019.

- *Recommendation (j): On data protection*

Given that there are likely to be significant issues of GDPR interpretation, the **Commission, as the DMA enforcer will liaise on these with the system of data protection regulation.**¹² The Commission should consider clarifying that active consumer consent requires that the gatekeeper provide a genuine choice, not a 'take or leave it' offer, and that consumers should be readily able to both give and revoke consent.¹³

- *Recommendation (k): On technical risks associated with the speed of implementation*

To limit the undue risk of technical error, there should be some potential for the regulator to, at its discretion, provide **additional time for implementation.**

The Commission needs to give thought to how it will deal with the more technically complex aspects of the regulation. It may need to arrange access to **technical 'Special Advisors.'**

- *Recommendation (l): Effective obligation and implementation*

More fundamentally, it is unlikely that the Obligations are going to be perfect. We consequently need a better system for good and EU interpretation of the obligations as well as a **better feedback loop whereby learning from experience is brought into implementation improvement.** For instance, a regular evaluation of the effectiveness and proportionality of the measures specified in Article 7 decision should be provided with the possibility for the Commission to re-specify the obligations if needed. More fundamentally, the list of Obligations in Articles 5 and 6 should be assessed at regular intervals with possibilities to add new obligations (as already foreseen in the Proposal) but also the possibility to remove obligations.

Finally, not discussed above, but while the obligation not to prohibit firms from raising issues with public authorities is welcome, it is unlikely to be fully effective until the Commission can offer a well-designed **whistleblowing function**, whereby complaints can be made in a way that protects the complainant's anonymity. Also, it would be useful to make explicit that the anti-circumvention element of the DMA (Article 11) implies that gatekeepers are prohibited from any retaliation against complainants or whistle-blowers, even if there is no explicit non-complaint clause in their contract.

5 Risks of unintended harm

In a previous paper, we proposed that there should be some potential for firms to make an objective justification defence for breaching an obligation, but on the relatively narrow grounds that compliance would harm fairness and/or contestability, and thus act contrary to the objectives of the regulation. Arguments based on the impact of the firm having lower revenues or higher costs, due to the regulation, would not be included.

In Table 1 above, we set out that many Obligations appear to be at least partially targeted at limiting unfair leverage into related markets (even if this is done via the fairness objective). As discussed above, **if this unduly restricts the ability of gatekeepers to enter new markets, then this has the potential to harm contestability in these related markets, rather than enhancing it.** This is a key risk to a core objective of the DMA. However, it is arguably addressed by our earlier recommendation.

Besides, drawing on the analysis in Table 3, there are many **other possible risks** of unintended harm arising from one or more obligations. These include:

¹² This recommendation links to the recommendation in the CERRE issues paper on institutional design which called for more involvement of national authorities, including data protection authorities.

¹³ We have made both recommendations (that consent needs to be fine granular and that consent should be more standardized) in this CERRE report: <https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/>.

- Risk to the **effectiveness of targeted advertising**.
- Risk to innovation, due to **overly restrictive technical requirements**.
- Risk that the '**consumer journey**' is **less smooth** than currently.
- Risk that **prices increase** for some elements of service. These could potentially fall disproportionately on vulnerable consumers, for example, if device prices increase or fees are introduced for currently free services.
- Risk of **increased refusal to deal** with particular business users and further integration into related markets.
- Risk to **privacy** and data protection.
- Risk of harm to **system integrity**.

The latter two categories of risk are largely **mitigated** by the formulation of the obligations, and the Article 9 public interest exemptions. Concerning the remaining risks, a degree of mitigation is provided by the proportionality requirement under TEU, which requires that the objectives of the DMA are achieved in the least restrictive way possible. The risks above would presumably be relevant to assessing the extent to which different measures for meeting DMA obligations are restrictive. That said, it is not clear why integrity is not included as a condition in Article 6(1)(f), and this would be useful to change.

There is also a general risk that these obligations, which involve substantial system change, could lead to **programming errors and a worse service to all users**, including potential security risk. This risk is exacerbated by the required speed of change. The incentives of the gatekeepers are aligned with their users in this area, and they will endeavour to **mitigate** this risk so far as possible. But mistakes could happen. This risk may be mitigated by recommendation (n) above, under which the Commission would have the discretion to provide longer timescales for implementation.

Finally, the much-stated **free rider concerns** relating to these various obligations would seem to be **minimal**, so long as they only apply (as is proposed) to the relevant CPS of the designated gatekeepers.

Annex: Assessment of individual obligations

Ob.	Summary of obligation	Likely effectiveness	Practical issues for specification and assessment	Risk of unintended harm
5a	No data fusion without user consent	<p>Likely for fairness, although noting the need to ensure that consent is genuine. Gatekeepers are in control of requesting consent and will have an incentive to design choice architecture to encourage it. Consent may not be meaningful if the choice is 'take it or leave it'. Also, should consumers be required to give consent to each data source separately. Otherwise, risk that they do not express their true preferences. E.g. they may be happy sharing data with Google generally, but not their Fitbit data.</p> <p>Maybe for contestability. Risk that user consent will still be given fairly easily, and thus there will be no real impact on data-driven platform envelopment.</p>	<p>Clarity issue: Specification not allowed, but a key clarity question will be what constitutes active consent for this obligation, and how to assess whether consent choice architecture is appropriate.</p> <p>Ongoing compliance supervision issue: How to assess whether data is being shared across services, in contravention of consumer consent, in practice.</p>	<p>Risk that consent process makes consumer journey less smooth.</p> <p>Risks harming contestability where gatekeepers are the most likely entrants into new, or currently monopolised, markets, since it removes an efficiency benefit related to such entry. If effective in limiting data aggregation, the downside could be less effective online advertising, which in turn could limit contestability in business user markets.</p>
5b	No wide MFN/parity clauses and no exclusive dealing	<p>Likely. MFNs make it harder to enter/expand via offering lower prices/different terms. Note that the ban does not relate to narrow MFNs, which reduces the potential for increasing contestability via platform disintermediation in the form of direct supply. The exclusive dealing provisions would arguably be valuable beyond the narrow scope of online intermediation services.</p>	<p>Ongoing compliance supervision: How to identify circumvention - e.g. via giving higher ranking/prominence to business users who don't price lower elsewhere.</p>	<p>Some risk that loses a benefit of MFNs in relation to preventing exploitation of greater willingness to pay off, e.g., Apple device users. But unlikely to be a major issue if plenty of competition between business users. Some risk of increased incentives for a gateway to vertical integrates in the business user market itself, which could be bad for contestability. NB: Only limited risk of free-rider effects undermining viability, so long as applied limited to regulated CPS (where gatekeeper is strong).</p>

5c	No steering anti-	<p>Likely for fairness. Maybe for contestability. In practice, steering may be limited by consumer inertia - they may simply find it easier to transact/contract via the CPS. Consumer's trust in the CPS may also limit consumers from engaging with business users outside the CPS.</p>	<p>Clarity issue: The examples in the Impact Assessment relate to the app stores. Not sure if/how the second half of the obligation applies to marketplaces. The first half potentially could, but not clear, but does this mean the first half doesn't either? Also, presumably the second half is only required if a subscription is also available through the app store. Otherwise, could this require investment in extra functionality?</p> <p>Timing question: Any potential for time extension? Could be technically risky to do in 6 months. Ongoing compliance supervision: how to identify circumvention, in the form of the gatekeeper offering incentives to achieve the same end.</p>	<p>If this were to apply to subscriptions/services/offers not available on the app store, this might be technically complex, creating risks of technical errors. Risk that this might increase incentives for a gateway to vertically integrate into the business user market itself, which could be bad for contestability. NB: Only limited risk of free-rider effects undermining viability, so long as applied limited to regulated CPS (where gatekeeper is strong).</p>
5d	No prevention of raising issues with public authorities	<p>Likely.</p>	<p>Upfront issue: Need to establish clear, anonymised whistleblowing processes. Users may otherwise still be cautious about raising issues. Also, clarify that gatekeepers are not allowed to retaliate against complaints/whistleblowers.</p>	<p>--</p>

5e	No tying to business users from CPS to ID services	<p>Likely for intermediation services, subject to no significant GDPR issue arising. Maybe for social log-in services, since even absent tying, business users may still have an incentive to offer popular social log-ins since this potentially widens their user base.</p>	<p>Clarity issue: The Impact Assessment refers to both social login services like "login with Facebook" and also the requirement by intermediation services that business users utilise their user ID. But if the latter is in scope, are there no GDPR issues that need addressing, or is the purchase process tantamount to giving consent for the associated data sharing?</p>	<p>Risk of less smooth consumer journey: Less easy sign-in for consumers if gatekeeper ID service is not an option. Risk that third-party ID services are less trustworthy. Risk that requiring consumers to use additional passwords deters usage of third-party sites, thus reducing contestability.</p>
5f	No tying from CPS to other CPS	<p>Likely for business users. Maybe for end users, since they may well just sign up anyway – that is, the process of signing up may be a relatively small inhibitor, especially if only need to sign up to each CPS once.</p> <p>NB Not clear that it applies to agreements between gatekeepers and OEMS, even though it seems to derive from the Google Android/Google Play concern.</p>	<p>Clarity issues: Does this requirement cover CPS pairs for which it makes little sense (e.g. app store and OS)? Hard to see how an end user could sign up to an app store without signing up to the OS. Also, does it cover OEMS (are they business users?). If so, for new contractual agreements with OEMS or existing ones?</p>	<p>Risk of Less smooth consumer journey: End users don't like the requirement to sign up to services separately. Also, if effective in separating end user decisions on search/social networks from decisions to receive advertising, then could reduce effectiveness of online advertising, which could in turn limit contestability in advertisers' markets.</p>
5g	Price transparency for ads	<p>Likely, although risk that pricing provides limited benefit for advertiser decision-making, as it is inherently only evident after the event, and the past may not be a good guide to the future. But should still help a rival CPS to prove its relative value for money.</p>	<p>Clarity issue: Specification not allowed, but may need some oversight of format for disclosure. In particular, there are various stages in the ad tech supply chain, some of which are more contestable than others. If this obligation is to open these up, prices for each stage need to be disclosed, not the price of the bundle.</p>	<p>—</p>

6.1a	No use of data related to business users to compete against them	Maybe , albeit may be hard to police in practice.	Ongoing compliance supervision: Identifying and evidencing such use of data is very hard.	Could be argued that there is a risk of limiting competition in the business user market by restricting entry/expansion by the gatekeeper. But not very credible – this obligation just puts any such rivalry on a level playing field.
6.1b	Allow un-installing of apps, unless essential to OS/device	Maybe. Key benefit is that it is likely to incentivise gatekeepers to include the app in the app store, which in turn brings additional requirements. Also, ability to uninstall could reduce default effects (“if it has to stay, I might as well use it”). But consumer inertia may well limit effectiveness in practice, as may ‘essentiality’ condition. The ability to uninstall may also address privacy concerns around tracking/surveillance.	Specification issue: How to assess what is required for OS to function. Ongoing compliance supervision: How to assess circumvention when an obvious route would be to move elements of OS into apps, to make these indispensable for the functioning of the device.	
6.1c	Allow ‘side loading’ of third-party apps or app stores, unless threatens integrity	Maybe , but risk that limited by consumer inertia. Risk that integrity concerns could be overstated (after all side-loading is possible on desktop).	Specification issue: How to assess integrity concerns.	Risk of lack of coordination between third-party apps and gatekeepers resulting in weaker app performance and/or harm to innovation (in apps or OS). Integrity risk may not be fully mitigated.
6.1d	No self-preferencing in rankings	Maybe , but EC cases show that ‘self-preferencing’ can be hard to define in practice, especially in paid-for rankings, where the gatekeeper can always pay more for rankings given that it keeps the proceeds. Not clear that obligation will bite on Amazon giving preference to sellers who are ‘Fulfilled By Amazon’ (FBA) or Google giving preference to Accelerated Mobile Pages (MP) in search rankings.	Specification issue and ongoing compliance supervision: Guidance on how to ensure that ranking criteria used are genuinely fair and how to ensure that ‘paid for’ rankings are not distorted by gatekeepers being active on both sides of the market.	Risk that could limit innovation if can't give prominence to new proprietary products without established history, but this could appear as bias. Also could limit benefits of free fast delivery if FBA and AMP can't be preferenced.

6.1e	No technical restriction of switching or multi-homing across apps using OS	Likely , although possible there may still be non-technical restrictions.	Clarity issue: Would this include the ability for consumers to change defaults within OS – e.g. changing default map for Apple calendar to Google Maps? Ongoing compliance supervision: How to identify a technical restriction?	Possible risk to innovation if it makes gatekeepers less willing to introduce new functionality for some apps, because they would also have to ensure it didn't inhibit switching/multi-homing.
6.1f	Access and interoperability for business users and ancillary services to OS should be as for proprietary ancillary services	Likely for payment services , albeit possibly a problem that no obligation on the pricing of access, and a risk that Art 9(2) public security concerns are overstated. Maybe for other business users and ancillary services , but what are these? Should this provision apply to all apps that come pre-installed?	Clarity issue: Why no reference to integrity concerns here? Also is Commission able to limit applicability to particular ancillary services through the specification process? Ongoing compliance supervision: Complexities of assessing access price. Art 9(2) public security concerns likely to be raised - how to assess these?	Risk that interoperability requirement unduly limits innovation, especially if far more wide-ranging than payment services.
6.1g	Performance transparency for ads	Likely , except risk that GDPR implications are overstated, which limits independent validation.	Specification questions: May need to oversee format. In particular, there are various stages in the ad tech supply chain, some of which are more contestable than others. If this obligation is to open these up, performance at each stage needs to be disclosed, not the performance of the bundle. Further specification needed on who gets to see what - e.g. do content providers on YouTube get to see what adverts are placed, or just the associated revenues? For external validation, data sharing formats and APIs need to be developed. Ongoing compliance supervision: Assessment of GDPR issues.	---

6.1h	Provide real-time data portability for end-users	<p>Maybe. As currently framed (unless the word 'effective' is doing a lot of work), there is no requirement to use Open APIs or to provide data in a consistent format over time. No requirement for direct transfer of data to third parties, rather than via end user. (Unless all of this done via specification process.) More generally, risk of consumer inertia and lack of consumer trust. Might be helped if a clear requirement for the gatekeeper to have an easily accessible dashboard of consents, with easy cancellation – but this is not currently required. GDPR arguably only requires portability for input data, but contestability needs observed data too.</p>	<p>Clarity issue: Obligation needs strengthening along the grounds in the previous column. Also, is it required to ensure portability of all data – it is arguably disproportionate? Can this be narrowed through the specification process? [NB How to fit with data portability requirement for cloud services in Free Flow of Data Regulation (for Iaas/PaaS).] Specification question: Oversee format for data porting, and potentially agree on what data are in scope. Timing question: Any potential for a time extension for delivery - could? Could be technically risky to do in 6 months. Is it required to ensure portability of all data – it is arguably disproportionate?</p>	<p>Risk that consumers give uninformed consent, and privacy is compromised. Risk of data leaks or abuse by third parties and lack of redress.</p>
6.1i	Provide real-time data sharing for business-users	<p>Maybe. GDPR requirement and gatekeeper control over the consent process could mean only aggregated data is available, and it is unclear how useful this will be.</p>	<p>Clarity issue: What does 'or' mean - can gatekeeper just provide aggregated data if it fancies? Specification question: Oversight of format for data sharing. And potentially of what data are in scope. Ongoing compliance supervision: Risk that gatekeepers make the process too cumbersome, despite the requirement that data access is 'high quality'. Oversight needed over consent process? Timing question: Any potential for time extension? Could be technically risky to do in 6 months.</p>	<p>Risk that consumers give uninformed consent, and privacy is compromised.</p>

6.1j	Data sharing obligation: FRAND access to click and query data	Likely , albeit some questions around effectiveness. How much the usefulness of the data would be harmed by fact that there is no requirement to adopt a consistent or Open API approach to data-sharing (unless this is implicit with the requirement of FRAND terms), and no explicit requirement that data be real-time or even recent? Or by there not being an explicit requirement to give access to all queries, click and view data, as opposed to a subset Also not clear how much usefulness of data will be limited by anonymisation process.	Clarity issues: Is 'reasonable' element in FRAND sensible to include (NB missing in 6.1k)? Addressing effectiveness issues around requirements. Specification issues: Oversight of any anonymisation process. Guidance on how to set FRAND terms?	Risk that anonymisation is not effective, and privacy is compromised.
6.1k	Fair and non-discriminatory terms of access to app stores	Maybe. Not clear how to define 'fair and non-discriminatory. Risk that still effectively favours own apps - e.g. in setting fees, and other terms of access, it is hard to overcome the incentive effects of gatekeeper acting on both sides of the auction.	Specification issue: What is meant by fair and non-discriminatory terms in specific circumstances? (E.g. is it okay to charge nothing to free apps?) More thought is needed on how to ensure that terms of access are 'fair' in the context of the gatekeeper being active on both sides of the market.	Risk of harm to business users (and their customers) that currently get a good deal (e.g. free apps who pay nothing). Risk of consumer harm due to free apps ceasing to be free if fees to them increase. Could impact vulnerable consumers. Some risk of app stores deciding not to carry certain apps, or offer certain functionality.



cerre

Centre on Regulation in Europe

📍 Avenue Louise, 475 (box 10)
1050 Brussels, Belgium

☎ +32 2 230 83 60

✉ info@cerre.eu

🌐 cerre.eu

🐦 @CERRE_ThinkTank