



EFFECTIVE AND PROPORTIONATE IMPLEMENTATION OF THE DMA

ALEXANDRE DE STREEL (COORD)

MARC BOURREAU

SALLY BROUGHTON MICOVA

RICHARD FEASEY

AMELIA FLETCHER

JAN KRÄMER

GIORGIO MONTI

MARTIN PEITZ

January 2023



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

This paper is part of a larger CERRE project entitled ‘Effective and Proportionate Implementation of the DMA’ which is a collection of nine papers focusing on the trade-offs around the different possible interpretations of the regulation. The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Apple, Arcep, Booking.com, ComReg, DuckDuckGo, Google, Mediaset, Meta, Microsoft, Qualcomm, Spotify, TikTok, Vodafone, Ofcom, and ARCOM. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report 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 of any sponsor or of members of CERRE.

The authors would like to thank the European Commission for their continuous participation and valuable input to the project. Amelia Fletcher would like to specifically thank the European Consumer Organisation (BEUC) for their helpful comments on the chapter ‘DMA Switching Tools and Choice Screens’. Martin Peitz, author of the chapter ‘The Prohibition of Self-preferencing in the DMA’ is grateful for the useful comments of Alexandre de Streel, Richard Feasey, Amelia Fletcher, Jens-Uwe Franck, Matthias Hunold, Jan Krämer, Giorgio Monti, and Julian Wright on an earlier draft.

© Copyright 2022, Centre on Regulation in Europe (CERRE)

info@cerre.eu – www.cerre.eu



TABLE OF CONTENTS

ABOUT CERRE.....	3
ABOUT THE AUTHORS.....	4
1. RECOMMENDATIONS FOR THE EFFECTIVE & PROPORTIONATE DMA IMPLEMENTATION..	8
2. DMA COMPASS	27
3. NOTE ON DESIGNATION OF GATEKEEPERS IN THE DIGITAL MARKETS ACT	40
4. DMA TRANSPARENCY REQUIREMENTS IN RELATION TO ADVERTISING	49
5. DMA SWITCHING TOOLS AND CHOICE SCREENS.....	69
6. THE PROHIBITION OF SELF-PREFERENCING IN THE DMA.....	88
7. DATA ACCESS PROVISIONS IN THE DMA.....	117
8. DMA: HORIZONTAL AND VERTICAL INTEROPERABILITY OBLIGATIONS.....	143
9. PROCEDURES AND INSTITUTIONS IN THE DMA.....	162



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 widely acknowledged academic credentials 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 improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments, and regulatory authorities, as well as at strengthening the expertise of the latter, since, in many Member States, regulators are part of a relatively recent profession.



ABOUT THE AUTHORS



Alexandre de Streel is a CERRE Academic Director and a Professor of European Law at the University of Namur and the President of the Namur Digital Institute (NADI). Since April 2021, he is also the Chair of the EU Observatory on Online Platform Economy.

He is visiting professor at the College of Europe and SciencesPo Paris, and also an 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



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.



Sally Broughton Micova is a CERRE Academic Co-Director and an Associate Professor in Communications Policy and Politics at the University of East Anglia (UEA). She is also a member of UEA's Centre for Competition Policy.

Her research focuses on media and communications policy in Europe.

She completed her PhD in the Department of Media and Communications at the London School of Economics and Political Science (LSE), after which she was an LSE Teaching and Research Fellow in Media Governance and Policy and Deputy Director of the LSE Media Policy Project.



Amelia Fletcher[†] CBE is a Research Fellow at CERRE and a Professor of Competition Policy at the Centre for Competition Policy, University of East Anglia. She is also a Non-Executive Director at the UK Competition and Markets Authority and a member of the Enforcement Decision Panel at Ofgem.

From 2013/4 to 2020, she was a Non-Executive Director at the Financial Conduct Authority and the Payment Systems Regulator, and has been a member of DG Comp's Economic Advisory Group on Competition Policy. She was a member of the Digital Competition Expert Panel, commissioned by the UK Treasury and led by Jason Furman, which reported in March 2019.

She was previously Chief Economist at the Office of Fair Trading (2001-2013), where she also spent time leading the OFT's Mergers and Competition Policy teams. Before joining the OFT, she was an economic consultant at Frontier Economics (1999-2001) and London Economics (1993-1999).

She has written and presented widely on competition and consumer policy. In her ongoing research, Amelia has a particular interest in the implications for competition and consumer policy of behavioural economics and online markets.

Amelia has a DPhil and MPhil in economics from Nuffield College, Oxford.

[†] Amelia Fletcher is Professor of Competition Policy at the University of East Anglia and a Non-Executive Director at the UK Competition and Markets Authority. This paper is written in her academic capacity and does not necessarily represent the views of the CMA.



Professor **Martin Peitz** is a CERRE Research Fellow and Professor of Economics at the University of Mannheim. He is also a Director of the Mannheim Centre for Competition and Innovation.

His policy research focuses on digital markets, regulation, and competition economics.

Martin holds a PhD in Economics from the University of Bonn.



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.



Marc Bourreau is an Academic Co-Director at CERRE and Professor of Economics at Télécom Paris (Institut Polytechnique de Paris). He is affiliated with the Interdisciplinary Institute for Innovation (i3) for his research, which focuses on competition policy and regulation, digital markets, and telecommunications. Marc holds a Ph.D. in Economics from the University of Paris Panthéon Assas.



Giorgio Monti is a CERRE Research Fellow and 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*.



RECOMMENDATIONS FOR THE EFFECTIVE AND PROPORTIONATE DMA IMPLEMENTATION

Alexandre de Stree (coord)



TABLE OF CONTENTS

INTRODUCTION	10
1. RECOMMENDATIONS ON GATEKEEPER DESIGNATION	11
2. RECOMMENDATIONS TO INTERPRET AND IMPLEMENT THE DMA OBLIGATIONS	12
2.1. General Recommendations	12
2.2. Increasing Online Advertising Transparency: DMA Article 5(9) and (10) and 6(8)	15
2.3. Switching Tools and Choice Screens: DMA Article 6(3) and 6(4)	17
2.4. Prohibition of Self-preferencing: DMA Article 6(5)	20
2.5. Vertical and Horizontal Interoperability: DMA Articles 6(4), 6(7) and 7	21
2.6. Data Portability for End Users and Business Users: DMA Articles 6(9) and 6(10)	22
2.7. Data Access for Search Engines: DMA Article 6(11)	23
3. RECOMMENDATIONS FOR EFFECTIVE PROCESS AND INSTITUTIONAL DESIGN	24



INTRODUCTION

The Digital Markets Act (DMA)¹ entered into force on 1 November 2022 and its rules will apply from 2 May 2023. The Commission should designate, for the first time, the gatekeepers subjected to the rules by September 2023 at the latest, and those platforms should comply with prohibitions and obligations in March 2024.

Building on a series of eight issue papers as well as previous work done by CERRE on the DMA,² this paper provides points of attention and recommendations to implement the DMA. Section 1 focuses on gatekeeper designation, section 2 focuses on the obligations, and section 3 deals with the process and the institutional design.

¹ Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1.

² See: <https://cerre.eu/publications/european-parliament-digital-markets-act-dma-resilient-effective/> and <https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/>



1. RECOMMENDATIONS ON GATEKEEPER DESIGNATION

The Commission should designate a gatekeeper on the basis of a three-criteria test: (i) significant impact on the EU internal market; (ii) the control of an important gateway for business users to reach end-users; and (iii) an entrenched and durable position.³ To facilitate such designation, there is a rebuttable presumption that the three criteria are fulfilled when some quantitative thresholds (in terms of financial and user size) are met. However, on the one hand, a firm above the thresholds may try to rebut the presumption and show it is not a gatekeeper, and, on the other, the Commission may designate a firm below the thresholds when it meets the three-criteria test. As the issue paper on gatekeeper designation explains, three legal issues would benefit from being clarified.

First, we recommend that **every decision to regulate a Core Platform Service (CPS) will require a designation that the undertaking in question is a gatekeeper in relation to the provision of that specific service** and that, accordingly, references to ‘active users’ for the purposes of gatekeeper designations are referenced only to users of this CPS in question.

Second, we recommend that the **evidential standards used** in market investigations considering whether **to exclude a firm that otherwise meets the quantitative thresholds for gatekeeper designation should be the same as those used** in market investigations considering whether **to include a firm that otherwise does not meet the same quantitative thresholds**,⁴ subject to the practical constraints that arise from differences in the timescales available to the Commission to complete its investigations.

Third, the **application of Annex A of the DMA**, with the possibility that services provided by the same firm within the same CPS category may be assessed separately for gatekeeper designation if they are used for ‘different purposes’, **will need to be clarified through specific cases** and firms should not be able to abuse this provision in order to evade designation. Conversely, the Commission should ensure that services are not unnecessarily included in the list of designated CPSs where firms are not gatekeepers in relation to the provision of those services.

³ DMA, Art.3.

⁴ Resp. DMA, Art.3(5) and 3(8).



2. RECOMMENDATIONS TO INTERPRET AND IMPLEMENT THE DMA OBLIGATIONS

The EU lawmaker decided to base the DMA on detailed rules instead of broad standards to facilitate its implementation and increase legal certainty.⁵ However, **several obligations and prohibitions are not self-executing** because, on the one hand, they apply to technologies and business models which are diverse, fast-evolving, complex, and not always fully understood and, on the other hand, several trade-offs between conflicting values and interests, such as between openness and privacy or service integrity, have been left open by the lawmaker. This section raises some points of attention and provides recommendations in order to make the implementation of those obligations effective and proportionate.

2.1 General recommendations

(a) Clarify the interpretation of the obligations

The legal interpretation of several obligations, in Articles 5, 6, and 7, would need to be clarified by the Commission and the Courts. Given the importance of legal certainty for gatekeepers and their business users alike, those clarifications will be crucial, especially for the obligations that need product re-design, which may take time. Those clarifications are of three types.

The first type relates to the **material and geographical scope of application of some obligations**. Regarding the material scope, as indicated below, clarifications may be needed on the definition of publisher that benefits from the online ad transparency regime (art.5.9, 5.10, and 6.8), on multiple issues regarding the switching and default obligations (art.6.3) and 6.4), on the applicability of self-preferencing prohibition (art.6.5), on the intended scope and depth of access of the vertical interoperability obligation (art.6.7), on which data and context that need to be ported (art.6.9 and 6.10) or on the beneficiaries of search data access (art.6.11). Regarding the geographical scope, as indicated below, clarifications may be needed on search data sharing or horizontal interoperability (art.7). Those clarifications should build – and be consistent with – the EU digital acquis such as the GDPR,⁶ cybersecurity legislation⁷, IP, and trade secret laws.⁸

The second type of legal clarifications relates to the **precise meaning of some obligations**. As indicated below, clarifications may be needed on the online ad metrics that need to be made more transparent (art.5.9, 5.10, and 6.8), on how many alternatives need to be included in the default setting or how many access points to switch a default should be offered by the gatekeeper (art.6.3

⁵ Impact Assessment Report of the Commission Services on the DMA, SWD(2020) 363, para.153.

⁶ Regulation 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 (General Data Protection Regulation), OJ [2016] L 199/1.

⁷ Such as Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ [2016] L 194/1

⁸ Such as Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29, OJ [2019] L 130/92 or Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ [2016] L 157/1



and 6.4), on which self-preferencing practice is prohibited given its context (art.6.5) or which consent should be required when data are ported (art.6.9 and 6.10).

The third type of clarification, which may be the most fundamental, relates to **how compliance with the obligation is to be assessed and demonstrated**. As explained in the issue paper on the DMA compass, this may include the agreement between the Commission, the gatekeepers, and the main other stakeholders on a **set of quantitative measurements** on the impact of each obligation on relations between the gatekeeper and other relevant parties. Those indicators should be designed with transparent, fair, and open industry-wide discussions. They would introduce a degree of objectivity and shared factual understanding even if the interpretation of the measurements and the conclusions to be drawn from them will remain a matter of contention and be under the control of the Commission. However, those quantitative measures would be one signal among others that need to be considered alongside qualitative representations from the gatekeepers and their business users.

To provide those legal clarifications ‘to the market’, the Commission has several means with different timings. Before March 2024, the Commission may discuss them informally and on a case-by-case basis with the gatekeepers and their business users. After 2024, the Commission may give those clarifications more formally and individually to each gatekeeper when it reacts to their compliance reports, when it engages in formal regulatory dialogue, and/or when it opens non-compliance proceedings.⁹ Ultimately, of course, the final clarification and legal interpretation will be given by the Court of Justice of the EU. As soon as there is a relevant body of experience, the Commission could then ‘codify’ those legal clarifications and interpretations in general guidelines.¹⁰

(b) Establish robust mechanisms for implementation

To comply with the DMA, **gatekeepers will have to adapt their products and services**. Those adaptations should ensure that the goal of each obligation and the DMA as a whole are met, while respecting the principle of proportionality.

In many cases, it is optimal that **those mechanisms are process-based and will be determined by the regulated gatekeepers** who know their products the best. However, to alleviate the risk that the gatekeepers undermine the effectiveness of the DMA, the establishment of those mechanisms should be done **in partnership with the business users who may want to rely on the mechanisms to offer their services, and under the supervision of the Commission**. In reviewing gatekeeper submissions, the Commission could seek input from third parties (including those representing consumers), draw on the extensive evidence collected by gatekeepers through A/B testing, and potentially require its own testing. The Commission could usefully also set out how it expects gatekeepers to engage with third parties too.

In some cases, the redesign of the product and/or the establishment of new mechanisms will entail significant engineering changes which can take time. This is why the **Commission should be able to ‘stop the clock’** of the very tight deadlines of the DMA when an obligation needs to be clarified to be

⁹ Resp. art.11, 8 and 29 DMA.

¹⁰ DMA, Art.47.



implemented and when the gatekeeper cooperates in good faith with the Commission and their business users.

(c) Effectiveness and proportionality

Those interpretation and implementation questions should be solved by applying the two main overarching regulatory principles of the DMA, effectiveness and proportionality.

First, the measures taken by the gatekeepers should be **effective** in two ways:¹¹ achieving the overall objectives of the DMA as a whole (general effectiveness) and achieving the objectives of each obligation (specific effectiveness).

- **General effectiveness** refers to the two DMA overarching objectives of “contestability” and “fairness”. Contestability mostly relates to reducing strategic and some structural entry barriers while fairness is an issue where the imbalance between gatekeeper and business user deprives the latter of adequate reward for its efforts. In the end, both objectives may be understood with reference to **(long-term) competition in digital markets** among the gatekeepers and between the gatekeepers and entrants. Thus, competition plays a central role at all times, but in a way that the DMA helps to channel or structure it or, in other words, that regulation aims to support and complement market forces to maximise end-user welfare instead of substituting them. Moreover, both objectives are linked and ultimately aim to promote business and end-user choice as well as the degree and the diversity of innovation in the digital economy.
- **Specific effectiveness** relates to the objectives of each obligation which can be measured, as suggested above, with quantitative metrics on the impact of obligations on relations between the gatekeeper and other relevant parties.

Second, the measures taken by the gatekeepers should also be **proportionate**.¹² The application of this principle has several consequences:

- It determines **whether a DMA measure is necessary**, in the sense that the same result might not be possible to achieve through a less intrusive measure. Thus, proportionality limits what the Commission may impose on the gatekeepers to comply with the DMA and how far the gatekeepers should adapt their products and services. Also, the proportionality principle channels the economic analysis that normally underpins an efficiency defence in antitrust (but is not present in the DMA) into a narrower framework and it compels the defendant firm to work within the specific set of core goals of the DMA.
- It also helps the Commission and the Courts to find the right **balance between the different trade-offs** left open within the DMA between conflicting values and interests, such as

¹¹ DMA, Art.8(1).

¹² DMA, Art.8(7).



between openness on the one hand, and privacy, service integrity, IP or user safety, on the other.

- In the same vein, it contributes to **avoiding or mitigating the risks of unintended consequences** of the DMA implementation, in particular, the reduction of innovation and consumer choice which are the ultimate objectives of the DMA. More specific examples mentioned below relate to the risk of collusion by increased transparency in online ads, the risk of unclear and misleading third-party prompts and ‘slamming’ when app stores become more open, or the risk of strengthening the position of the gatekeepers to the detriment of smaller players.
- It also contributes to ensuring **consistency across the different legislations composing the quickly expanding EU digital platforms acquis** and to solving the tension between different laws having different objectives, such as the DMA and the GDPR or the cyber security legislations.

The principle of proportionality will also determine how far **objective justification based on service integrity, security, or privacy**, as allowed in the DMA, can be relied upon by the gatekeepers.¹³

2.2 Increasing Online Advertising Transparency: DMA Article 5(9) and (10) and 6(8)

(a) Legal clarifications needed

The implementation of the provisions about advertising transparency will need to establish the **definition of ‘publisher’**, as it is not defined in the DMA. A useful approach would be to draw on the understanding of ‘publisher’ elaborated in recitals 54-60 in the **Copyright in Digital Single Market Directive**.¹⁴ The term publisher would then refer to firms that invest in the production or acquisition of content and associated rights and have editorial responsibility. A wider definition of publisher that includes others that sell advertising inventory, including social media possibly owned by gatekeepers, for example, could significantly complicate the implementation of these provisions.

The **term ‘metric’** is also not defined in the DMA, which is understandable as ‘metric’ may be defined in numerous different ways, and there is potential for innovation in this area. However, it may still be advisable to **set some parameters** to demonstrate what providing “information on a daily basis on (...) the metrics on which each of the prices, fees, and remunerations are calculated”¹⁵ means. The information should be broad enough to allow the receivers to gain a **thorough understanding of how the prices** have been established and be specific to individual ads without the involvement of personal data. These should allow for comparison across advertisers and across CPSs where multiple services are offered by the same gatekeeper.

¹³ DMA, Art.6(3), 6(4), 6(7), 7(3) and 7(6).

¹⁴ This Directive also fails to exactly define ‘publisher’ among its definitions; however Recitals 54-60 give an indication of what they are understood to be: Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29, OJ [2019] L 130/92.

¹⁵ DMA, Art.5(9)



Through greater transparency, the DMA should facilitate fair and open industry-wide discussions on assessing advertising effectiveness and appropriate performance indicators. Striking the right balance between providing actors in the ecosystem with the information necessary to ensure contestability and fairness, and safeguarding the users of advertisement-supported services will likely **require extensive discussions about what measures of effectiveness are appropriate and what metrics should be used at all.**

(b) Effective mechanisms to implement the obligations

Daily provision of information in most cases should be done **through an API** for it to be useful. There will likely need to be an **experimental phase** during which gatekeepers, advertisers, and publishers try various solutions. Given the history of tensions and power imbalances among these three groups of stakeholders, the Commission may need to undertake a listening exercise afterwards with the intention of setting parameters or issuing guidance.

Giving access to performance measurement tools rather than data can give equitable access to the insight from personal data, where it is used in performance measurement, without further dissemination of user data. **Tools can be made available in a way that benefits smaller publishers and advertisers in the same way as larger ones.** However, there is also a risk that widespread access to gatekeeper performance measurement tools will further solidify the position of certain definitions of performance and data-intensive practices. There is a need for engagement with these tools by advertisers and publishers to spark an industry-wide discussion about methods and approaches to measure performance, independence, and auditability.

As discussed in the issue paper on online advertising transparency, the incentives to consent to share pricing information are not the same for advertisers and publishers. Third-party agents acting on behalf of advertisers will often have separate interests and incentives quite different from the advertiser that has engaged them. Given the level of concentration on the key function of ad-buying and the role that they play combined with the fact that only a few Member States have laws that ensure transparency between them and advertisers, their position in the consent chain merits close attention. **The implementation of these provisions by gatekeepers should be done in a manner that facilitates or even encourages consent from advertisers, publishers, and their agents.** If this does not happen in the short term once the DMA has gone into effect, the Commission might need to develop guidance on the means of getting consent from these businesses.



(c) Avoiding unintended consequences

Sharing pricing information can come with a **risk of collusion**. Trade in advertising that goes through digital gatekeepers is often highly automated and automated systems using machine learning may tend towards collusion, even without communication or instruction, both in pricing strategies and in bidding strategies. Such tendencies might not necessarily trigger antitrust responses, but a balance must be made, and **careful monitoring** will likely be necessary to ensure that fairness and contestability are maintained or established across the various functions in the advertising ecosystems where gatekeepers are involved.

Access to information on pricing and data for independent ad verification will be useful to publishers that have the capacity to process the data and adapt strategy based on the insight gained. This may lead to a **widening gap between larger publishers**, such as those with media holdings in multiple Member States or those with strong positions in large national markets, **and smaller publishers**, such as regional or local media. This **could raise competition and media plurality concerns**. Regulators responsible for media plurality in Member States will need to assess the consequences for smaller publishers once the DMA will have been in force for some time.

More fundamentally, the DMA must include **respect for the principles enshrined in the GDPR**, even in the often data-intensive trade in advertising. The provisions in Articles 5(9&10) and 6(8) should **not be implemented in a way to encourage the further spread of highly targeted and personal data-intensive types of advertising**.

2.3 Switching Tools and Choice Screens: DMA Article 6(3) and 6(4)

The following recommendations relate to issues of scope and probable effectiveness of the default switching elements of Articles 6(3) and 6(4). As these articles are multi-faceted, the focus is on three key clauses:

- Article 6(3.ii) relates to the second sentence of Article 6(3), which relates to the provision of switching tools to facilitate the ongoing ability of end users to change their default settings;
- Article 6(3.iii) relates to the third sentence of Article 6(3), which relates to the requirement of an upfront choice screen for end users to select their default settings;

Article 6(4.ii) relates to the second and third sentences of Article 6(4), which relates to the ability of third-party apps and app stores to prompt end users to switch default, and the ensuing ability of end users to do so.



(a) Legal clarifications of the scope of application

Application of Article 6(3) to non-standard browsers

It seems likely that **search apps and in-app browsers would be classified as browsers**, therefore Article 6(3) should apply to them on that basis. While this may have some benefits for contestability, it also risks being misleading where such browsers do not offer appropriate functionality to be used as default browsers. It may therefore be appropriate for **gatekeepers to place some minimum requirements on what functionality ‘browsers’ must offer in order to be chosen as a default**, but such requirements should be transparent and proportionate.

Application of Article 6(3.ii) to services other than browsers, virtual assistants, and search engines

In our view, Article 6(3.ii) should be interpreted as covering all products or services for which there is a default setting on its operating system, virtual assistant, or web browser, and not just browsers, virtual assistants, and search engines. Mail, Calendar, Maps, and audio player services seem obvious examples.

At the same time, **‘within browser’ defaults should arguably be out of scope**. However, the line between what is effectively part of the browser and what is distinct may well be subject to debate. It would be useful to have clarification on these issues.

Application of Article 6(3.ii) to non-proprietary defaults

While the wording within Article 6(3.ii) is not totally clear, Recital 49 suggests that Article 6(3.ii) is most likely to apply only to those default settings which relate to a gatekeeper’s own proprietary services and **not to defaults where services are provided under contract by a third party**. However, the legal position on this important issue is complex and requires clarification.

In addition, in the specific case of default settings for apps on operating systems, we note that there is also a potential link here with Article 6(4)(i). This requires that gatekeepers enable the ‘effective use’ of third-party apps and app stores with their operating system. One possible interpretation is requiring the easy switching of any relevant default settings within a designated Operating System (albeit this does not apply to default settings within browsers or voice assistants). This requirement is not limited to situations where the gatekeeper has its own rival services. Again, it would be helpful to have more clarity on how Article 6(3)(ii) relates to Article 6(4)(i).

Application of Article 6(4.ii) to pre-installed apps/app stores

Article 6(4.ii) formally applies only to downloaded third-party apps and app stores. As such, it seems to **exclude any apps and app stores that have been pre-installed**, meaning that they would not have the right to prompt end users to switch their default setting to them. However, this seems somewhat at odds with Recital 50. It would be useful to have clarification on this issue.

The issue of multiple ‘access points’

We consider that Articles 6(3) and 6(4) could reasonably be interpreted as requiring gatekeepers to enable end users to choose to **switch a default across all access points at once**, but also – for those



who are keen or for those search engines with more limited interoperability – to enable choices **also to be made separately** for each individual access point.

We consider that this conclusion is relevant to both the ongoing switching tools required in Article 6(3.ii), the initial choice screens for browsers, virtual assistants, and search engines required under Article 6(3.iii), and the ability to switch following a prompt under Article 6(4.ii). It would be useful to have clarification on this issue.

(b) Effective mechanisms to implement the obligations

Design of the Article 6(3.ii) switching tools

It seems reasonable to conclude that, in enabling end users to change their default settings under Article 6(3.ii):

(1) end users should be able easily to **switch to (at least) any alternative option that is currently installed on the user’s device;**

(2) the switching tools should **provide a full list** of the relevant currently installed options;

(3) the gatekeeper should **not be allowed to charge** providers a fee to be ranked higher on this list,

and (4) access to the switching tools should be easy. It would be useful for Commission to confirm whether it supports these conclusions.

The need to be able to reverse decisions

The Commission could consider further the importance of enabling **default switching decisions also to be easily reversed.**

The use of behavioural techniques to inhibit switching or induce switching back

It is likely that the **disproportionate or discriminatory use by gatekeepers of behavioural techniques** – such as prompts and warnings – to inhibit switching, or induce switching back, would be **non-compliant** with the DMA. It would be useful to clarify this.

Timing of initial choice screens

The Article 6(3.iii) wording “end user’s first use” seems most likely to mean that **defaults must be chosen anew with every first use (or installation) on a new device.** However, it would be useful to have clarification on this point.

Payment for access to initial choice screens

It may be reasonable to conclude that gatekeepers should **not charge for access or prominence** on the Article 6(3.iii) choice screens, but it would be useful to have clarification on this point. We note that the DMA is silent on the question of whether the gatekeeper can charge an ongoing fee, or revenue share, to providers who are successful in being chosen.



Choice architecture of the initial choice screen

The Commission should set out its high-level expectations around the **choice architecture of the initial choice screens, and hold the gatekeepers to account in showing how they are meeting these expectations**. In reviewing their submissions, it should seek the input of third parties, draw on the extensive evidence collected by gatekeepers through A/B testing, and potentially require its own testing.

(c) Avoiding and mitigating unintended consequences

The risk of unclear and misleading third-party prompts and ‘slamming’

In designing its user interface to address the risk of end-user harm arising from **misleading third-party prompts and ‘slamming’**, the gatekeepers face a delicate balance. The Commission should meet with gatekeepers and third parties to consider **solutions**. More generally, this is an area that should be kept under review.

The risk of excessive prompts and choice fatigue

Given the clear risk of **‘choice fatigue’** arising from excessive switching prompts by third parties, based on their rights under Article 6(4.ii), it would be useful for the Commission to meet with gatekeepers and third parties to seek **solutions**. More generally, this is an area that should be kept under review.

The risk of harming services with limited market power

Article 6(3.iii) could have the **unintended consequence of requiring the opening up of some default settings to competition where the current service provider is relatively small**, to the potential benefit of their larger rivals. It is not entirely clear how it can be avoided under the existing DMA framework, but the Commission should be alert to this possible outcome and keep the issue under review.

2.4 Prohibition of Self-preferencing: DMA Article 6(5)

(a) Legal clarifications needed

It could be clarified whether Article 6(5) is widely applicable, in the sense that the prohibition of a more favourable treatment of a gatekeeper’s products or services compared to third-party offers **applies both on the end user and the business user side**. We recommend following such a broad interpretation for reasons of effectiveness. A narrow focus on end users would allow a platform as the first-party provider of complementary services sold to sellers to escape the self-preferencing prohibition.

It is unclear to what extent fees associated with rankings are subject to Article 6(5), and if so, whether charging high symmetric fees could be a violation of Article 6(5). It could be clarified whether and to what extent a gatekeeper’s pricing of ranked items falls within the meaning of Article 6(5). While high or differential fees may fall under different provisions of the DMA, **Article 6(5) could be restricted to the design of rankings as a non-price strategy** (which does not preclude the possibility that a third party has to make a payment to be ranked).



(b) Implementation issues

The prohibition on self-preferencing of the DMA requires context. Therefore, the Commission and the Courts should **not apply this prohibition in a mechanistic manner**. Instead, they should identify self-preferencing conducts that are likely to be against the long-term interest of consumers and use guidance from economics to specify adequately the self-preferencing prohibition. That requires understanding when consumers consider a first-party offer superior to similar third-party offers. Giving prominence to a superior first-party offer should not be seen in conflict with Art 6(5), as such behaviour coincides with the one of a gatekeeper who acts in the best interest of consumers.

Platforms can make life difficult for third-party sellers by using price and non-price instruments. Thus, in the context of self-preferencing, an effective policy against foreclosure and refusal to deal may require **a combination of Articles 6(5) and 6(12)**. Specific commitments must be seen in a broader context to avoid circumvention through other means.

2.5 Vertical and Horizontal Interoperability: DMA Articles 6(4), 6(7) and 7

(a) Legal clarifications needed

The **vertical interoperability provision in Article 6(7) is broad**. Therefore, the gatekeeper may receive several access requests for different essential functionalities. To make the provision effective, there should be a process for handling access requests efficiently. One possible approach would be to allow the **gatekeeper to define this process under regulatory oversight**.

The **geographical scope** of the horizontal interoperability obligation should also be clarified, in particular, whether the scope is European (i.e., the obligation only requires that a user in the EU should be able to communicate with any other user also based in the EU) or global (i.e. it requires every user to connect to every other user, including outside of the EU).

(b) Effective mechanisms to implement the obligations

Gatekeepers should be able to define the technical terms of access but follow the **'equivalence of input' when this respects the principle of proportionality**; that is, the entrant should have access to the same functionalities, and on the same terms, as the vertically integrated gatekeeper for its own complementary products and services relying on the essential features. When it is not proportionate, an equivalence of output may alternatively be imposed.

To ensure compliance with those principles, one possibility would be to have a first level of monitoring, where access providers would submit compliance reports, certifying that they satisfy with the principle. In the case of business user complaints, more stringent forms of monitoring (e.g., via audits) could be introduced.

The most appropriate approach for defining access interfaces for interoperability would be to **let the gatekeeper manage access and interfaces** because it has the best knowledge of its services and user interface design, potential risks to integrity, and user security and safety and how those risks evolve over time. In case of complaints and concerns about possible non-compliance, the regulator would investigate the technical specifications of the access interface.



To protect the integrity and security of hardware and software systems, it would make sense to offer access only to players that comply with certain security or privacy standards. **To screen access seekers, access licenses** could be granted based on objective criteria and revoked in case of misconduct. One possible approach would be to allow the gatekeeper to grant access licenses based on public and objective criteria. Another possible approach would be to confer this role to the regulator or an independent third party. Finally, there could be a middle ground where the gatekeeper grants access, but if the access seeker is denied access, it can appeal to the regulator.

(c) Avoiding and mitigating unintended consequences

The DMA provides that interoperability must be provided “free of charge.”, but the precise scope of this principle is not totally clear. To ensure that the implementation of the interoperability sends the right incentives to all parties, we would recommend that, provided that the principle of non-discrimination is respected, the **costs of providing access for the gatekeepers be covered**, at least partly, **by the access seeker**.

Horizontal interoperability may **reduce multihoming**, which is another important driver of contestability. Therefore, the Commission should monitor the extent of multihoming for messaging services following the implementation of the horizontal interoperability provision.

2.6 Data Portability for End Users and Business Users: DMA Articles 6(9) and 6(10)

(a) Legal clarifications needed

The **precise scope of the data** covered by the portability obligations could be clarified, in particular regarding observed data, and whether contextual information in data should also be provided. Specifically, with regard business users’ portability, it could be clarified whether **adversarial portability** is covered.

Several issues related to **user consent for data portability** could also be clarified, especially how granular the consent should be, and whether end-user consent needs to be obtained for each business user or for each core platform service separately. All those clarifications should be consistent with the GDPR rules.

(b) Effective mechanisms to implement the obligations

The implementation of data portability obligations will require the development of **new tools and mechanisms combining data portability with the protection of privacy, security, and service integrity**. Those tools will support the collection of users’ consent and the transfer of the data. It should be clarified whether end-users should rely on the tools provided by the gatekeepers or may also use tools provided by third parties provided security and service integrity is protected. Any such tools would need to take into account the obligations imposed upon data controllers/gatekeepers by the GDPR to verify the identity of an individual before providing access or portability to personal data relating to them. Those tools could also rely on **open standards** and protocols.

The effectiveness of the portability tools could relate to the **availability and performance of the interface** used for data portability. If the availability and performance of the provided interface is low,



then portability cannot be effective. Performance and availability can be benchmarked against the gatekeeper's other consumer-oriented interfaces

(c) Avoiding and mitigating unintended consequences

The obligation to offer tools for data portability to consumers may **crowd out independent Personal Information Management Systems (PIMS)** and therefore reduce competition in the market for data intermediation services.

2.7 Data access for Search Engines: DMA Article 6(11)

(a) Legal clarifications needed

The **precise scope** of data to be shared (with respect to the detail on the query, the search results page, and the user), what is the **scale of data to be shared** (e.g., full or random samples), and what is the appropriate **timeliness of the data** (frequency of updates and recency of the data) could be clarified.

More clarification is also needed on **which platforms could benefit** from the search data access, more specifically, whether the obligation only benefits the general search engines or goes broader as search engine data may be repurposed to innovate and pursue different types of services. In the latter case, search data sharing obligation may provide a stepping stone for entry of new digital firms (not necessarily in the search market) which may ultimately be able to become a sizable competitor and thus increase contestability in digital markets.

The **geographical scope** of the obligation could also be clarified: does it cover only data provided by users in the EU or does it go beyond?

(b) Effective mechanisms to implement the obligations

The gatekeepers, in agreement with the business users and under the supervision of the Commission, could set up a **combination of technical and institutional mechanisms which achieve more contestability through search data access while respecting privacy and security**. Technical solutions cover K-anonymity, differential privacy, and the recent development towards the creation of 'synthetic search logs'. Institutional solutions involve trusted data intermediaries and data sandboxing (*in-situ* data access).

Regarding the **determination of FRAND price**, a mechanism for negotiation between the gatekeeper and search data access seeker could be established and adapted to the technical and institutional mechanisms set up as well as the arbitration between the key rights and interests at play. In particular, this mechanism could clarify what is the process by which data access options are determined (i.e., who can pick data to be provided and how many different access options must be made available) and whether a price of zero could ever be 'fair and reasonable'.



3. RECOMMENDATIONS FOR EFFECTIVE PROCESS AND INSTITUTIONAL DESIGN

(a) Oversight and compliance tools

The **compliance report** is a central feature of the DMA: it is the basis upon which the Commission and third parties can monitor the degree to which gatekeepers comply with their obligations.¹⁶ We recommend that these reports should set out both **how the gatekeeper proposes to modify its conduct so as to comply as well as a demonstration that these measures are likely to prove effective**. In the first instance, this may be achieved by the following means: (i) demonstrating that various options were considered and the one most likely to fulfil the aims of the DMA chosen; (ii) showing that discussions with interested third parties about compliance measures were carried out to test various compliance options; (iii) embedding a regular review of the effectiveness of these measures in the process in collaboration with the compliance officer. The last point suggests that compliance reports should be **living instruments that evolve** as gatekeepers understand how to make compliance more effective and as technology changes. Given the importance of these reports, the **Commission should advise on the form and content** of compliance reports early on to set expectations about their contents in line with the suggestions we have made above.¹⁷

Two procedures exist when gatekeepers are in doubt about how to comply with Articles 6 and 7 obligations: **specification decisions and regulatory dialogue**.¹⁸ While the former is well governed, more detail should be provided about the role and place of the regulatory dialogue. We recommend that dialogue is a less intrusive form of regulation that should occur before starting proceedings for a specification decision. However, the process for dialogue should be transparent and involve third parties.

As already indicated above, to facilitate compliance assessment, the Commission, the gatekeepers, and all other stakeholders could agree on a set of **quantitative measurements, each relating to a particular obligation or obligations**, on the impact of obligations on relations between the gatekeeper and other relevant parties. Those quantitative measures, combined with more qualitative representations from the gatekeepers and their business users would be useful in assessing the compliance with - and the effectiveness of - the DMA obligations.

Powers to require **enhanced supervision**¹⁹ should only be triggered when other enforcement mechanisms do not function.

(b) Responsive enforcement

While the DMA has no hierarchy of enforcement methods, we recommend that an **approach based on responsive regulation should be deployed**. This system relies on assuming that gatekeepers wish to comply and that third parties have a voice in shaping that compliance effort. It follows that the first

¹⁶ DMA, Art.11.

¹⁷ DMA, Art.46(1f).

¹⁸ DMA, Art.8.

¹⁹ DMA, Art.26.



stage is to persuade gatekeepers to comply via regulatory dialogue informed by the views of third parties. If this does not secure compliance, then enforcement can become progressively harsher until the gatekeeper responds to these signals and complies. This means that greater recourse is made to the supervisory measures in the DMA than to the punitive measures.

In the aftermath of a non-compliance decision, the gatekeeper is expected to explain how it proposes to comply. We recommend two things: (i) that these proposals are **market-tested** as a matter of routine; (ii) that the **Commission gives a clear signal** whether the proposal complies with the DMA.

Fining policy²⁰ is likely to emerge incrementally but we **do not recommend issuing fining guidelines in the short term**. It is prudent to facilitate cooperative compliance in the first instance.

Gatekeepers enjoy a series of fundamental rights and are entitled to a good administrative process.²¹ **Secondary legislation to codify procedures is required to ensure fundamental rights protection** and respect for the principles of good administration. Best practices documents can emerge like in antitrust that can accompany procedural rules.

(c) Participatory enforcement and private enforcement

Third-party involvement²² can be enhanced by affording participation at every stage when the gatekeeper is required to design or redesign its compliance efforts – e.g. during the initial phase of writing the compliance report, during regulatory dialogues and procedures leading to a specification decision as well as in the aftermath of a non-compliance decision. At each stage and while protecting confidentiality and business secrets, **the third party should be able to comment on a gatekeeper’s proposal based on clear information**.

Private enforcement is available as the DMA is a Regulation that has direct effect;²³ however, we recommend that **gatekeepers facilitate alternative dispute resolution** with business users for those obligations that deal with the relationship between business users and gatekeepers. The coordination mechanisms set out in the DMA²⁴ to prevent national courts from rendering decisions that may not be in line with the policy of the DMA are the same as in antitrust law and no more can be achieved to prevent divergent decisions. **Claimants may be advised to exercise self-restraint and pursue follow-on actions** – i.e. bring damages claims after a formal finding by the Commission. **Assigning DMA cases to a court specialised** in similar topics in the Member State may be helpful.

(d) Adaptative enforcement

The Commission should **monitor the evolution of the market conditions**, particularly the quantitative measurements on the impact of obligations on relations between the gatekeeper and other relevant parties (as suggested above). This will allow the Commission to determine whether the DMA obligations and the measures taken by the gatekeeper to comply with them achieve their intended

²⁰ DMA, Art.30.

²¹ DMA, Arts. 21, 22, 23, 34, 36.

²² DMA, Art.27.

²³ TFEU, Art.288.

²⁴ DMA, Art.39.



effects. If it is not the case, the Commission may engage in a discussion with stakeholders (gatekeepers, business users, end users ...) to understand why so. This information will allow the Commission to decide whether to adopt the specification of the measure to be taken by the gatekeeper or to open a non-compliance proceeding.²⁵

(e) Institutional design and support by national authorities

National Authorities have a potentially important role to play as sources of information about non-compliance or as investigators assisting the Commission.²⁶ We recommend that **National Authorities make it clear that they are points of contact for complaints** and they could cooperate to agree on how to best facilitate the processing of complaints. Also, as done for banking supervision, the Commission could set up a **joint investigation team** with a staff of the national authorities.

The **DMA high-level group**²⁷ which is the hub between the Commission and several networks of national authorities coming from different legal fields (competition law, consumer protection, data protection, electronic communications, and media) could have the following important tasks: (i) ensuring **consistency in the application of the EU digital acquis**, hence consulted on the interpretation of DMA obligation or assessment of tools for which there is a potential tension between the DMA objectives and rules with other EU rules and objectives (such as privacy, competition, security ...), and (ii) **coordinating the EU and national cases against the gatekeepers**.

²⁵ Resp. DMA, Art.8(9) and Art.29.

²⁶ DMA, Art.37.

²⁷ DMA, Art.40.

cerre

Centre on Regulation in Europe



DMA COMPASS

Alexandre de Stree



TABLE OF CONTENTS

INTRODUCTION: THE NEED FOR AN IMPLEMENTATION COMPASS.....	29
1. OBJECTIVES AND NORMATIVE STANDARD FOR INTERVENTION.....	30
2. CLUSTERING OBLIGATIONS.....	32
3. REGULATORY PRINCIPLES: EFFECTIVENESS, PROPORTIONALITY AND OBJECTIVE JUSTIFICATION	34
4. MEASURING COMPLIANCE	36
5. THE DIRECTION OF EU BIG TECH REGULATION	38



INTRODUCTION: THE NEED FOR AN IMPLEMENTATION COMPASS²⁸

In the course of the Digital Market Act's²⁹ (DMA) implementation, **numerous interpretation issues will be raised and several trade-offs** will have to be decided in the first instance by the Commission or national courts, and ultimately by the Court of Justice of the European Union (EU). More fundamentally, the DMA is establishing a new field within EU economic regulation, and the first interpretation and enforcement actions by the Commission will determine the direction of future EU digital economic regulation.

Those issues will be **particularly difficult to decide** because the DMA regulates technologies and business models which are diverse, fast-evolving, complex and not always fully understood, while the asymmetry of information between regulators and the regulated platforms is massive. Therefore, an **interpretation and implementation “compass” is needed** for the Commission to effectively enforce the DMA, for the gatekeeper to understand how they should comply with the DMA, and for their business users to understand how the DMA can help them enter the digital markets. Calibrating that compass will not be straightforward, given the structure of the DMA. From the higher-level statement of objectives, on the one hand, down to the three key elements of “core platform services”, “gatekeepers” and the list of obligations, on the other, the conceptual chain seems not as strong as it could be. The DMA misses a general definition of core platform services³⁰ and a general clause tying together the list of 22 obligations,³¹ that would link these elements with the objectives. Nevertheless, the compass can be calibrated through deduction from its objectives, some clustering of the obligations, and with the help of regulatory principles that are picked up in the DMA.

²⁸ This issue paper draws on P. Larouche and A. de Stree, ‘A compass on the journey to successful Digital Markets Act implementation’, *Review Conurrences*, 2022/3.

²⁹ Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1.

³⁰ Outside of the operative clauses, Rec. 13 and 14 provide some characteristics of core platform services.

³¹ DMA, Art. 12(5) provides some guidance on the type of practices that would lead to the imposition of supplementary obligations.



1. OBJECTIVES AND NORMATIVE STANDARD FOR INTERVENTION

The DMA has two main overarching aims of “contestability” and “fairness” which are defined in the Recitals of the law.

Contestability is defined as:

*(...) the **ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and service.** (...) This Regulation should therefore ban certain practices by gatekeepers that are liable to increase barriers to entry or expansion, and impose certain obligations on gatekeepers that tend to lower those barriers. The obligations should also **address situations where the position of the gatekeeper may be entrenched to such an extent that inter-platform competition is not effective in the short term, meaning that intra-platform competition needs to be created or increased.***³²

Thus, **contestability mostly relates to reducing strategic and some structural barriers to entry**, thereby facilitating market entry on the demand side (by facilitating switching and multi-homing), and on the supply side (by opening up the data and platforms of the gatekeepers). Note that some structural barriers to entry, such as networks and ecosystems, generate efficiencies that should be taken into account when interpreting and implementing the DMA's obligations.

Unfairness is defined as:

*(...) an **imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage.** Market participants, including business users of core platform services and alternative providers of services provided together with, or in support of, such core platform services, should have the ability to adequately capture the benefits resulting from their innovative or other efforts. Due to their gateway position and superior bargaining power, it is possible that gatekeepers engage in behaviour that does not allow others to capture fully the benefits of their own contributions, and unilaterally set unbalanced conditions for the use of their core platform services or services provided together with, or in support of, their core platform services (...).*³³

At face value, fairness would be a matter of balance in the business-user-gatekeeper relationship. Yet, there must be some limiting feature, otherwise the DMA would potentially cover countless redistribution issues between business users and gatekeepers, even absent any real impact on competition or, more broadly, on welfare.³⁴ Rather, as the above excerpt indicates, **fairness becomes an issue where the imbalance between gatekeeper and business user deprives the latter of**

³² DMA, recital 32. Also DMA, Art.12(5b).

³³ DMA, recital 33. Also, Art.12(5a).

³⁴ Indeed there are situations where firms at different levels of the value chain will argue over the distribution of the total profit to be realised on a given product, without the outcome of that argument having any significant impact on the final user in terms of price or otherwise. In such situations, the final distribution will reflect the relative power of firms, and it is difficult to assess that distribution based on objective criteria. An argument has been made that many FRAND disputes between SEP holders and implementors fit that description, and hence that it was not justified to invest competition enforcement time and resources in these disputes. Schweitzer, supra note 18, also suggests to interpret the fairness objective with reference to competition and cautions against a pure distributional interpretation of this objective.



adequate reward for its efforts. In technical terms, the gatekeeper uses its market power to confiscate producer surplus that would otherwise flow to the business users as a reward for their efforts. Under these circumstances, as the DMA signals, the incentives for business users are adversely affected, especially regarding innovation, with a ripple effect on competition and innovation in the digital economy.³⁵

Thus, both objectives should be **understood with a reference to long-term competition.**³⁶ Moreover, both **objectives are linked**³⁷ and **ultimately aim to promote business and end-user choice, as well as the degree and diversity of innovation in the digital economy.**³⁸ Indeed, the DMA obligations promote, on the one hand, innovation by business users offering complementing services on the regulated platforms and, on the other hand, innovation by disruptive entrants offering alternative services to the regulated platforms.³⁹

³⁵ In the same vein, J. Cremer et al., 'Fairness and Contestability in the Digital Markets Act', Yale Tobin Center for Economic Policy, Policy Discussion Paper 3, 2021, at pg. 6 define fairness as '*the organization of economic activity to the benefit of users in such ways that they reap the just rewards for their contributions to economic and social welfare and that business users are not restricted in their ability to compete.*'

³⁶ H. Schweitzer, 'The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal', *ZEUP*, 2021, at pp. 509-518.

³⁷ DMA, Recital 34.

³⁸ DMA, Recital 32 states that: '*weak contestability reduces the incentives to innovate and improve products and services for the gatekeeper, its business users, its challengers and customers and thus negatively affects the innovation potential of the wider online platform economy.*' Also see Art.12(5b).

³⁹ P. Larouche and A de Stree, 'The European Digital Markets Act: A Revolution Grounded on Traditions', *Journal of European Competition Law & Practice*, Vol. 12, Issue 7, 2021, at pp. 548-552. On the link between contestability, fairness and innovation, see also Cremer et al., *supra*.



2. CLUSTERING OBLIGATIONS

The DMA contains a list of **22 prohibitions and obligations included in three separate provisions** (see the Annex to this note).

- Article 5 enumerates 9 items, mostly prohibitions, which are supposed to be self-explanatory and self-executing;
- Article 6 lists 12 items, mostly obligations, which may require additional specificity by the Commission; and
- Finally, Article 7 adds a horizontal interoperability obligation among communications applications, which requires a phased implementation given its complexity.

Even if the DMA itself does not cluster these prohibitions and obligations, it can be useful to **group them around four categories**. This clustering of obligations allows the link between the objectives of the DMA and its substantive part, as well as the relationship between the individual obligations, to be made more explicit.

1. Preventing anti-competitive leverage from one service to another. This category includes the prohibition of tying one regulated core platform service (CPS) to another regulated CPS, or tying one CPS to identity or payment services, as well as the prohibition of specific discriminatory or self-preferencing practices.

2. Facilitating business and end users switching and multi-homing, thereby reducing entry barriers arising from user demand. This category includes the prohibition of Most Favoured Nation clauses, anti-steering and anti-disintermediating clauses, as well as disproportionate conditions to terminate services. It also includes the obligation to ensure that it is easy to install applications or change defaults, as well as to port data outside of core platform services.

3. Opening platforms and data, thereby reducing supply-side entry barriers and facilitating the entry of complementors, competitors and disruptors. This category includes horizontal and vertical interoperability obligations,⁴⁰ FRAND access to app stores, search engines and social networks, and data access for business users as well as data sharing among search engines on FRAND terms.

4. Increasing transparency in the opaque and concentrated online advertisement value chain. This more specific category includes transparency obligations on price and performance indicators, which are to the benefit of advertisers and publishers.

The first category includes mostly prohibitions that are inspired by competition cases⁴¹ and are hence drafted in a relatively detailed manner. The second and – especially – the third categories include mostly obligations couched in more general terms and sometimes going beyond what could be imposed by way of competition law remedies. Each of these categories points to different aspects of contestability and fairness, as defined above. When the obligations are read together with the

⁴⁰ Resp. DMA, Art.7 for horizontal interoperability and Arts.6(4) and 6(7) for vertical interoperability including side loading.

⁴¹ For a correlation between DMA obligations and antitrust cases, see A. de Streel and P. Larouche, 'The European Digital Markets Act proposal: How to improve a regulatory revolution', *Concurrences*, 2021/2, at pp. 43-63.



corresponding recitals, it becomes apparent that almost all of them relate to contestability, and many of them to fairness as well. The justifications set out in the recitals often blend contestability and fairness, underlining that they are indeed linked and that contestability seems to be the leading objective.



3. REGULATORY PRINCIPLES: EFFECTIVENESS, PROPORTIONALITY AND OBJECTIVE JUSTIFICATION

The third group of elements to calibrate the DMA compass rely on the regulatory principles which will guide the intervention of the Commission.

(a) Effectiveness

Article 8 of the DMA provides for a general **effectiveness principle** by stating that:

1. The gatekeeper shall ensure and demonstrate compliance with the obligations laid down in Articles 5, 6 and 7 of this Regulation. The measures implemented by the gatekeeper to ensure compliance with those Articles shall be effective in achieving the objectives of this Regulation and of the relevant obligation (...)

7. In specifying the measures under paragraph 2, the Commission shall ensure that the measures are effective in achieving the objectives of this Regulation and the relevant obligation, and proportionate in the specific circumstances of the gatekeeper and the relevant service.

Thus, the DMA measures have to be **'effective' in two ways: (i) with regard to the overall objectives of the DMA as a whole and, (ii) with regard to the individual goal of each obligation.** Point (i) is interesting because one can ask questions about the combined effectiveness of all the obligations, but it also shows that the Commission should have some idea of what the overall aim is if it is to apply the DMA properly when reviewing conduct and compliance reports.

Next to this general clause, **some Article 6 obligations specifically refer to the effectiveness** of their implementation. This is the case of (i) access and interoperability of apps and/or app stores (Art 6.4), interoperability for providers of services and hardware (Art 6.7), end-user data portability (Art 6.9), and business user data sharing (Art 6.10).

(b) Proportionality, efficiency defence and objective justifications

The principle of proportionality implies that the **interpretation and implementation of the DMAs obligations should not exceed what is necessary to achieve its objectives.**⁴² Thus, proportionality should play a central role since it provides a template for the Commission to apply and specify the DMAs obligations and decide on the trade-offs left open within the DMA, for instance between openness and privacy, or service integrity, or between business users and end users interests.⁴³ Proportionality will also play a central role when the Court of Justice of the EU will have to judge the Commission's decisions.

⁴² Proportionality is a general principle of EU law: Art. 5(4) TEU which provides that: ' Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties'.

⁴³ DMA, Art.8(7). The companion CERRE issue papers on obligations show how proportionality play a role in specifying the obligations.



The proportionality principle implies that contestability and fairness are accepted as valid core goals, and will be key in deciding whether the DMA measure is necessary, considering whether the same result might be achieved through a less intrusive measure.

A related question is the absence of an efficiency defence in the DMA.⁴⁴ It might be more accurate to say that, in accordance with the avowedly regulatory nature of the DMA, **the efficiency trade-offs have been decided by the legislator and the efficiency defence as it is raised in individual competition law proceedings,⁴⁵ has been replaced with a discussion of proportionality in relation to the measures taken under the DMA.⁴⁶** In other words, any type of “efficiency defence” argument is beside the point, unless it goes to show that the conduct, or the defendant firm, already achieves – in whole or in part – the contestability and fairness objectives as defined in the DMA. The proportionality principle, therefore, allows linking the DMAs objectives directly to its interpretation and implementation. Seen from that perspective, the proportionality principle channels the economic analysis that underpins an efficiency defence into a narrower framework. It also compels the defendant firm to work within the specific set of core goals of the DMA.

While there is no antitrust-type efficiency defence, there are some possibilities of objective justifications. Several Article 6 and 7 obligations explicitly provide for the **possibility of a necessary and proportionate objective justification based on service integrity, security or privacy reasons**. This is in the case of:

- The obligation related to app installation and default setting changes: Art. 6(3);
- Access and vertical interoperability of apps/app stores: Art. 6(4);
- Vertical interoperability for providers of services and hardware: Art. 6(7); and
- Horizontal interoperability obligation: Arts. 7(3) and (6).

More generally, Article 8(1) of the DMA provides that its measures should **comply with several EU laws, in particular regarding privacy and security**. Moreover, some obligations specifically refer to the GDPR requirements,⁴⁷ such as the: prohibition on data combination (Art. 5(2)), provision of data access for business users to data associated with their services (Art. 6 (10)) and access to search data (Art. 6(11)).

⁴⁴ DMA, Rec. 10. Some commentators deplored the absence of any efficiency defence: P. Ibáñez Colomo, ‘The Draft Digital Markets Act: a legal and institutional analysis’, *Jour. of European Competition Law & Practice* 7(12), 2021, at 568 and, for some obligations, L. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. Valletti, M. Van Alstyne (2021), *The EU Digital Markets Act A Report from a Panel of Economic Experts*, Joint Research Center of the European Commission.

⁴⁵ Guidance of 3 December 2008 on the Commission’s Enforcement Priorities in Applying Articles [102 TFEU] to Abusive Exclusionary Conduct by Dominant Undertakings O.J. [2009] C 45/7, paras.28-31. Even though the track record of the efficiency defense in formal litigation is meagre, efficiency arguments are probably more successful at the investigation stage.

⁴⁶ Some of which are more in the nature of a generally-applicable legislative measure than an individual decision.

⁴⁷ Regulation 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 (General Data Protection Regulation), OJ [2016] L 199/1.



4. MEASURING COMPLIANCE

The aim of the various obligations that are introduced by the DMA is to influence and alter the conduct of gatekeepers and, by so doing, to advance the overall objectives of contestability and fairness in digital markets. The impact of any changes in the conduct of gatekeepers on downstream markets will also depend upon the conduct of those who might be affected (for example, users or other firms) and upon other factors which influence market performance and outcomes. Whether a gatekeeper is complying with a particular obligation is therefore a question which can, and no doubt will, be subject to differing views and opinions, but is one on which the Commission will ultimately be required to form a view before deciding whether to take enforcement action.

The **assessment of the** measures taken by gatekeepers and their compliance with the DMA could be approached in two different manners:

- One view is that compliance ought to be assessed with reference to the **processes** that are adopted by the gatekeeper, on the assumption that these processes will influence the gatekeeper's conduct; and
- Another view is that compliance should be assessed with reference to **outputs or changes to competitive conditions and outcomes in the markets** which are likely to be affected by the gatekeeper's conduct, with less attention paid to the processes which underpin these changes.

Views also differ as to whether compliance can be determined by reference to the achievement of outcomes or targets which can be specified in advance or whether conversely, the focus should be on changes to the competitive process irrespective of the outcomes this produces. Other approaches lie between these extremes.

To facilitate compliance assessment, the Commission, the gatekeepers and all other stakeholders could agree on a **set quantitative measurements, each relating to a particular obligation or obligations**, on the impact of obligations on relations between the gatekeeper and other relevant parties⁴⁸. One purpose of such measurements is to provide the Commission with data to inform its compliance assessments. However, if the results were published and the measurements consulted upon and agreed with stakeholders in advance, then these measurements may also allow the gatekeeper to better persuade both the Commission and third parties that the measures it has taken are being effective. Alternatively, they may also assist third parties in demonstrating that a particular set of measures have been ineffective. Gatekeepers might themselves use the measurements to monitor their own compliance and to influence conduct within the organisation. Thus, quantitative measurements would **introduce a degree of objectivity and shared factual understanding even if**

⁴⁸ An example of a measurement regime intended to assess compliance with non-discrimination obligations can be found in the Commission's 2013 Non-Discrimination and Costing Recommendation for telecommunications operators. Paras 19-26 detail how regulated operators should report against certain KPI measures 'to allow for comparison between services provided internally to the downstream retail arm, of the SMP operator and those provided externally to third party access seekers': Commission Recommendation 2013/466 of 11 September 2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment, O.J. [2013] L 251/13. Some of the DMA obligations address similar access concerns, although others have different objectives and would require different approaches to measurement.



interpretation of the measurements and the conclusions to be drawn from them will remain a matter of contention.

These quantitative measurements would not represent specific targets or thresholds against which compliance would be assessed and nor would they attempt to measure the effect of changes in conduct upon market outcomes for users or competition generally. However, they would allow the Commission to better understand how the obligations in the DMA are affecting the conduct of gatekeepers and others in the affected markets and should help identify instances where further investigation might be required in order to assess compliance. Thus, these quantitative measures would be **one signal among other that need to be considered alongside other evidence**, such as complaints or qualitative representations from affected parties, including gatekeepers. Indeed changes - or lack thereof - in market indicators may take place for reasons that may not directly relate to the effectiveness of DMA as a tool. For example, it could be informed by the lack of business user demand for a specific access, the continued popularity and success of a gatekeeper product and its superior quality or wider economic or societal trends.



5. THE DIRECTION OF EU BIG TECH REGULATION

By including (long-term) competition in the analysis at all stages (objectives, obligations and principles), the DMA should complement competition law in order to make digital markets work better and stimulate inter- and intra-platform competition. The **DMA then comes closer to the ‘managed competition’ model** that underpins other bodies of EU economic regulation, such as electronic communications law.⁴⁹ Managed competition implies that competition plays a central role at all times and that the DMA helps to channel or structure it, or in other words, that regulation aims to support and complement market forces to maximise end-user welfare instead of substituting them.

While ‘managing competition’ seems to be the best future scenario for the DMA, two other future scenarios are possible but seem less desirable: fossilisation and gatekeeper entrenchment. In the **fossilisation scenario, the detailed rules of the DMA will be, at best, quickly outdated, and at worst, immediately circumvented**. Ultimately, the DMA would remain a piece of paper in the Official Journal, with much ado about nothing. The risk of fossilisation has been taken seriously by EU lawmakers as the DMA provides for a broad anti-circumvention clause and for the possibility of the Commission to update the obligations with a delegated act (which is akin to a simplified and expedited legislative procedure).⁵⁰ These mechanisms will have to be used effectively now by the Commission to avert fossilisation. Later on in the future, when the DMA will be revised and experience will have been gained, an evolution towards more flexible and standards-based provisions may be conceivable in order to increase the resilience of the DMA in an environment which is moving rapidly.⁵¹

In the **gatekeeper entrenchment scenario, the DMA becomes a kind of all-encompassing ‘public utility’ regulation based on the US model, while the role of competition recedes and fades away**. It is true that, under this scenario, users of the platforms are likely to be well-protected and gatekeeper-user relationships will probably be fair. At the same time, extensive regulation will probably not support entry that could threaten gatekeeper power; rather, it is bound to entrench the gatekeeper position. In other words, the DMA would then protect complementors, but not stimulate market forces to encourage the entry of frontal competitors and diagonal disruptors. This is a scenario that we have seen in some public utilities and from financial sector regulation, where an increase in regulation did not lead to a proportional increase in competition. Given the fact that innovation and competition may potentially be strong in digital markets⁵² and that, when platforms and data are open, the benefit of network and ecosystem effects may be combined with competition, a natural monopoly or public utility type of regulation would not be good future prospects for EU digital regulation.⁵³

⁴⁹ L. Hancher and P. Larouche, “The coming of age of EU regulation of network industries and services of general economic interest” in P. Craig and G. de Búrca, eds., *The Evolution of EU Law*, 2nd ed, Oxford University Press, 2011, pp. 743-781.

⁵⁰ DMA, Art. 12 and Art.13.

⁵¹ A similar evolution has taken place in EU electronic communications law. While the first Directive 97/33 imposing access and interconnection was very much based on detailed rules, since 2002 the successive Directives (2002/21 and now the Electronic Communications Code 2018/1972) are based on broad standards: Hancher and Larouche, *supra*, note 42.

⁵² N. Petit, *Big Tech and the Digital Economy: The Monigopoly Scenario*, Oxford University Press, 2020.

⁵³ Similarly, Schweitzer, *supra*, at p. 542 recommends that the DMA should not be read as, or evolve into, a regime of public utility regulation. In the US, W.P. Rogerson and H. Shelanski, ‘Antitrust Enforcement, Regulation, and Digital Platforms’, *Univ of Pennsylvania Law Rev*, Vol. 168, 2020, pp. 1911-1940, warn against utility regulation-type regulation for the digital platforms and recommend a ‘light-handed pro-competitive regulation’ which is similar to our concept of managed competition.



Annex: List of DMA Article 5 and 6 Obligations and Prohibitions

Art.5	9 Prohibitions-obligations
5(2)	No combination of data from different services or require logging in and identification without user consent sought once p.a.
5(3)	No wide and narrow MFNs/parity clauses
5(4)	No anti-steering : allow business users to communicate w users off the platform, free of charge
5(5)	No anti-disintermediate : allow access and use by end users of services even if acquired elsewhere
5(6)	No prevention of raising issues of non-compliance with public authorities
5(7)	No tying of CPS to ID services, web browser engine or payment services
5(8)	No CPS Tying : no requirements to use other core platform services
5(9)	Online ad transparency for advertisers : provide for ad placed by the advertisers prices and related metrics free of charge on daily basis
5(10)	Online ad transparency for publishers : provide for ad displayed on publisher inventory prices and related metrics free of charge on daily basis
Art.6	12 Prohibitions and obligations
6(2)	No data use in dual role : do not use data about business users to compete with them
6(3)	- Enable un-installing of apps on OS, unless essential to OS/device, - Enable easy changing of default settings on OS, virtual assistance or browser and require initial prompt (at first use) for choice of default search engine, virtual assistant and browser
6(4)	Allow side loading : enable interoperability for third party apps and app store and allow prompts to users to make these defaults, <u>with</u> integrity/security defence
6(5)	No self-preferencing or discrimination in ranking , and related indexing and crawling, services and transparency around ranking criteria
6(6)	No restriction of switching or multi-homing across services accessed via the CPS – device neutrality
6(7)	Access and interoperability for providers of services or hardware to same features of OS or virtual assistant that are available to gatekeepers own services and hardware – free, <u>unless</u> impossible for integrity reasons
6(8)	Online ad transparency : provide performance tools and access to ad data to publishers, advertisers, free of charge
6(9)	Data portability effective, real time, free of charge
6(10)	Data access for business users to data associated with their services , real-time free of charge
6(11)	Data sharing for ranking, query, click and view data (subject to anonymization for personal data) at FRAND
6(12)	Access for business users to app stores, search engines and social networking services at FRAND + Requirement for alternative dispute settlement mechanism
6(13)	No disproportionate conditions or process for termination of service
Art.7	1 obligation
	Horizontal interoperability of basic functionalities for number independent interpersonal communications services



NOTE ON DESIGNATION OF GATEKEEPERS IN THE DIGITAL MARKETS ACT

Richard Feasey



TABLE OF CONTENTS

1. DMA GATEKEEPER DESIGNATION MECHANISMS	42
2. ISSUES TO BE CLARIFIED.....	44
2.1 One Gatekeeper Designation of Multiple Designations?	44
2.2 Same or Different Standards to Rebut the Presumption Based on Quantitative Thresholds?	45
2.3 The Application of Anti-Circumvention Rules	46
3. CONCLUSIONS	48



1. DMA GATEKEEPER DESIGNATION MECHANISMS

The purpose of the designation process is to identify those firms and services that will be subject to the obligations of the DMA.

The first step is to identify the firms providing services that are regulated, who are referred to as gatekeepers (Art 3(1)). A firm will be presumed to be a gatekeeper if it meets or exceeds the following **quantitative thresholds**:

- it has yearly European revenues (from all activities) of over €7.5bn in each of the last 3 years, or an average market cap of €75bn over the last 3 years (Art 3(2)(a) and (c));
- it provides a Core Platform Service (CPS) that has had 45 million monthly active end users in the EU and 10,000 average yearly active business users in each of the last 3 years (Art 3(2)(b) and (c)).

Firms must notify the European Commission within 2 months of meeting these thresholds and the Commission must designate them as a gatekeeper no later than 45 days after this (Art 3(3)). If firms fail to notify then the Commission can still designate on the facts available to them.

Firms must adopt the **definitions of active users and the methodology** for reporting them that is specified in Annex A of the DMA. This states, amongst other things, that different CPSs that are provided and consumed together by users should be assessed separately (that is, active end users for the purposes of Art 3(2)(b) should be counted separately for each CPS, even if they are the same individuals in each case) and that the different commercial services that form part of the same CPS and which may be consumed by the same users should also be assessed separately provided that they are ‘used for different purposes’ (that is, active end users for the purposes of Art 3(2)(b) should be counted separately for each commercial service).

There is also an **‘anti-circumvention’ provision** (Art 13) which prohibits firms from configuring or reconfiguring their services to evade the quantitative thresholds. The Commission can request information to investigate this and can still designate the firm as a gatekeeper of a regulated CPS if it considers circumvention has been attempted.

The European Commission must **review existing designations** of gatekeepers and CPSs every 3 years and consider whether to add new gatekeepers every year (Art 4(2)).

Firms can submit ‘sufficiently substantiated’ arguments as to why, despite meeting all of the quantitative thresholds under Art 3(2), they are **not a gatekeeper** (Art 3(5)). If these are accepted by the Commission within 45 days as ‘manifestly questioning’ the presumption, then the Commission will have a further 5 months to assess the merits of the case in a market investigation (Art 15(3)) and designate or not designate as a result.

The **Commission can designate as gatekeepers firms that do not meet the presumptive thresholds** following a market investigation which must not last more than 12 months (Art 3(8)) and Art 15). The criteria to be applied by the Commission in making such a designation are wide ranging, but the gatekeeper must satisfy each of the three qualitative criteria in Article 3(1) – significant impact on the



internal market, important gateway for business users to reach to consumers (thereby excluding B2B), and entrenched market position. Three or more Member States can also request such an investigation. One circumstance in which the Commission could do this is if the firm in question meets the thresholds but has only done so for a period of less than 3 years and it is expected to meet them in future. In these circumstances the Commission can apply a sub-set of the obligations (Art 17(4)). The Commission could designate on other grounds as well.

The European Commission can, at any time, propose to add or remove services from the list of CPS (as well as adding or removing obligations which will apply to regulated CPS) (Art 19).



2. ISSUES TO BE CLARIFIED

2.1 One Gatekeeper Designation of Multiple Designations?

The DMA defines a gatekeeper as a firm that provides a CPS which has been designated as such (Art 2(1)). **One interpretation is that this means a single firm can be designated as a gatekeeper multiple times, with each designation corresponding to a specific CPS or commercial service that the firm provides.** In this case, a firm may not be a gatekeeper in relation to CPS or commercial service X, but would be a gatekeeper in relation to CPS or commercial service Y. This is implied by Article 3(1), which refers to a firm being designated as a gatekeeper in relation to the provision of a (singular) CPS.

The alternative interpretation is that, once a firm is designated as being a gatekeeper in relation to one CPS or service, there will then be a further and separate question as to which of the various other CPS that the gatekeeper provides should be regulated and added to the list. On this view, the addition of new CPS to the list would not involve a new designation (since the act of designation appears to relate to a decision on whether a firm is a gatekeeper rather than to a decision as to whether a particular CPS should be regulated). Evidence for this approach is:

- The definition of a gatekeeper as a singular undertaking providing core platform services (plural) in Article 2(1), Article 3(8) – which says a firm will be designated as a gatekeeper (singular) but may have a number of CPSs (plural) which are then to be listed pursuant to Article 3(9) –, and Article 15(1).
- Article 4(2), which suggests that the European Commission should review gatekeeper and CPS decisions independently of each other (rather than a review of a gatekeeper designation necessarily involving a particular CPS).
- Articles 5 and 6, which require a gatekeeper to comply with the obligations in respect of each of the CPS listed in the designation decision.

This ambiguity is unhelpful. On the first interpretation, the Commission would need to make a gatekeeper designation each time it wishes to include a new CPS or service within the scope of regulation. On the second interpretation, the existing gatekeeper designation would apply and any new CPS which the Commission wished to regulate would then be added to (or removed from) the list. More substantively, it may affect the implementation of Article 17(4) in cases where a firm is already an ‘entrenched’ gatekeeper supplying a CPS and subject to the full set of obligations and then designated as an ‘emerging gatekeeper’ in relation to another CPS. Article 17(4) refers to a sub-set of obligations then applying ‘to that gatekeeper’ rather than to a specific CPS, whereas the intention is clearly that the sub-set of obligations would apply only to the specific CPS which met the ‘emerging gatekeeper’ criteria and not to other CPSs which that firm may supply and which are already regulated.

We would therefore recommend that the text make it clear (e.g. in Articles 3(8), 3(9), 4(2), 15(1) and 17(4)) that **every decision to regulate a CPS requires a designation that the undertaking in question is a gatekeeper in relation to the provision of that specific service.** This is consistent with the idea that firms will have market power in relation to the provision of a specific service and that market



power with respect to one service does not automatically mean that a firm will also have market power in relation to another. It would also mean that the number of ‘active users’ under Article 3(2)(b) will refer to the users of the specific CPS which is being designated and not to any CPS the firm in question might supply. It would also mean that an undertaking may be the subject of multiple gatekeeper designations, with each being applicable in respect of a different service and each based on a different set of relevant facts.⁵⁴

2.2 Same or Different Standards to Rebut the Presumption Based on Quantitative Thresholds?

Art 3(5) enables firms to submit ‘arguments’ as to why, despite meeting the quantitative thresholds under Art 3(2), they should not be designated as gatekeepers and the CPS or service in question should not be regulated. Art 3(8) provides for the opposite situation, in which the European Commission may designate a gatekeeper despite the firm or CPS in question not meeting the quantitative thresholds under Art 3(2). In this case, the text provides a list of ‘elements’ which the Commission is required to take into account ‘insofar as they are relevant’ when undertaking its assessment.

However, it is not clear whether the intention is for the same evidential thresholds and relevant factors to apply in both situations. Art 3(5) states that exemptions will be ‘exceptional’. This appears to be intended to discourage firms providing CPSs which the DMA is intended to regulate from submitting arguments that they should be exempted and/or to allow the Commission to reject most of those that are submitted. However, it may also serve to limit the number of exemptions which the Commission can make without the risk of legal challenge by interested third parties⁵⁵. In contrast, Art 3(8) does not say that designations of firms that do not meet the quantitative thresholds will be exceptional, and Art 4(2) expressly requires the Commission to review markets every year in order to identify new firms that it should designate under Art 3(8).

Whether designations of firms not meeting the quantitative thresholds will outnumber exclusions of firms that do may depend on whether the Commission applies the same evidential standard to its own assessments under Art 3(8) as it requires from firms submitting arguments under Art 3(5). It may also depend on whether the criteria employed by the Commission in their assessment, which are listed in Art 3(8), are the same criteria that firms are expected to address when advancing ‘substantiated arguments’ under Art 3(5). There are good reasons to think that the same considerations should be relevant to both situations.

⁵⁴ There are two ways in which ‘conglomerate effects’ might still be taken into account in the designation. First, in quantitative terms the market capitalisation and revenues of the firm (Art 3(2)(a)) will reflect the totality of its activities and not just the individual CPS service for which the firm is designated a gatekeeper. Second, in qualitative terms, Art 3(8) allows the Commission to have regard to conglomerate effects derived from other activities in the assessment, including those that might be obtained from prospective acquisitions. This aside, each service is assessed separately.

⁵⁵ The inclusion of the term ‘exceptionally’ in Art 3(5) is unsatisfactory in the sense that it seems to prejudge how often firms that meet the quantitative criteria might nonetheless prove not to be gatekeepers. This could only be determined after considerations of the facts, rather than being something that could be predicted in advance. Even if the standard of proof is very high, it is still possible that a significant number of services might reach it.



As regards evidential standards, Article 17 would seem to envisage the European Commission undertaking a similar form of market investigation when arguments for exemption have been accepted under Art 3(5) and when the Commission proposes to designate under Art 3(8). The reference in Art 3(5) to whether a firm has presented ‘sufficiently substantiated arguments’ in favour of exemption relates only to the decision of the Commission as to whether or not to proceed to the next step of initiating a market investigation and *not* to the outcome of that investigation. In other words, the presumption in favour of designation if a firm meets the relevant quantitative thresholds affects the likelihood of the Commission being persuaded to undertake a market investigation. This is so presumably in order to reduce the risk of the Commission finding itself otherwise obliged to devoting valuable resources to market investigations when it is already clear that the firm in question is a gatekeeper for the purposes of the Act, and the investigation will simply delay compliance and add uncertainty into the regime. That said, the question of what constitutes a ‘sufficiently substantiated’ argument for the purposes of moving to a market investigation under Art 3(5) seems likely to be litigated.

Once the Commission has decided to proceed to a market investigation then it would seem appropriate that the assessment would be undertaken by the Commission adopting the same evidential standard as it would apply to any other market investigation, including an investigation undertaken pursuant to Art 3(8). At this stage of the process, therefore, the standards for exclusion of a firm meeting the quantitative thresholds or inclusion of firm that did not meet the thresholds ought to be the same. Having said this, the Commission will have only 5 months in which to assess whether a firm meeting the quantitative thresholds should be excluded from designation but 12 months in which to assess whether a firm not meeting the thresholds should be included. Although there is no a priori reason to think that a decision to exclude a firm from designation would require less evidence, or evidence to a lesser standard, than a decision to include a firm, the difference in timescales must have some practical implications for nature of the assessment which the Commission is able to undertake.

2.3 The Application of Anti-Circumvention Rules

The intention of the anti-circumvention provisions of Art 13 in addressing strategic behaviour by firms and preventing the ‘slicing and dicing’ of services to evade regulation is clear. At the same time, however, Annex A appears to encourage or at least accept such ‘slicing and dicing’ by accepting that firms may offer different commercial services which may each form part of the same CPS and be provided to the same set of users, and allowing each to be reported, assessed and designated separately provided they are used for ‘different purposes’.

In order to address strategic behaviour, therefore, the Commission will either need to show that commercial services within the same CPS class are not, in fact, being used for ‘different purposes’ and users of these services should be aggregated together for the purposes of Art 3(2)(b), or that the motive for disaggregating services was to evade regulation rather than for some other legitimate commercial purposes, such as responding to changes in user preferences or competition. This may prove challenging: internal documents may assist in answering the latter question, but regulated firms may anticipate this, and motivations for changing commercial practices may be complex. Whether



two services are being used for a different or the same 'purpose' by users is likely to become a contested question and something which may also be capable of being influenced by the firms themselves.



3. CONCLUSIONS

We recommend that the European Commission clarify that **every decision to regulate a CPS will require a designation that the undertaking in question is a gatekeeper in relation to the provision of that specific service** and that, accordingly, references to ‘active users’ for the purposes of gatekeeper designations are references only to users of the CPS in question.

We recommend that the Commission confirm that it will **apply the same evidential standards in market investigations considering whether to exclude a firm that otherwise meets the quantitative thresholds for gatekeeper designation as in market investigations considering whether to include a firm that otherwise does not meet the same quantitative thresholds**, subject to the practical constraints that arise from differences in the timescales available to the Commission to complete its investigations.

The **application of Annex A, with the possibility that services provided by the same firm within the same CPS category may be assessed separately for gatekeeper designation if they are used for ‘different purposes’, will need to be clarified through specific cases**. The Commission will want to ensure that firms do not abuse this provision in order to evade designation.

cerre

Centre on Regulation in Europe



DMA TRANSPARENCY REQUIREMENTS IN RELATION TO ADVERTISING

Sally Broughton Micova



TABLE OF CONTENTS

INTRODUCTION	51
1. THE DMA OBJECTIVES	52
1.1 The Advertising Ecosystem.....	52
1.2 What the DMA is Trying to Achieve	52
2. TRANSPARENCY IN TRANSACTION INFORMATION.....	54
2.1 The DMA Obligations	54
2.2 Interpretation and Implementation Issues to be Clarified	58
2.2.1 What is an advertisement and what is a publisher?	58
2.2.2 How will consent be managed?	58
2.2.3 What will getting ‘metrics’ mean?	59
3. TRANSPARENCY IN PERFORMANCE MEASUREMENTS	61
3.1 Obligations and Their Possible Impacts.....	61
3.2 Interpretation and Implementation Issues to be Clarified	63
3.2.1 Whose performance is this about?	63
3.2.2 What will constitute a request and how will they be handled?	64
4. OVERARCHING ISSUES	65
5. CONCLUSIONS	66
REFERENCES	67



INTRODUCTION

In the years preceding the adoption of the Digital Markets Act (DMA), market investigations in the UK and Australia by competition authorities found problematic concentration of platform power and anti-competitive situations in online advertising (Australian Competition and Consumer Commission, 2019; Competition & Markets Authority (CMA), 2020). The French competition authority took up a case against Meta over the withdrawal of APIs to third party ad tech providers, eventually receiving concessions.⁵⁶ The US Department of Justice launched a suit against Google in relation to search advertising.⁵⁷ The European Commission launched a formal anti-trust investigation into anti-competitive behaviour by both Google and Meta in the market for online display advertising in early 2022⁵⁸. There had been mounting evidence from academics as well of various problems of concentration in the market for online advertising (Andreou et al., 2019; Broughton Micova & Jacques, 2020b; Geradin & Katsifis, 2019). Issues were identified with lack of transparency, unfair data-driven advantages, conflicts of interests and dependencies at crucial points in the ecosystem.

The DMA aims to address some of these problems in relation to gatekeeper undertakings. It contains measures directly related to the problems of opacity in the trade of online advertising and in the measurement of its effectiveness. This issue paper covers these measures, which are contained in Articles 5 and 6 of the DMA. It begins with a brief overview of the online advertising ecosystem. The paper then elaborates the aims of the DMA as indicated in the recitals and provisions. It later takes in turn each of the provisions of the DMA related to transparency in online advertising, first addressing those related to transaction in Articles 5(9) and 5(10) and then those related to performance measurement in Article 6(8). Finally, it provides an interpretation of each of the provisions and identifies some outstanding questions to be dealt with in implementation.

This paper argues that there are crucial definitions to be established, namely of advertisement, publisher, and metrics, and that how these are defined will have significant implications for the effects of the DMA. It also points out that questions need to be answered about how the consent of advertisers and publishers will be managed, how they will be enabled to make requests for access to measurement tools and data, and how they will receive data. The potential to improve contestability and fairness in the advertising ecosystem could be stymied by overly cumbersome processes for consent or requests, or by ineffective delivery of the information that is supposed to be made transparent. This paper also highlights two overarching issues, one related to the designation of gatekeeping services and the other arising from the role that personal data processing plays in some of the information due to be made more transparent. In conclusion it argues that, with user fairness considerations at the forefront, the implementation of the advertising transparency requirements in the DMA could encourage industry-wide re-evaluation of measures of value and effectiveness and a move away from personal data-intensive types of advertising.

⁵⁶ See: <https://www.autoritedelaconurrence.fr/en/press-release/meta-makes-commitments-autorite-de-la-concurrence>

⁵⁷ See: <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>

⁵⁸ See: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1703



1. THE DMA OBJECTIVES

1.1 The Advertising Ecosystem

As has been argued in an earlier CERRE report (Broughton Micova & Jacques, 2019) and other scholarly work (Broughton Micova & Jacques, 2020a; Eisenhardt et al., 2018; Stallone & Klaas, 2019), the trade in advertising takes place within a **highly complex ecosystem of demand actors, suppliers, intermediaries and other services**. Efforts to visualize this either as interconnected value chains (Adshead et al., 2019) or as evolving ecosystems (Gusic & Stallone, 2020) have shown that some undertakings are present in multiple parts of these ecosystems, and may tend towards aggregation or consolidation.

The DMA specifically classifies online advertising services as a type of core platform service, including any advertising networks, advertising exchanges and any other advertising intermediation services, if they are provided by an undertaking that also provides any other core platform service. Nevertheless, nearly all the other types of core platform services identified in Article 2 of the DMA also have some role to play either as the supplier of the inventory (search engine, social network, or video-sharing platform) or as a service through which data is gathered that feeds into advertising (web browser, virtual assistant). Several functions must be fulfilled for advertising to be purchased and delivered to an end-user:

- inventory provision;
- inventory sale (reserve & auction);
- auction management & execution;
- ad verification;
- optimization & planning (including re-targeting, which requires 1st party data);
- ad serving;
- performance tracking.

The importance of consumer data in this ecosystem has been well evidenced (Boerman et al., 2017; Bourreau et al., 2017; Competition & Markets Authority (CMA), 2020), but transactional data and increasingly contextual data related to the content around advertising inventory are also crucial to some functions and types of advertising and thus are also of considerable value (Broughton Micova & Jacques, 2020b; Krämer et al., 2020). Access to these types of data is highly uneven, however. There is a clear **lack of transparency in transaction data and performance data** that makes it difficult for advertisers to “exercise choice effectively” (Competition & Markets Authority (CMA), 2020, p. 16), and for publishers to understand and represent the value of their inventory (Broughton Micova & Jacques, 2020b; Jeon, 2021). The DMA contains provisions intended to increase transparency in the transactions that take place in the advertising ecosystems and in the measurement of performance.

1.2 What the DMA is Trying to Achieve

The DMA has two overarching aims: contestability and fairness.

Contestability – The DMA aims to rectify weak contestability where, according to Recital 13 “extreme scale economies, very strong network effects, an ability to connect many business users with many



end users through the multi-sidedness of these services, lock-in effects, a lack of multi-homing or vertical integration are the most prevalent.” Theoretically there should be adequate contestability across all the advertising functions listed above. The DMA should therefore facilitate rivalry among firms and market entry in the provision of each function. This requires firms wishing to provide a service to be able to access the information that serves as the raw material for the function that service would provide. For example, both ad verification and campaign optimization require data that is generated at the point where an ad is served to an end user. Firms wishing to compete as ad verification services or agencies providing campaign planning and optimisation need continual access to that data (Jeon, 2021). Contestability in the functions performed in the advertising ecosystem also requires firms to be able to make informed choices. For example, inventory holders need to have a choice of auction services and ad servers with which to partner, and must be able to access information upon the basis of which to make that choice among providers.

Fairness – As stated in Recital 7, the DMA is concerned with fairness for both end users and business users. The concern comes from the fact that certain core platform services have “gained the ability to easily set commercial conditions and terms in a unilateral and detrimental manner for their business users and end users.” The aim here is to enable fair conditions for marginal decision-making by business users and end users. Business users need to be able to access the information necessary to assess the fairness and value of their commercial relationships with core platform services. For example, an advertiser should be able to decide how to allocate its budgets across ad networks. End users should also be treated fairly in relation to conditions of use. For example, they should not receive poorer quality service if they refuse to consent to data collection for the purposes of advertising, as set out clearly in the Act. Fairness towards the end user would also be informed by the principles set out in the GDPR. End users should be able to understand what personal data is being collected and for what value-creating purpose, and only the minimal data required should be gathered.

Articles 5 and 6 of the DMA set out transparency requirements for information about the transactions involved in the trade in advertising and information necessary for the measurement of performance within the ecosystem. The next sections discuss each of these in turn and raise some issues with each that should be considered in the implementation and enforcement of the Act.



2. TRANSPARENCY IN TRANSACTION INFORMATION

2.1 The DMA Obligations

Article 5 of the DMA sets out the general obligations on gatekeepers. Both 5(9) and 5(10) below deal with the transparency of financial information generated in the trade of advertising.

Article 5(9)

The gatekeeper shall provide each advertiser to which it supplies online advertising services, or third parties authorised by advertisers, upon the advertiser's request, with information on a daily basis free of charge, concerning each advertisement placed by the advertiser, regarding:

- (a) the price and fees paid by that advertiser, including any deductions and surcharges, for each of the relevant online advertising services provided by the gatekeeper,*
- (b) the remuneration received by the publisher, including any deductions and surcharges, subject to the publisher's consent; and*
- (c) the metrics on which each of the prices, fees and remunerations are calculated.*

In the event that a publisher does not consent to the sharing of information regarding the remuneration received, as referred to in point (b) of the first subparagraph, the gatekeeper shall provide each advertiser free of charge with information concerning the daily average remuneration received by that publisher, including any deductions and surcharges, for the relevant advertisements.

Article 5(10)

The gatekeeper shall provide each publisher to which it supplies online advertising services, or third parties authorised by publishers, upon the publisher's request, with free of charge information on a daily basis, concerning each advertisement displayed on the publisher's inventory, regarding:

- (a) the remuneration received and the fees paid by that publisher, including any deductions and surcharges, for each of the relevant online advertising services provided by the gatekeeper,*
- (b) the price paid by the advertiser, including any deductions and surcharges, subject to the advertiser's consent; and*
- (c) the metrics on which each of the prices and remunerations are calculated.*

In the event an advertiser does not consent to the sharing of information, the gatekeeper shall provide each publisher free of charge with information concerning the daily average price paid by that advertiser, including any deductions and surcharges, for the relevant advertisements.



The table below breaks down the provisions, showing what information it ensures for the demand side and the supply side of advertising respectively and where the consent of either is required.

Table 1: Breakdown of the provisions in Article 5(9) & 5(10) of the DMA

INFORMATION GIVEN TO ADVERTISER OR AUTHORISED 3RD PARTY	INFORMATION GIVEN TO PUBLISHER OR AUTHORISED 3RD PARTY	CONSENT?
The price and fees paid for each advertisement including deductions and surcharges	The remuneration received and the fees paid by that publisher for each advertisement displayed, including any deductions and surcharges	No consent required
The remuneration for each advertisement received by the publisher, including any deductions and surcharges	The price paid by the advertiser for each advertisement displayed on the publisher's inventory, including any deductions and surcharges	Consent required from publisher for remuneration data and advertiser for price paid data
The metrics on which each of the prices, fees and remunerations are calculated	The metrics on which each of the prices and remunerations are calculated	No consent required
The daily average remuneration received by that publisher for an advertiser's advertisements	The daily average price paid by that advertiser, including any deductions and surcharges, for advertising on that publisher's inventory	No consent needed – This is the alternative offered if consent is not given where needed.

As can be seen in the table, these two provisions will give advertisers and publishers equivalent access to transaction information, if consent is given on both sides. However, **each of these groups of business users of core platform services would use or derive value from this information slightly differently.**

For advertisers, or the media agencies working on their behalf, having the detailed information on the prices they paid per ad is **important for campaign planning and optimisation** as it is an important measure of efficiency. Media agencies, the likely authorised third parties, would normally already have access to this information across all their clients, though not necessarily in real time. In some jurisdictions there are transparency requirements governing the relationships between advertisers and their media agencies. The Sapin Law, for example, ensures this in France and could contribute to the effectiveness of this provision, but the relationships between advertisers and their authorised third parties are outside the scope of the DMA. Combining price paid with information on the remuneration received by the publishers will allow advertisers to see the cost of the intermediation involved in the placing of advertisements. For some advertisers this might be used as a measure of efficiency, for instance in order to calculate how much of their ad spend is going to various



intermediaries. The concentration among intermediaries on the buying side has been documented as well as the consequences for advertisers (Decarolis & Rovigatti, 2021). However, the advertisers would not necessarily be interested in how much any given publisher receives.

Whether seeing how much of their advertising spend is extracted between the price paid and the remuneration received would lead advertisers to change routes to those publishers will firstly depend on whether alternative routes are available and secondly on whether there is sufficient competition and fairness towards publishers. If the power dynamics between a core platform service and publishers allows the platform service to extract the lowest price for the inventory, which could even be under cost, then going through a gatekeeper's core platform service will still result in a lower price paid by the advertiser. The advertiser will then have no incentive to choose an alternative route that allows a higher percentage to reach the publisher.

Information on the metrics used to calculate prices could be invaluable to advertisers for the marginal decision making involved in assessing and planning campaigns, which would encourage fairer competition in the supply of inventory and possibly among the exchanges and brokers involved in executing auctions. The latter will depend on how widely the term 'metrics' is interpreted, and whether it captures the situations in which price is not so much calculated as it is the result of a bidding process, in which the intermediary may be using different metrics for demand and supply sides. For example, Google Ads sometimes uses cost per click (CPC) to charge advertisers, but cost per impression (CPM) to pay publishers. Also, the price paid at auction is often not the highest bid, which means that information on the final price paid may blur the actual value of the inventory. In order for an advertiser to assess efficiency and fairness in a second price auction, for example, it would need to know all the other bids, their sources, and granular details on the ad. A wide and detailed approach like this has been proposed in the US to encourage competition in digital advertising.⁵⁹ **Giving advertisers and their representatives sufficient level of detail has the potential to enable them to identify unfair practices and generate evidence for competition-related complaints.** Experiments with the bidding behaviour of learning algorithms, which are frequently used by large buying agents, have shown that the effects of the nature of ad trading auctions and amount of feedback information received by the bidding side can vary in terms of the prices achieved and the potential for tacit collusion (Banchio & Skrzypacz, 2022; Decarolis et al., 2022). **A delicate balance will have to be achieved** and monitoring put in place to ensure that the level of detail does not enable collusion or other unfair practices too.

The term 'publisher' is not defined in the DMA, which is a significant gap. If it refers to all those selling advertising inventory through core platform services it could include a variety of different business users, from a local non-news website to a major newspaper group or broadcaster. It could

⁵⁹ The Bill to prevent conflicts of interest and promote competition in the sale and purchase of digital advertising proposed in the US Senate would require data "(II) for each identifier [unique to advertising space] described in subclause (I), all bids received, and, for each bid received, the bid submitted to the digital advertising exchange on behalf of the buy-side brokerage customer, the winning price, the uniform resource locator or other property identifier at the lowest level of granularity, the identity of the digital advertising exchange or other digital advertising venue returning the bid, date, time that the bid response was received in microseconds or a lower level of granularity, web domain associated with the advertising creative, the advertising creative size and format, and whether the bid won the seller's impression". See: <https://www.congress.gov/bill/117th-congress/senate-bill/4258/text>



also include social media, comparison or niche search services, or even marketplaces, owned by the same provider as the core platform service. Such a wide definition of publisher would include a vast number of small inventory holders that would have little, if any, capacity to make use of the data these provisions would allow them to request and so would not be likely to request this data. It therefore makes sense for the purpose of this discussion, and arguably the DMA's implementation, to **assume a narrower definition** of publisher akin to the way the term is used in the Copyright Digital Single Market Directive⁶⁰, describing firms that invest in the production or acquisition of content and associated rights and have editorial responsibility.

For such publishers, mainly audiovisual media and press publishers, having data on the prices paid by advertisers, including any surcharges and discounts, for their inventory would be invaluable. If they **are able to effectively combine it with the information on their own remuneration using unique identifiers, it would allow them to assess the efficiency and fairness of core platform services**. If there are alternatives, they could potentially compare and chose the best option based on the % of the paid price that they receive, enabling fair competition in the sale and auction functions among supply side platforms, ad exchanges, and other intermediaries. Those core platform services not provided by designated gatekeepers would arguably have an incentive to provide equivalent information to the publishers even though they would not be obliged to do so in order to be competitive. Large publishers with the capacity to process and utilise large amounts of such data for pricing and inventory planning would likely derive the most benefit.

Information on the metrics on which prices and remuneration are calculated will be useful for publishers in a similar way as it would be for advertisers. Metrics can be more than whether a price is calculated on click or impression, it would also be how a click or an impression is determined. Value determining information could also include the format, the number of total impressions available, and the type of data used for targeting, if any. This is particularly important for publishers who have been using core platform services operated by companies that also operate social media or video-sharing platforms that compete with them in the provision of inventory. **Metrics of sufficient breadth, granularity, and timeliness could enable publishers to compare intermediary services and to identify any unfair practices**, especially in programmatic trading and auctions. However, it may also allow publishers that also sell directly to advertisers to compare the data they have from direct sales with the prices advertisers are willing to pay for certain conditions through the gatekeeper.

Where large publishers use automated systems with learning capacity there are **risks that these will tend toward tacit collusion** (Calvano et al., 2020), or that the advantages they gain from the additional information will further widen the gap between them and smaller publishers. Competition authorities will need to monitor closely the way this information is used by publishers in advertising markets more widely, and regulators responsible for media plurality will need to assess the consequences for smaller publishers.

⁶⁰ This Directive also fails to exactly define 'publisher' among its definitions, however Recitals 54-60 give an indication of what they are understood to be: Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29, OJ [2019] L 130/92.



This account of how transaction information might be used by advertisers and publishers contains a number of “ifs”. The DMA leaves several important questions unresolved, that will need to be attended to in the implementation in order for these provisions to be effective in achieving contestability and fairness.

2.2 Interpretation and Implementation Issues to be Clarified

2.2.1 *What is an advertisement and what is a publisher?*

These two questions are linked because a clear definition for one could indicate the definition of the other. An advertisement could be a paid for ranking or prominence such as on Booking.com results or in Amazon’s ‘buy box’. It could also include promotion by a game streamer arranged through Twitch’s ‘Bounty Board’, a branded filter in Instagram, or another form of what the Audiovisual Media Services Directive⁶¹ defines as ‘commercial communication’ but that is not inventory provided by a press publisher or audiovisual media. If the term advertisement is to be understood in a very comprehensive way, it could imply that the term publisher would be similarly understood, and not necessarily in the way discussed above.

One thing that does seem clear in the DMA, however, is that the **term advertisement does not only refer to openly traded display advertising**. The annex to the DMA for designation of gatekeeper status for online advertising services explicitly gives a measure for ‘active end-users’ and ‘active business users’ for both proprietary sales of advertising and services that operate open trading. The transparency requirements in Article 5(9) and (10) are not so important for those large services whose advertising is sold only through their own proprietary trading systems as they already have access to all of the transaction data covered by these provisions. However, if implemented forcefully the requirements **could be very meaningful for advertisers and for those ad inventory sellers who compete with large platforms in the provision of inventory**.

2.2.2 *How will consent be managed?*

Advertisers will only have an interest in the information on publisher remuneration if it helps them reduce the costs and improve the efficiency of their advertising overall, and have little or no incentive to consent to allowing publishers to see their price paid information. The business of media agencies has historically been in arbitrage, and they continue to make income off the difference between what they pay for advertising and what they charge their advertiser clients. They will have little interest in encouraging or facilitating advertiser consent to the release of transaction data to publishers or vice versa. Publishers would have an incentive, or at least no disincentive, for giving consent to the sharing of data on the remuneration they receive, and would likely derive the most benefit from getting access to advertisers’ price paid data. Whether it is in the interest of the core platform services managing the request and consent processes to make those processes easy or cumbersome may depend on whether

⁶¹ Directive 2010/13 of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ [2010] L 95/1, as amended by Directive 2018/1808



it is also trading ad inventory from other services it provides or it is engaged in other parts of the ecosystem.

For the provisions in Article 5 on transaction transparency to be effective, these incentives will need to be balanced out in the implementation of consent for the release of the data on both sides. As has been seen with the implementation of the e-privacy Directive⁶², and even to some extent GDPR,⁶³ consent processes can be designed so as to render the policy essentially meaningless and even frustrate users (Fassl et al., 2021; Sanchez-Rola et al., 2019). **Article 5 of the DMA does not require end user consent, but the consent of the business involved in the trade.** The data released should not be personal data, but transaction related non-personal data. In the implementation of the DMA **steps should be taken to ensure that the processes for making requests and giving consent are designed to encourage both.**

For example, could they be automated and or integrated into the buying and selling process? Could they be made on a regular basis, perhaps annually, as a blanket consent, rather than ad hoc for individual campaigns or trades? A daily average is considerably less useful for both sides, especially for the marginal decision-making that could encourage competition among inventory holders and online advertising services. The aims of improving contestability and fairness withing the advertising ecosystem will only be served if most transaction data is shared, if essentially the default is that advertisers and publishers both consent and receive the data.

2.2.3 What will getting 'metrics' mean?

This question addresses two issues, the first of which is determining the kind of data that will qualify as 'metrics', and the second of which is the way the metrics will be made available. Without clarity on the first, there is a danger of the implementation of this provision being at odds with the principle of minimization of personal data use. Prices for online advertising can be determined through a variety of ways depending on the type of advertising and the purchasing pathways used (Broughton Micova & Kostovska, 2021), some of which rely on personal data. Display advertising alone can be traded through open auction, in which case the price is determined by the bidding process such as in the example above, or through premium channels where prices may be determined by the characteristics of the inventory and/or the targeting criteria. As with the old arbitrage systems for offline advertising, prices, discounts, or rebates can also depend on volume and duration. It may be that not all the possibilities are relevant to the kinds of undertakings likely to be designated gatekeepers, however there should be a wide enough understanding to cover the variety of information used to determine pricing, from the granular bid data from auctions to the viewability and geolocation characteristics feeding into premium buys. Where price determination may involve the processing of personal data generated by users, it will be vital that this data is not shared.

⁶² Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ [2002] L 201/37 as amended by Directive 2009/136.

⁶³ Regulation 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 (General Data Protection Regulation), OJ [2016] L 199/1.



Metrics that are consistent and comparable are most useful for encouraging contestability and fairness, as trends can be identified and services compared. However, industry standards remain somewhat patchy. Viewability criteria have been defined in various ways to suit the players who have the power to define them, and there has been little interest in standardisation (Expósito-Ventura et al., 2021). Though efforts have been made to produce guidelines on impressions and accredited measurement services, these seem to skip over bigger questions about what effectiveness actually is, and whether ever more granular, and arguably invasive “measurement” is merited.

The DMA states that metrics should be provided for free, on a daily basis and for each advertisement. This could come in a form that renders it pretty much useless or it could be provided in forms that are appropriate to the type of data and that make it useable to the receiver. **For most of the data, the most appropriate mechanism would be for it to be provided through an API. The metrics data would also need to be linked to unique identifiers** for the ads (not the users), or at least for the transaction in order to be very useful to publishers for assessing and demonstrating the efficiency of their ad inventory. They would need to be able to connect price, price-determining metrics, and other performance data by advertiser and across core platform services when multiple are provided by a single gatekeeper.



3. TRANSPARENCY IN PERFORMANCE MEASUREMENTS

3.1 Obligations and Their Possible Impacts

Article 6 of the DMA contains a provision that obliges gatekeepers to give advertisers and publishers, or third parties authorised by them, access to performance measuring tools and ad verification related data.

Article 6(8)

The gatekeeper shall provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, upon their request and free of charge, with access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data. Such data shall be provided in a manner that enables advertisers and publishers to run their own verification and measurement tools to assess the performance of the core platform services provided for by the gatekeepers

Unlike in relation to transactional data, there is no consent required in this provision. The performance measuring tools will rely on data collected by the gatekeeper through its core platform service(s) as first party data or data from third parties. Where the advertising business model is heavily reliant on targeting and user behaviour tracking, measurement tools will involve processing personal data. In such cases, the consent relevant to this data is that of the end user, whose interaction with the ad and other behaviour online generates it. The gatekeeper manages this end user consent, which cannot be assumed on the basis of engagement with an ad.⁶⁴

According to this provision, if they request it, advertisers, publishers, or their authorised third parties will be given access to:

- performance measuring tools of the gatekeeper; and
- the data necessary to carry out independent ad verification.

As stated in the provision, the purposes of the access are to enable them to:

- run their own ad verification; and
- assess the performance of the core platform services.

The Interactive Advertising Bureau (IAB), Europe's leading industry association promoting digital advertising, defines **ad verification** as: "a process which attempts to verify that one or more attributes of a served online ad have been executed in a manner consistent with the terms specified by the advertiser or agency and agreed to as part of the ad campaign terms" (IAB, 2012, p. 5). Terms can include placement conditions such as targeting related user characteristics or contextual conditions such as avoiding children's content. They can also include a variety of delivery characteristics such as

⁶⁴ This is made clear in the EDPB's guidelines on the targeting of social media users https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf and in the Article 29 Working Party Opinion on profiling and automated decision making, which confirms that consent must be explicit and that 'legitimate interest' cannot be used to justify the use of this data <https://ec.europa.eu/newsroom/article29/redirection/document/49826>.



those aimed at combatting bot-related fraud or those that determine the quality of the ad impression, such as viewability or sound quality. Ad verification does not have to require user tracking and extensive personal data, but often does.

This information is important to advertisers and their agencies for ensuring that the terms for the purchase of advertising inventory are being met. It allows them to assess the quality of the online advertising services through which their campaigns are being executed, particularly the ad servers that deliver the advertisement in front of the end user. Advertisers and their agencies tend to get this information already directly from core platform services or from third party ad verification providers. Several verification providers already have special relationships with core platform services that give them access to the necessary data through the consent obtained by the core platform service. The provisions of Article 6(8) have the potential to open this up and perhaps inspire more advertiser focus on alternatives to user data intensive practices.

Publishers also value the data used for ad verification, as such data would allow them to see how their inventory is being perceived by those on the demand side. They would be less interested in the individual verification of ad placements as they would be in the trends and tendencies associated with their inventory. It is not in their interest to allow fraudulent impressions or poor viewability as it devalues their inventory. Publishers would derive great value from access to performance measurement tools if they enable them to assess the performance of ads served on their inventory. This kind of information can also help them make decisions about their pricing and inventory offerings, among others. Some of the same independent verification services that cater to advertisers also provide services to publishers for these purposes. As it does for advertisers, the DMA provision would also enable publishers to request the data used for verification themselves and may enable new publisher facing services to emerge. The volume and complexity of the data used for verification means that most individual publishers are not likely to have the capacity to derive much value from it on their own, however access to performance measurement tools could be done so as to be useful to smaller publishers as well.

The provisions in Article 6(8) have the potential to increase competition among firms providing ad verification services and to allow all players to access the information they would need in order to check whether they are being treated fairly. Theoretically, an advertiser could access ad verification data directly to check whether they are getting good service from their independent verification service. A publisher could do the same to check whether their inventory is being fairly represented by such services or other online advertising services. It is also possible that widespread use of the performance measurement tools of the core platform services by publishers enables fairer competition in the provision of advertising inventory. However, here also there remain some questions to be answered in order for the DMA to be effective in achieving contestability and fairness throughout the ecosystem.



3.2 Interpretation and Implementation Issues to be Clarified

3.2.1 Whose performance is this about?

In addition to the data necessary for ad verification, Article 6(8) ensures access to the “performance measurement tools” of the gatekeeper and the data necessary for advertisers and publishers to “run their own[...]measurement tools to assess the performance of the core platform services”. These can be about different types of performance, and the DMA is not clear as to whether this is about achieving transparency in the performance of advertising or in the performance of online advertising intermediaries, or perhaps both.

Recital 58 identifies one of the problems this provision aims to address, namely “a lack of information for advertisers and publishers about the effect of a given advertisement”. Advertisers or their agencies can access large amounts of information from some core platform services on this and use it to make real time decisions on ad placement and for campaign planning. However, as mentioned above, there remains **a lack of consensus around measures in the industry**, and also there remain questions about the independence and veracity of the auditing of the information. This has been a significant contributor to creating an unlevel playing field in the provision of inventory because some of those selling inventory also have access to vast amounts of data to evidence the effectiveness of their inventory, whereas others do not (Broughton Micova & Jacques, 2019, 2020b). Those that also have access to vast amounts of user behaviour data can evidence a purchasing pathway using click throughs, engagement with other content, and maybe even purchases. They make performance measuring tools available to advertisers and their agencies to be able to use this data to track the performance of campaigns that use their inventory and that of others sold through their intermediary services.

Though some data may overlap, this is not the same function as ad verification. It is used to demonstrate the value of the inventory and can lock-in advertisers or their agencies that need to demonstrate return on investment. Press publishers, audiovisual media services, and other media have been struggling to match this ability to measure and demonstrate the effect or performance of their online inventory. If they sell their inventory through online advertising intermediary services provided by those large players with access to vast amounts of ad performance measurement data, the advertisers who buy their inventory may have access to it, but not the publishers.

The provision in Article 6(8), it seems, would only give publishers the ability to access the same tools that advertisers can use to track the performance of ad sold through those online advertising intermediary services. This should help publishers assess the value of some of their inventory. However, if this provision does not enable access to the tools for measuring the performance or effect of a given ad on services where that is being tracked, then it will not do much to even the playing field between publishers and ad-dependent platforms whose providers are also operating online advertising services, or ad tech. Determining exactly which “performance measuring tools” of the gatekeeper are within the scope of this provision will thus be important.

Measuring “the performance of a core platform service” would require different types of data depending on the type of core platform service. As discussed above, the ad verification process



essentially does that for those services involved in the placement and serving of the ads. Measuring the performance of ad exchanges or other trading platforms would require the transactional data covered by Article 5.

3.2.2 What will constitute a request and how will they be handled?

The DMA conflates advertisers, publishers, and their authorised third parties in Article 6(8) even though they have rather different interests and incentives in the acquisition of performance data. The provision is not specific about how requests should be made or fulfilled, but does state that performance data should be given in a manner that enables the receiver to use it for ad verification and be able to use measurement tools.

A media agency or third-party verification service being used by an advertiser will likely already have access to the kind of performance information dealt with in Article 6(8). The processing and interpreting of that data would be a significant part of the service they are providing to the advertiser. These third parties will have an interest in discouraging requests directly from advertisers to core platform services. At the same time, a publisher's sales house might operate a proprietary supply side platform that collects some of the information, while it may pay a third party that has access to data to process and interpret it. Some large advertisers and publishers may have in-house capacity and the ability to draw on the data from multiple brands (Procter & Gamble or Axel Springer, for example).

This provision has the potential to encourage competition in the provision of verification and performance measurement by eliminating the exclusivity of access to data from core platform services that some firms have currently (through trusted partner programmes, for instance) and by making it easier for publishers and advertisers to combine data from core platform services with performance data from other sources. However, this unlikely to happen if requests have to be given for each campaign or for each ad, or otherwise on a frequent and unmanageable basis.

For this data to be useful for advertisers and publishers to understand the value of ad inventory or to identify weaknesses or unfairness in core platform services they need to be able to do performance measurement continually. At the same time, for any new firm to enter the market for verification and measurement services they will need assured access to the data ahead of, or at least congruent to, taking on any given client. Requests would likely need to be executed as one-time permissions, rather than ad hoc or piecemeal, and handled through APIs in order to be useful for achieving greater contestability and fairness.



4. OVERARCHING ISSUES

How designation is handled will have consequences for the effectiveness of these transparency provisions for transaction and performance data. Undertakings may provide multiple ad tech services within the ecosystem. Some of these individually might meet the thresholds while other may not. Undertakings providing ostensibly one service may be able to easily institute artificial separation of the service based on inventory type, business user type, or different end-user platforms. If an undertaking that is designated as a gatekeeper based on one core platform service is not obligated to provide the transparency called for in Articles 5 and 6 for all their services, there may be an incentive for separation. Therefore, an overarching issue is **whether undertakings providing ad tech services will be designated as a gatekeeper for ad tech services in general, with obligations automatically applicable to all the undertaking's individual services or whether each ad tech service will need to be designated**. This issue is discussed in more detail in another CERRE Issue paper by Richard Feasey on designation.⁶⁵ As Feasey argues, the Commission may struggle to evidence that any disaggregation was strategic avoidance of regulation under the anti-circumvention provisions in Article 13. It may be necessary to set out a broad understanding of “purposes” for the specific case of ad tech services so that minor differences, such as in types of inventory or users, do not exclude major providers involved in the ecosystem.

A second overarching issue is how these provisions will be implemented effectively without being at odds with the principles of GDPR. As evident in the discussion above, personal data processing can be involved in determining price paid, in ad verification, and in ad performance measuring. This would likely be most prevalent where the core platform service enables highly targeted and/or behavioural advertising. It may be relatively easy for core platform services to achieve pro forma compliance with GDPR by including the right wording in their consent terms, as they might for partner services. However, this would be arguably counter to the principles of the GDPR, especially given the evidence that consent terms are often inaccessible to the average reader (Becher & Benoliel, 2021) and that consent can be given amidst unfair power imbalances between platform services as data processors and their users (Clifford et al., 2019). **These provisions in the DMA should not be used to undermine the protections in GDPR and expand the use of personal data intensive and invasive forms of advertising**. Striking the right balance between providing actors in the ecosystem with the information necessary to ensure contestability and fairness and safeguarding the users of advertising supported services will likely require extensive discussions about what measures of effectiveness are appropriate and what metrics should be used at all.

⁶⁵ Available at: <https://cerre.eu/publications/effective-and-proportionate-implementation-of-the-dma/>



5. CONCLUSIONS

The transparency provisions in the DMA have the potential to make a significant difference in the advertising ecosystem. They also have the potential to be rendered ineffectual if the processes for granting consent for transactional data and requesting both kinds of data are not designed in a manner that encourages transparency. They could also be undermined if the transactional and performance data provided is overly narrow or delivered in an unusable fashion. There are significant undertakings that provide core platform services for supply, demand, and intermediation functions within the advertising ecosystem. The provisions in Articles 5 and 6 of the DMA will oblige those undertakings to make available data from their core platform services in intermediation that helps their competitors in the provision of ad inventory compete with them better.

One of the main sources of dominance that has been identified in the advertising ecosystem is the ability to combine and leverage vast amounts of consumer data, especially from online behaviour, for the purposes of providing highly sophisticated profiling and targeting of end users (Bourreau et al., 2017; Broughton Micova & Jacques, 2019; Competition & Markets Authority (CMA), 2020; Jeon, 2021). **The transparency provisions in the DMA are not designed to directly address that imbalance. An approach to DMA implementation that would encourage publishers to compete in ever increasingly sophisticated personal data intensive, surveillance-based advertising is not desirable.** It would be counter to the GDPR and would be at odds with the steps taken in the Digital Services Act to put at least some constraints on targeting.⁶⁶ If effectively implemented and with fairness toward users as a priority, the transparency provisions may help to encourage a move away from the more invasive targeting techniques by giving more visibility to the effectiveness and relative value of contextual, broadly segmented, and other types of advertising.

⁶⁶ The Digital Services Act Article 24 bans targeting based on sensitive personal information.



REFERENCES

- Adshead, S., Forsyth, G., Wood, S., & Wilkenson, L. (2019). *Online Advertising in the UK*. UK Department of Media Culture and Sport.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777996/Plum_DCMS_Online_Advertising_in_the_UK.pdf
- Andreou, A., Silva, M., Benevenuto, F., Goga, O., Loiseau, P., & Mislove, A. (2019). *Measuring the Facebook Advertising Ecosystem*.
https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-1_Andreou_paper.pdf
- Australian Competition and Consumer Commission. (2019). *Digital Platforms Inquiry: Final report*. ACCC.
<https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>
- Banchio, M., & Skrzypacz, A. (2022). Artificial Intelligence and Auction Design. *Proceedings of the 23rd ACM Conference on Economics and Computation*, 30–31. <https://doi.org/10.1145/3490486.3538244>
- Becher, S. I., & Benoliel, U. (2021). Law in books and law in action: The readability of privacy policies and the gdpr. In *Consumer Law and Economics* (pp. 179–204). Springer.
- Boerman, S. C., Kruijkemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363. Complementary Index.
- Bourreau, M., De Streel, A., & Graef, I. (2017). Big Data and Competition Policy: Market power, personalised pricing and advertising. *Personalised Pricing and Advertising (February 16, 2017)*. <https://ssrn.com/abstract=2920301>
- Broughton Micova, S., & Jacques, S. (2019). *The Playing field for audiovisual advertising: What does it look like and who is playing*. Centre on Regulation in Europe (CERRE).
- Broughton Micova, S., & Jacques, S. (2020a). Platform power in the video advertising ecosystem. *Internet Policy Review*, 9.
- Broughton Micova, S., & Jacques, S. (2020b). The Functions of Data in the Competition between Audiovisual Media and Video Sharing Platforms for Advertising. *Journal of Information Policy*, 10, 514–548. JSTOR. <https://doi.org/10.5325/jinfopoli.10.2020.0514>
- Broughton Micova, S., & Kostovska, I. (2021). Advertising funded video-sharing platforms under the revised AVMSD: Commercial Communication Functionalities. *Journal of Digital Media & Policy*, 12(3).
- Calvano, E., Calzolari, G., Denicolo, V., & Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. *American Economic Review*, 110(10), 3267–3297.



Clifford, D., Graef, I., & Valcke, P. (2019). Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. *German Law Journal*, 20(5), 679–721.

Competition & Markets Authority (CMA). (2020). *Online platforms and digital advertising: Market study final report*.

https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020.pdf

Decarolis, F., & Rovigatti, G. (2021). From mad men to maths men: Concentration and buyer power in online advertising. *American Economic Review*, 111(10), 3299–3327.

Decarolis, F., Rovigatti, G., Rovigatti, M., & Shakhgildyan, K. (2022). *Artificial Intelligence, Algorithmic Bidding and Collusion in Online Advertising*.

Eisenhardt, K., Gawer, A., & Hannah, D. (2018). *Shaping Sectors, Changing Architectures, Constructing Ecosystems* (S. Taneja, Ed.; Vol. 2018, p. 12100). Academy of Management Briarcliff Manor, NY 10510.

Expósito-Ventura, M., Ruipérez-Valiente, J. A., Parra-Arnau, J., & Forné, J. (2021). A Survey of the Role of Viewability Within the Online Advertising Ecosystem. *IEEE Access*, 9, 134593–134610.

Fassl, M., Gröber, L. T., & Krombholz, K. (2021). *Stop the consent theater*. 1–7.

Geradin, D., & Katsifis, D. (2019). An EU competition law analysis of online display advertising in the programmatic age. *European Competition Journal*, 15(1), 55–96.

<https://doi.org/10.1080/17441056.2019.1574440>

Gusic, N., & Stallone, V. (2020). *The digital advertising ecosystem: Status quo, challenges and trends*. 36–42.

IAB. (2012). *Guidelines for the Conduct of Ad Verification*. Interactive Advertising Bureau Europe. iab.com/wp-content/uploads/2015/06/Ad-Verification-Guideline-for-the-Conduct-of.pdf

Jeon, D.-S. (2021). *Market power and transparency in open display advertising – a case study*. Observatory on the Online Platform Economy.

<https://platformobservatory.eu/app/uploads/2021/03/06CasestudyonMarketpowerandtransparencyinopendisplyadvertising.pdf>

Krämer, J., Schnurr, D., & Micova, S. B. (2020). *The role of data for digital markets contestability: Case studies and data access remedies*. Centre on Regulation in Europe asbl (CERRE).

Sanchez-Rola, I., Dell’Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). *Can i opt out yet? Gdpr and the global illusion of cookie control*. 340–351.

Stallone, V., & Klaas, M. (2019). *The Digital Advertising Ecosystem Visualization—Literature Review*. Held on the 12th IADIS International Conference on Information Systems.

cerre

Centre on Regulation in Europe



DMA SWITCHING TOOLS AND CHOICE SCREENS

Amelia Fletcher



TABLE OF CONTENTS

INTRODUCTION	71
1. THE DMA AND ITS OBJECTIVES	72
1.1 The Relevant Provisions	72
1.2 Intention of the Provisions	73
1.3 The Importance of ‘Choice Architecture’ in the DMA	755
2. QUESTIONS OF INTERPRETATION AND CHALLENGES FOR IMPLEMENTATION.....	777
2.1. Scope Issues	777
2.2 Effectiveness Issues: Articles 6(3)(ii) and 6(4)(ii)	81
2.3 Mitigating Unintended Consequences: Article 6(4)(ii)	83
2.4 Effectiveness Issues: Article 6(3)(iii)	844



INTRODUCTION

In the years preceding the adoption of the Digital Markets Act (DMA), there had been growing concern, reflected in a variety of competition cases, regarding the ability of the largest gatekeeper platform firms to leverage from one service into another, by making their proprietary offering the ‘default’ for users.

For example, the European Union’s (EU) 2018 *Google Android* decision found Google to have breached competition law when it required Android device manufacturers to pre-install and make prominent several of its apps (and in particular Google Search) as a condition of access to Google’s must-have Play app store.⁶⁷

Such defaults are important for both positive and negative reasons. On the positive side, they enable end users to start using services as easily as possible, without having to make too many upfront decisions. On the negative side, end users are strongly inclined to accept the default options they are given and to stick with these over time. This means that making proprietary services ‘default’ options can act as *de facto* tying, and thereby enable firms to leverage market power from one service to another.⁶⁸

Such *de facto* tying is especially likely to be anti-competitive where (i) the core (tying) service is a critical gateway for end users to the related (tied) services; and (ii) end users are not easily able to change their choices (for example, to terminate and switch their default option) over time.

A few different provisions within Article 6 of the DMA aim to address some of these problems in relation to gatekeeper undertakings. The particular focus of **Article 6(3)** is leverage from Operating Systems, Browsers and Virtual Assistants into other services. The particular focus of **Article 6(4)** is leverage from Operating Systems into App Stores and Apps. **Article 6(6)** then focuses on enabling take-up of – and switching to – third-party services, while **Article 6(13)** relates to enabling the termination of proprietary services.⁶⁹

This issue paper covers these measures, with the focus being on Articles 6(3) and 6(4). It begins with a brief overview of the wider context of the DMA before describing the key measures and their intentions. It highlights some intrinsic challenges associated with any requirements that seek to change end-user behaviour. It then examines each of the provisions in more detail, highlighting questions of interpretation, and finally emphasising some possible limitations to their effectiveness.

⁶⁷ Commission Decision of 18 July 2018, Case 40 099 *Google Android*.

⁶⁸ The General Court judgment in *Google Android* confirms that pre-installation combined with status quo bias can lead to *de facto* tying: Case T-604/18 *Google v. Commission*, ECLI:EU:T:2022:541.

⁶⁹ The DMA’s end user data portability provision, Article 6(10) is also relevant to end user switching. It is not considered here, as it is the subject of a companion CERRE paper.



1. THE DMA AND ITS OBJECTIVES

The DMA has two overarching aims: contestability and fairness. Both are relevant to these provisions. If they are effective in limiting the leverage of market power from one service to another, this will clearly enhance **contestability** for (at least) these latter services. At the same time, by re-leveling the playing field between proprietary and third-party services, they should also promote **fairness**.

The objectives are important. Given the purposive nature of EU law, they provide general context for the interpretation of the DMA provisions, but they are also explicitly relevant under Article 8. Specifically:

Article 8(1)

*The gatekeeper shall ensure and be able to demonstrate compliance with the obligations laid down in Articles 5, 6 and 7 of this Regulation. The measures implemented by the gatekeeper to ensure compliance with those Articles **shall be effective in achieving the objectives of this Regulation** and of the relevant obligation.*

1.1. The Relevant Provisions

Articles 6(3) and 6(4) are both complex provisions, with several elements. For ease throughout the rest of the paper, we have separated these into numbered sub-elements.

Article 6(3)

- (i) *The gatekeeper shall allow and technically enable end users to **easily un-install any software applications** on the operating system of the gatekeeper, without prejudice to the possibility for that 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.*
- (ii) *The gatekeeper shall allow and technically enable end users to **easily change default settings** on the operating system, virtual assistant and web browser of the gatekeeper that direct or steer end users to products or services provided by the gatekeeper.*
- (iii) *That includes **prompting** end users, at the moment of the end users' first use of an online search engine, virtual assistant or web browser of the gatekeeper listed in the designation decision pursuant to Article 3(9), **to choose, from a list** of the main available service providers, the online search engine, virtual assistant or web browser to which the operating system of the gatekeeper directs or steers users by default, and the online search engine to which the virtual assistant and the web browser of the gatekeeper directs or steers users by default.*

Article 6(4)

- (i) *The gatekeeper shall allow and technically enable the installation and effective **use of third-party software applications or software application stores using**, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper.*



- (ii) *The gatekeeper shall, where applicable, **not prevent the downloaded third-party software applications or software application stores from prompting** end users to decide whether they want to set that downloaded software application or software application store as their default. The gatekeeper shall technically enable end users who decide to set that downloaded software application or software application store as their default to carry out that change easily.*
- (iii) *The gatekeeper shall not be prevented from taking, to the extent that they are 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 measures are duly justified by the gatekeeper.*
- (iv) *Furthermore, the gatekeeper shall not be prevented from applying, to the extent that they are strictly **necessary and proportionate, measures** and settings other than default settings, enabling end users to effectively protect **security** in relation to third-party software applications or software application stores, provided that such measures and settings other than default settings are duly justified by the gatekeeper*

Article 6(6)

The gatekeeper shall not restrict technically or otherwise the ability of end users to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper, including as regards the choice of Internet access services for end users.

Article 6(13)

The gatekeeper shall not have general conditions for terminating the provision of a core platform service that are disproportionate. The gatekeeper shall ensure that the conditions of termination can be exercised without undue difficulty.

1.2. Intention of the Provisions

As discussed above, the core intention of these provisions is to promote contestability and fairness by reducing the potential for gatekeepers to leverage market power from one gateway service into others, by enabling and promoting the use of third-party services. However, they seek to achieve this in a variety of different ways.

Specifically, the provisions can be split into three key categories. Provisions that:

- (a) seek to enable **easy switching of defaults** by end users, including the ability to access **switching tools** and the **use of prompts** by third parties;
- (b) require the **use of initial choice screens** to force end users to make active choices; and
- (c) seek to **promote end user choice** – and thereby switching and multi-homing – more generally (including requirements relating to termination of service and uninstallation).



The following table summarises the aims and coverage of each of the provisions, based on this categorisation.

Table 1: Breakdown of the provisions

(a) Provisions seeking to enable easy switching of defaults

PROVISION	LIMIT LEVERAGE		ADDITIONAL DETAIL
	FROM	TO	
Art 6(3)(ii)	OS, web browsers or virtual assistants	Apps and services (NB including browsers, virtual assistants and search)	Enable easy switching of defaults
Art 6(4)(ii)	OS	Apps and app stores	Enable third-party prompts AND easy switching of defaults

(b) Provisions requiring the use of initial choice screens

PROVISION	LIMIT LEVERAGE		ADDITIONAL DETAIL
	FROM	TO	
Art 6(3)(iii)	OS, web browsers or virtual assistants	Search engine, virtual assistant and browser	Initial choice screen for default at first use of service

(c) Provisions seeking to promote end user choice generally

PROVISION	LIMIT LEVERAGE		ADDITIONAL DETAIL
	FROM	TO	
Art 6(4)(i)	OS	Apps and app stores	Enable effective use of third-party apps and app stores
Art 6(6)	Any gateway CPS	Apps and services accessed through CPS	Enable switching between, and subscription to, different apps and services
Art 6(3)(i)	OS	Apps	Enable un-installation of apps on a gatekeeper's OS
Art(13)	Any gateway CPS		Enable termination of gatekeeper CPS

As regards this final category, it should be noted that the term 'multi-homing' does not in fact come up within the provisions themselves. However, the key factor underpinning these provisions is the need for effective end user choice of service. This could in principle involve an end user switching service fully, but it could also involve multi-homing. In practice, where end users are reluctant to leave a gatekeeper's proprietary service completely, multi-homing may be a more realistic source of contestability than switching.

This final category is not discussed further in this paper. **The focus is on Articles 6(3)(ii), 6(3)(iii) and 6(4)(ii).** Article 6(4)(i) is, however, discussed in the companion CERRE Issue Paper on interoperability.



1.3. The Importance of 'Choice Architecture' in the DMA

A key challenge for these various provisions is that their effectiveness depends critically on their impact on end user behaviour. For example, enabling end users to switch their defaults will only be effective in enhancing contestability if end users take advantage of these options.

At the same time, we know that most end users are inexpert and that choice can be a mental burden, with end users typically disinclined to spend significant time making decisions. This is a key reason why online platforms focus on designing their systems in a user-friendly and trustworthy way. They seek to ensure that end users enjoy a smooth consumer journey, without having to make too many choices, and – where choices must be made – that this can be done so in a clear, quick and easy manner, with some protection against decisions that would be harmful. It is this very preference for a smooth and trusted consumer journey that gives default options their power. Given a default option, many end users will happily adopt it, and will not revisit that decision.

This means that the effectiveness of the DMA in promoting contestability and fairness requires more than simply enabling more end user choice. At the very least, **end users need to be able to make any choices easily, and ideally they need to be explicitly prompted or required to do so**. Recognition of this led to a number of late stage changes in wording in the DMA. For example, the wording in Article 6(3) and 6(4) relating to defaults and prompts is all new since the previous public draft of the DMA, as is the addition of the word 'easily' in these obligations.

More generally, however, end user choices will be critically impacted by the way in which those choices are presented to them – the so-called 'choice architecture' they face. End users frequently use heuristics to make decisions in the face of complexity. While such heuristics can be optimal, given the cost involved in more deliberative decision-making, they can nonetheless lead end users to exhibit **'default bias', 'ranking bias' and 'saliency' bias, whereby they tend to pick the default, highest ranked, or most salient or prominent options**. In many situations, these will also be the best options, but this need not be the case. End users are likely to be cautious, and thus likely to try out new options only if they are clear that they can reverse their decision easily. They will also have a natural tendency to choose the names they know. Finally, end users exhibit 'status quo bias' in terms of being inclined to stick with an existing service.⁷⁰

These elements of end user behaviour can be ameliorated, or alternatively exploited, depending on the precise design of the **choice architecture** facing end users. As such, the choice architecture adopted by the platforms will be critical for the effectiveness of the DMA in achieving its objectives.

The DMA also recognises the importance of choice architecture in Article 13 (anti-circumvention), which mentions the structure and design of user interfaces specifically, as shown in the emboldened wording below.

⁷⁰ These various behavioural tendencies arise from the use of simple heuristics to deal with complex decision-making situations. The Competition and Markets Authority's recent evidence review on [Online Choice Advertising](#) surveys the extensive academic research that has been carried out into the wide selection of such biases, while 'status quo' bias is much discussed in the 2018 EU decision on [Google Android](#) (recently upheld by the [ECJ](#)). [Fletcher \(2019\)](#) also discusses the relevance of behavioural insights for competition policy.



Article 13(4)

*The gatekeeper shall not engage in any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7 regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, **or consists in the use of behavioural techniques or interface design.***

Article 13(6)

The gatekeeper shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6 and 7, or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users and business user's autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.

These two Article 13 provisions, alongside the general effectiveness provisions within Article 8, are potentially very powerful in ensuring that the provisions discussed in this paper are effective.



2. QUESTIONS OF INTERPRETATION AND CHALLENGES FOR IMPLEMENTATION

The remainder of this paper sets out several questions relating to the interpretation of Articles 6(3) and 6(4). We consider questions of scope, as well as issues arising from the requirement to ensure that these provisions are effective in achieving the core DMA objectives of contestability and fairness. For the latter, we consider, Articles 6(3)(ii) and 6(4)(ii) first, and then Article 6(3)(ii).

In several cases, we highlight that clarification is required. In some cases, the Commission is well-placed to provide this clarification, for example through the Article 8 specification process or through formal guidance. In others, the clarification may require the Courts to opine.

2.1 Scope Issues

(i) Application of Article 6(3) to non-standard browsers

Browsers are defined relatively widely under the DMA. **Article 2(11)** states that:

‘Web browser’ means a software application that enables end users to access and interact with web content hosted on servers that are connected to networks such as the Internet, including standalone web browsers as well as web browsers integrated or embedded in software or similar.

This definition clearly includes general use browsers such as Chrome, Safari or Firefox. But it would seem to be more inclusive than this.

First, under the definition above, **it seems likely that search apps would be classified as browsers, and that Article 6(3)(ii) should apply to them on that basis. However, this could usefully be clarified.**

This would in turn seem to have two significant implications.

- *In relation to choice of search engine:* Gatekeepers with their own designated search apps are required to open these up to offering alternative search engines, again under both Article 6(3)(ii) and Article 6(3)(iii); and
- *In relation to choice of browser:* Designated gatekeepers are required to treat third-party search apps as browser services when enabling users to change their default settings in relation to browsers under Article 6(3)(ii) and when providing an initial choice screen under Article 6(3)(iii).

The first of these seems broadly beneficial, not least because there is otherwise a risk that gatekeepers could subtly circumvent Article 6(3) by promoting their own search apps (which do not have to offer search engine choice) over their own browsers (which do).

There are, however, pros and cons of the first and of the second implication. On the positive side, it should be useful in driving contestability in both browsers and search, since it provides more opportunities for rival search engines to gain end users and increases the number of browser options available. On the negative side, third party search apps are not always full-function browsers. For example, they may not allow for the direct entry of web addresses or for multiple tabs. If designated



gatekeepers are required to treat such apps as browser services and offer them as default options alongside full-function browsers, this could potentially mislead consumers.

A similar situation applies to ‘in-app’ browsers, since these too will typically meet the definition of ‘browser’ under Article 2(11). These are browsers which are embedded within apps by default. Many of these in-app browsers use the OS’s own default web viewing software, but this need not be the case. These are designed to enable the viewing of web content only, and do not typically include a default search engine, but they could. Again, it is not obvious that it would be beneficial (and could be misleading) to allow end users to select such ‘in app’ browsers as their default browser, since they cannot be utilised on a stand-alone basis.

This suggests that **it may be appropriate for gatekeepers to place some minimum requirements on what functionality ‘browsers’ must offer in order to be chosen as a default, but any such criteria should be transparent and proportionate.**

(ii) Application of Article 6(3)(ii) to services other than browsers, virtual assistants and search engines

The Article 6(3)(ii) requirement to enable easy switching of defaults relates to:

*“default settings on its operating system, virtual assistant and web browser that direct or steer end users to products or services **provided by the gatekeeper.**”*

The clause which follows (Article 6(3)(iii)) goes on to talk specifically about browsers, virtual assistants, and search engines. But does this mean that Article 6(3)(ii) is restricted to these products or services? For example, if it provides a default mail app that opens up when a “mail to” link is clicked in a browser, it should be easy for end users to switch that default too. Calendar, Maps and audio players services can likewise act as defaults in a similar way.

In our view, **Article 6(3)(ii) should be interpreted as covering all products or services for which there is a default setting on its operating system, virtual assistant and web browser, and not just browsers, virtual assistants and search engines. Mail, Calendar, Maps and audio player services seem obvious examples.** There is no explicit wording limiting it to the narrower set of products, and the more expansive view also seems consistent with the “*That includes*” language at the start of Article 6(3)(iii).

It would be useful if this could be confirmed, however.

In addition, there is also a question as to whether Article 6(3)(ii) applies to ‘within browser’ defaults that are effectively part of the core browser product. We would suggest not. As an example, a browser itself inherently shows links, which a user can click on. It would make little sense for a user to have to specify the default browser that these links lead to. This would simply create a poor user experience and generate little benefit. Likewise, it seems unlikely that this provision is intended to apply to the default photo viewer that is used within the browser.

As such, **‘within browser’ defaults should arguably be out of scope. However, we note that the line between what is effectively part of the browser and what is distinct may well be subject to debate.** It would be useful to have clarification on these issues.



(iii) *Application of Article 6(3)(ii) to non-proprietary defaults*

The Article 6(3)(ii) requirement to enable easy switching of defaults relates to:

*“default settings on its operating system, virtual assistant and web browser that direct or steer end users to products or services **provided by the gatekeeper.**”* (Bold added)

The term ‘provided by the gatekeeper’ raises an important question. It clearly requires gatekeepers to enable switching of defaults where they currently provide their own proprietary service as a default. However, the situation is less clear in the context where they are provided under contract by a third-party service.

On the other hand, it could also be argued that the provision does apply to third-party defaults. Such defaults are still services ‘provided by the gatekeeper’. Moreover, Article 6(3)(ii) should arguably be read in the context of Article 8, which stresses the importance for effectiveness. Enabling easy switching for all default settings (irrespective of whether the firm has a proprietary service) would seem likely to be more effective in promoting contestability, at least where the third-party default service in question is itself designated as the proprietary offering of another gatekeeper.

Against this interpretation, the relevant Recital – which was written later than Article 6(3) itself and thus might provide a more final view, explicitly refers to gatekeepers’ *“own software applications and services”*, and *“the online search engine listed in the designation decision”*.

Recital 49

*Gatekeepers should also allow end users to easily change the default settings on the operating system, virtual assistant and web browser when those default settings favour **their own software applications and services.** This includes prompting a choice screen, at the moment of the users’ first use of an online search engine, virtual assistant or web browser of the gatekeeper listed in the designation decision, allowing end users to select an alternative default service when the operating system of the gatekeeper directs end users to those online search engine, virtual assistant or web browser and when the virtual assistant or the web browser of the gatekeeper direct the user to **the online search engine listed in the designation decision.*** [Bold added]

Overall, on the basis of Recital 49, Article 6(3)(ii) might seem most likely to apply only to those default settings which relate to a gatekeeper’s own proprietary services and not to defaults where services are provided under contract by a third party. However, the legal position on this important issue is complex and requires clarification.

In addition, the specific case of default settings for apps on operating systems, we note that there is also a potential link here with Article 6(4)(i). This requires that gatekeepers enable the ‘effective use’ of third-party apps and app stores with their operating system. One possible interpretation is requiring the easy switching of any relevant default settings within a designated Operating System (albeit this does not apply to default settings within browsers or voice assistants). This requirement is not limited to situations where the gatekeeper has its own rival services. Again, it would be helpful to have more clarity on how Article 6(3)(ii) relates to Article 6(4)(i).



(iv) Application of Article 6(4)(ii) to pre-installed apps/app stores

Article 6(4)(ii) requires easy switching of default settings for third-party apps and app stores. However, **it formally applies to “downloaded third-party software applications or software application stores”**. (Underlining added)

As such, it seems to exclude any apps and app stores that have been pre-installed, meaning that they would not have the right to prompt end users to switch their default setting to them.

However, it could be argued that the effectiveness requirements of the DMA militate against taking a narrow view and excluding pre-installed apps and app stores from the application of Article 6(4)(ii). Indeed, this could even disincentivise third-party apps and app stores from seeking to be pre-installed, which –given the competitive benefits that can arise from being pre-installed – would not be good for contestability.

Overall, the restriction of Article 6(4)(ii) to downloaded apps does not seem in keeping with the contestability objective of the DMA. It is also noteworthy that the relevant Recital (50) refers only to third party apps and app stores and makes no reference to whether or not they are downloaded. However, the Recital could be viewed as having less power than the wording of the Article itself.

Overall, it would be useful to have clarification on this issue.

(v) The issue of multiple ‘access points’

For some services, end users potentially access them via a variety of different pathways. The most extreme example is search. If I want to search for something on the web: (i) I could go to a search app, (ii) I could go to a browser and use its default search service; (iii) I could search via the virtual assistant, and use its default search service, (iv) I could use text search/look-up from within an app and use its default search service; (v) I could search via a widget on my homescreen. This could potentially be a browser widget (with its own default search service) or a search widget.

This variety of different access points creates inherent complexity in terms of switching defaults. Suppose an end user wishes to switch to a new search engine across all of these services. If this has to be done separately for each one, they may be discouraged from switching at all, and thus the provisions to encourage such switching will be ineffective. This would not seem to be in keeping with the requirement that switching default should be easy, or the effectiveness and anti-circumvention provisions of Articles 8 and 13.

At the same time, there may be risks from being too prescriptive about requiring gatekeepers to enable users to switch a default across all access points at once, as it could restrict the ability of end users to pick and choose which search engines they wish to use where, and could even limit entry if not all search engines can function with all access points.

Overall, **we consider that Articles 6(3) and 6(4) could reasonably be interpreted as requiring gatekeepers to enable end users to choose to switch a default across all access points at once, but also – for those who are keen or for those services with more limited interoperability – to enable choices to be made separately for each individual access point.** Even in this latter case, however, the choice should be as easy as possible, for example with a set of tick boxes on a single screen.



We consider that this conclusion is relevant to both the ongoing switching tools required at Article 6(3)(ii), the initial choice screens for browsers, virtual assistants and search engines required under Article 6(3)(iii), and the ability to switch following a prompt under Article 6(4)(ii). It would be useful to have clarification of this issue.

2.2 Effectiveness Issues: Articles 6(3)(ii) and 6(4)(ii)

The intention of enabling the easy switching of defaults is clear. By limiting the ability to gatekeepers to set the default choices, the expectation is that this will open these services up to greater competition. But what challenges arise in doing this?

(vi) Design of the Article 6(3)(ii) switching tools

Article 6(3)(ii) requires that the gatekeeper should enable easy switching of default settings on its OS, virtual assistant and web browser. But it is silent on what these switching tools should look like, and which, or how many, alternative providers it should be possible to switch to.

Formally, Article 6(3)(ii) would in fact be met if the gatekeeper were to provide a simple switching tool which literally just offered one alternative provider for each type of default service. However, it seems clear that providing such a restricted choice set would not be in keeping with the spirit of the DMA and would be unlikely to meet the general effectiveness requirements.

At the same time, it is not obvious that end users should be given a choice of all possible providers, even if they do not currently have their service installed on their device. First, this could be a long and unmanageable list, which creates ‘choice overload’ and thereby worsens decision-making. Second, the time involved in downloading and installing the service would worsen the consumer journey. Third, some of these providers may offer poor or unduly privacy-intrusive services. While these should certainly be available to consumers as default options if they so wish, it would be preferable to ensure they were only available to consumers that had made an active choice to download them.

In general, and especially given the link with the requirement for easy switching of default settings under Article 6(4)(ii), we conclude that **end users should be able easily to switch default settings on designated operating systems to (at least) all alternative options that are currently installed as an app or app store on the user’s device.**

For default settings on browsers and voice assistants, which are outside the scope of Article 6(4)(ii), the situation is less clear. However, given that end users are unlikely to be clear on the distinction between default settings and apps, the intention to make switching ‘easy’ could reasonably be interpreted as again requiring that **default choices should include (at least) the alternative options that are currently installed on the user's device.** For example, if a user specifically downloads and installs a particular search app, then that search engine should appear as a search engine option in the relevant browser or voice assistant.

In terms of the design of the switching tools, there are at least two key ways in which a switching tool could be designed:

- First, within the relevant app settings, the tool could comprise a prominent and simple to use ‘make this my default’ button; and



- Second, within a separate ‘default settings’ section, users could be offered a list of possible default services to choose between.

In practice, if switching default settings is to be made easy for all end users, irrespective of how they use their device, it seems reasonable to assume that both should be made available. In either case, it is important that users can access the switching tool easily, without having to click too many times or scroll too much.

The provision of any list of possible default options then raises another question: the ordering of these options. In general, these should be ordered in a way that allows for meaningful choice and is not misleading. Critically, we would argue that **the gatekeeper should not be allowed to charge providers a fee to be ranked higher on this list, and certainly (if this not accepted) that any fee should not be set on the basis of an auction.** This would seem to be in breach of Article 13(6), which requires the avoidance of non-neutral choice architecture. It would be useful if the EU Commission could confirm whether it supports these conclusions.

The DMA is, however, silent on the issue of whether gatekeepers could charge services for pre-installation (which would guarantee a place on the list). It is also silent on whether they could charge a fair, reasonable and non-discriminatory ongoing fee to providers who are successful in being chosen, potentially in the form of a share of revenues.

(vii) The need to be able to reverse decisions

Under Article 6(3)(ii), it is clearly intended that end users should be able to pro-actively switch default settings at any time. As discussed above, this implies that they should have ready access to an easy to use list of possible providers.

The situation is very different under Article 6(4)(ii). Here, it is intended that switching would result from an end user responding positively to a third-party prompt. As such, this provision would not necessarily require the existence of any such list of options. The user may simply see (or hear) a single choice box with two options: ‘switch’ or ‘don’t switch’.

This raises the issue of what happens if an end user chooses to switch a default via such a choice box, and then changes their mind. Will there be a way for them to simply reverse that decision? It would not be a good outcome if end users got stuck with default settings they did not like. The ability for an end user to reverse their decision is also important for giving them the confidence to switch in the first place. Without the ability to reverse a bad switching decision, they may simply avoid switching and this would not be good for contestability.

For app stores and some apps, this issue will arguably be solved by the requirement under Article 6(3)(ii) that gatekeepers must allow end users to easily change default settings on its operating system. This would presumably apply at least to those app stores and apps that compete with “services provided by the gatekeeper”? However, it may not apply otherwise.

To ensure that Article 6(4)(ii) is effective in promoting contestability, **we would encourage the EU Commission to consider further the importance of enabling default switching decisions also to be easily reversed, including where the gatekeeper does not provide a competing service.**



(viii) The use of behavioural techniques to inhibit switching or induce switching back

Even if switching of defaults is enabled in principle, gatekeepers could potentially inhibit switching in practice through the use of behavioural techniques. For example, while it may be appropriate for gatekeepers to issue warnings to end users seeking to switch default, where this choice would genuinely create risk, such warnings could potentially be made **overly complex or unnerving**, and thus unduly deter switching. For end users who have already switched, the gatekeepers could issue **repeated prompts** to induce end users to switch the default back.

In our view, however, **it is likely that the disproportionate or discriminatory use by gatekeepers of behavioural techniques – such as prompts and warnings – to inhibit switching, or induce switching back, would be non-compliant with the DMA**, given (i) the word ‘easily’ in Articles 6(3)(ii) and 6(4)(ii), and (ii) the provisions described above in Articles 8 and 13. A/B testing may be valuable in determining on which side of the line any such conduct lies. **It would be useful for the Commission to clarify this.**

2.3 Mitigating Unintended Consequences: Article 6(4)(ii)

(ix) The risk of excessive prompts and choice fatigue

A potential unintended consequence of Article 6(4)(ii) could be that third party downloaded apps and app stores overwhelm end users with prompts to make their service their default. This could prove unpopular with end users and could also lead to ‘choice fatigue’ which stops end users making sensible decisions. This could lead to inertia or mistakes on the part of end users, either of which will reduce the effectiveness of this provision in driving contestability.

Recognising these sorts of factors, Article 5(1) places a limit on gatekeepers from re-requesting consent for data collection and usage more than once per year. However, **there is no similar limitation on the prompts of third parties in relation to switching defaults**, and gatekeepers are also prohibited from limiting these prompts (the only caveat to this provision relates to security).

This risk is not considered in the DMA. Gatekeepers may be able to mitigate the risk somewhat through their own interface design, but clearly there is a balance to be struck, however if gatekeepers go too far in doing so, they risk breaching the DMA.

Given the clear risk of ‘choice fatigue’ arising from excessive switching prompts by third parties, based on their rights under Article 6(4)(ii), it would be useful for the Commission to meet with gatekeepers and third parties to seek solutions. More generally, this is an area that should be kept under review.

(x) The risk of unclear and misleading third-party prompts and ‘slamming’

Another risk with third party prompts is that they could be presented to end users in a way that is unclear or non-neutral. For example, end users could potentially receive prompts where the option of changing a default is very prominent relative to the option of not doing so. At an extreme, **they may not even realise they have agreed to switch a default setting.**

There may even be a potential risk of third parties’ misreporting the choices of end users to the gatekeepers, leading to end users’ **default settings being switched when they never chose this.**



Such fraudulent competition is not the form of contestability that the DMA is seeking to promote. It would also not be fair on those apps and app stores who adopt more neutral prompts. In telecoms, these practices are known as ‘slamming’, and new regulations and codes have been introduced to address it.

There is nothing currently within the DMA to address such issues. However, such misleading or fraudulent conduct would likely be prohibited under EU consumer law.⁷¹ The risk of such conduct could be mitigated through the gatekeepers’ user interface design. For example, they could ensure (i) that third party prompts are clear and consistent and (ii) that the user is then taken to the relevant setting page to make the switch, rather than making the switch directly.

While this would be positive, there is again a risk of the gatekeeper being overly prescriptive here and limiting contestability. **In designing its user interface to address the risk of end user harm arising from misleading third-party prompts and ‘slamming’, the gatekeepers therefore face a delicate balance. The Commission should meet with gatekeepers and third parties to consider solutions. More generally, this is an area that should be kept under review.**

2.4 Effectiveness Issues: Article 6(3)(iii)

Article 6(3)(iii) includes a requirement that gatekeepers must prompt end users “*to choose, from a list of the main available service providers, the online search engine, virtual assistant or web browser to which the operating system of the gatekeeper directs or steers users by default, and the online search engine to which the virtual assistant and the web browser of the gatekeeper directs or steers*”.

The clear intent of requiring such an initial choice screen is to limit leverage from OS, browsers and virtual assistants into browsers, virtual assistants and browsers, and in so doing enhance contestability for the latter. However, a number of issues of interpretation and implementation again arise.

(xi) Timing of initial choice screens

As discussed above, there are risks associated with asking end users to make too many choices in terms of generating choice fatigue. As such, there is merit in limiting the occasions at which end users are prompted to a manageable number. Reflecting such concerns, Article 6(3)(iii) only imposes an active choice screen at an end users ‘first use’ of a service.

However, it is not entirely clear what an “*end user’s first use*” is. Is it only (i) the first time they use the service in question (such that pre-existing users are not affected), (ii) the first time they do so after the DMA comes into force? or (iii) the first time they use (or install) an OS, browser or virtual assistant on a new device?

⁷¹ In particular, Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ [2005] L 149/22, as amended by Directive 2019/2161. On the application of this Directive on dark patterns, see Commission Guidance of 17 December 2021 on the interpretation and application of Directive 2005/29 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, OJ [2021] C 526/1, section 4.2.7.



There is arguably a trade-off here. Initial choice screens may not be especially popular with users, who primarily want to get on with using their device, and thus may prefer to receive as few choice screens as possible, as rarely as possible.

On the other hand, if the first or second of these options is the right interpretation, then the impact of this provision might be expected to be relatively limited, at least once the DMA is in place, given there are relatively few new end users coming into the market over time, and relatively little switching by existing users between ecosystems.

Given the general focus within the DMA on effectiveness, therefore, **the Article 6(3)(iii) wording “end user’s first use” seems most likely to mean that defaults must be chosen anew with every first use (or installation) on a new device. However, it would be useful to have clarification on this point.**

(xii) Payment for access to initial choice screens

The DMA is silent on whether gatekeepers can charge third parties for access to – or prominence on – the initial choice screens required under Article 6(3)(iii).

However, any such charging would create new issues. First, there is a serious risk that the gatekeeper’s own service would always win any bid for prominence, given that the gatekeeper itself gets to keep the proceeds.⁷² This has been a recognised problem in the context of the remedies to the EU’s *Google Shopping* case.⁷³ Second, there is a risk that the third parties that are most likely to bid highest are going to be those that offer the worst deal to end users, for example in terms of extracting and using the most data. Again, this would not seem to be a good outcome, or generate the ‘right’ type of contestability. This risk materialised in the EU *Google Android* case, and indeed Google has now made access to the choice box free for eligible search providers.⁷⁴

Moreover, gatekeepers are strictly required to list “the main available service providers” and moreover Article 13(6) requires that they must not offer “choices to the end-user in a non-neutral manner”. On the basis of these requirements, **it seems reasonable to conclude that gatekeepers should not charge for access or prominence on the Article 6(3)(iii) choice screens, and certainly (if this not accepted) that any fee should not be set on the basis of an auction.** This interpretation also fits with the general DMA focus on effectiveness. It would be useful to have clarification on this point. We note that the DMA is silent on the question of whether the gatekeeper can charge a fair, reasonable and non-discriminatory ongoing fee, or revenue share, to providers who are successful in being chosen.

(xiii) Choice architecture of the initial choice screen

As discussed above, the design of choice screens can be critical to their success. It is useful that Article 13(6) requires that they not be designed in a non-neutral manner. However, to make the choice

⁷² As discussed in J. Crémer et al (2022), “The Digital Markets Act: An economic perspective on the final negotiations”, VoxEU, <https://cepr.org/voxeu/columns/digital-markets-act-economic-perspective-final-negotiations>.

⁷³ Commission Decision of 27 June 2017, Case 39 740 *Google Search (Shopping)* which has been upheld by the General Court in Case T-612/17 *Google v. Commission*, EU:T:2021:763.

⁷⁴ See: <https://blog.google/around-the-globe/google-europe/changes-android-choice-screen-europe/>



screen work effectively to promote fairness and contestability, more guidance may be required, not least because it is typically impossible to design choice architecture that is perfectly neutral.

Relevant design questions include:

- How many options should be included? The provision refers to “*the main available service providers*”, but how long should this list be? In general, the list should be **long enough** to provide real choice and promote real contestability, **while not leading to choice overload**. But this still provides substantial leeway;
- What order should options be provided in? It may seem natural to include the most popular option first, but this is unlikely to be the best option for promoting contestability. On the other hand, randomising may give a poor user experience, when they already know what option they want. **Stratified randomising** might potentially strike a reasonable balance (for example, the top 3 services in random order, followed by the next 5 in random order);
- How much description should be provided? Given that end users are likely to exhibit “familiarity bias”, whereby they are more likely to choose familiar options, it could be argued that there would be merit in providing **short descriptions of each option**, alongside each name.
- Should users be reassured that their choice is reversible? Given that end users are likely to be cautious, it would also be valuable to be able to **reassure them that they can easily switch their default back later** if they wish to do so; and
- How should choice screens be varied for virtual assistants? People may react differently to choices that they listen to. For example, they may lose concentration if asked to listen to a long list of options. In principle, the aim should be to strike a balance between usability and contestability. One approach might be to allow **a shorter core list of ‘main available service providers’ to be provided on virtual assistants, but adding one or two of the next tranche of main available providers, to be included on a randomised basis, to preserve contestability.**

The answers to these (and other) questions will be critical to the success of Article 6(3)(iii). However, there are also risks associated with the Commission being too prescriptive in terms of answers.

In our view, **the Commission should therefore set out its high level expectations around the choice architecture of the initial choice screens, and be tough in holding the gatekeepers to account in showing how they are meeting these expectations. In reviewing their submissions, it should seek the input of third parties, draw on the extensive evidence collected by gatekeepers through A/B testing, and potentially require its own testing. The Commission could usefully also set out how it expects gatekeepers to engage with third parties too.**

The Commission should also leave itself leeway to make changes over time, as we learn more about the effectiveness of these provisions in promoting contestability.



(xiv) The risk of harming services with limited market power

The requirement to provide an initial choice screen only applies for gatekeepers that have designated search engines, virtual assistants or web browsers. This restriction is useful in limiting the application to situations where there is a serious contestability issue. Nonetheless, there is a risk that certain browsers and search engines could be designated – based on their user numbers and their strength in a particular segment – despite their having a relatively small position in the sector as a whole.

For such services, **Article 6(3)(iii) could have the unintended consequence of requiring the opening up of some default settings to competition where the current service provider is relatively small, to the potential benefit of their larger rivals.** It is far from clear that this is the DMA's intention, but **it is not entirely clear how it can be avoided under the existing DMA framework. The Commission should be alert to this possible outcome and keep the issue under review.**



THE PROHIBITION OF SELF-PREFERENCING IN THE DMA

Martin Peitz



TABLE OF CONTENTS

1. INTRODUCTION	90
2. SELF-PREFERENCING IN THE DMA	91
2.1 The Prohibition of Self-Preferencing	92
2.2 What is a Separate Service or Product under Article 6(5)?	93
2.3 What is a First-Party Offer and What is a Third-Party Offer?	93
2.4 How to Determine the Absence of Self-Preferencing?	96
3. SELECTED INTERNATIONAL COMPARISON: APPROACHES TO DEAL WITH SELF-PREFERENCING.....	99
3.1 Self-Preferencing in the German Competition Act (GWB)	99
3.2 Self-Preferencing According to the CMA.....	100
3.3 A Look Across the Atlantic.....	100
4. CASES OF SELF-PREFERENCING IN EU AND MEMBER STATES.....	102
4.1 Cases at the European Commission	102
4.2 Cases in Member States	103
5. INTERPRETING THE DMA PROHIBITION: THE ECONOMICS OF SELF-PREFERENCING	106
5.1 First- and Third-Party Offers: The Economics of the Dual Mode.....	106
5.2 Competitive Effects of Self-Preferencing.....	108
5.3 Economists Empirically Assessing Self-Preferencing in the Real World	110
6. CONCLUSION	113
REFERENCES	114



1. INTRODUCTION

In the years preceding the adoption of the Digital Markets Act (DMA), the issue of self-preferencing has appeared in the context of e-commerce platforms (Amazon), search engines (Google Search, Google Shopping), and mobile app stores (Google and Apple), but it is of broader concern. Self-preferencing can be seen as part of the platform's design decision (Belleflamme and Peitz, 2021, chap. 6), how a platform manages its ecosystem, which includes decisions about the treatment of third-party products and services relative to its own products and services.

Article 6(5) of the DMA prohibits the practice of self-preferencing by gatekeeper platforms when self-preferencing is understood to be a more favourable treatment *in ranking and related indexing and crawling* of first-party products and services than third-party offers.

The issue of self-preferencing by intermediaries does not only arise in the digital world. Retailers such as supermarkets and department stores also have to decide how to allocate shelf space to private labels and manufacturer brands, and being hidden in a dark corner in a shop may come close to delisting. In the digital world, the dark corners of the shop correspond to being demoted to page two or three in the listing of offers. What is different? One may argue that the sheer size of some digital platforms and the enormous power they hold over their users constitutes the difference between the physical and the digital world.

This issue paper elaborates on the prohibition of self-preferencing in Article 6(5) of the DMA, focusing on interpretation issues. It identifies some discussion points, which need clarification, and draws on the economics literature to elaborate on the implications of a prohibition of self-preferencing. The paper argues that economic analysis should be used to define the scope of the prohibition and to assess the proportionality of interventions.



2. SELF-PREFERENCING IN THE DMA

The DMA has two overarching aims: contestability and fairness. Recital 7 states that the DMA aims at “contestability and fairness for the markets in the digital sector in general, and for business users and end users of core platform services provided by gatekeepers in particular.” The DMA focuses on digital services that feature “extreme scale economies, very strong network effects, an ability to connect many business users with many end users through the multi-sidedness of these services, lock-in effects, a lack of multi-homing or vertical integration” (Recital 13). While this is a potpourri of certain market characteristics (which are partly determined by the decisions of the economic actors), it provides the context for which services are to be addressed. The concern about gatekeeper platforms stems from the claim that undertakings providing certain core platform services have “gained the ability to easily set commercial conditions and terms in a unilateral and detrimental manner for their business users and end users” (Recital 13). While several commercial conditions have differential impacts on business users and end users (Belleflamme and Peitz, 2021, chapter 6), self-preferencing is a candidate for harming third-party sellers and end users alike.

Contestability – The DMA aims to rectify weak contestability where contestability is defined in Recital 32 as “the ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and services.” The emphasis on contestability can be seen as reflecting the German *ordo-liberal* school of economic thought according to which the State has to protect or restore the well-functioning of markets. The same recital continues with two statements: “The features of core platform services in the digital sector, such as network effects, strong economies of scale, and benefits from data have limited the contestability of those services and the related ecosystems. Such a weak contestability reduces the incentives to innovate and improve products and services for the gatekeeper, its business users, its challengers and customers and thus negatively affects the innovation potential of the wider online platform economy.” While these statements deserve some qualifications, they reflect the spirit in which the DMA was written.

Favouring first-party products and services can be seen as distorting the competition between the various undertakings in a sector and may limit the contestability of the market. For example, if a gatekeeper reduces the visibility of superior third-party offers, third-party sellers have weaker incentives to provide such quality in the first place. Similarly, if any effort in cost reduction by a third-party seller is offset by an equivalent increase in fees charged by the gatekeeper, third-party sellers do not have an incentive to reduce their costs. This shows that the prohibition of self-preferencing can be derived from the overarching aim of contestability.

Fairness – As stated in Recital 7, the DMA is concerned with both end users and business users. However, regarding fairness, Recital 33 states more specifically that “for the purpose of this Regulation, unfairness should relate to an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage.”⁷⁵

⁷⁵ In some contexts, such as social networks, there is no clear dividing line between business users and end users.



A differential treatment of first-party and third-party offers may be deemed unfair. While there are different notions of fairness and self-preferencing should primarily be seen as a contestability issue, it may also be argued that fairness is violated if business users could not fully anticipate a differential treatment when making their participation or investment decisions.⁷⁶ Then, rules against self-preferencing protect vulnerable providers of third-party content (when transparency obligations as part of Article 5 of the DMA and the EU Regulation on platform-to-business relations (P2B Regulation) are deemed insufficient to protect those providers).⁷⁷

2.1 The Prohibition of Self-Preferencing

Articles 5 and 6 of the DMA specify the general obligations of gatekeepers. Article 6(5) deals explicitly with self-preferencing.

Article 6(5)

The gatekeeper shall not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party. The gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking and related indexing and crawling.

When implementing the prohibition of self-preferencing, its scope will have to be defined. The obligation spelled out in the second sentence arguably applies to ranking (and related indexing and crawling) in cases when the gatekeeper offers first-party services or products. **The DMA has a broad notion of rankings, which includes, but is not restricted to algorithmic rankings.** Article 2(22) defines it: *“Ranking’ means the relative prominence given to goods or services offered through online intermediation services, online social networking services, video-sharing platform services or virtual assistants, or the relevance given to search results by online search engines, as presented, organised or communicated by the undertakings providing online intermediation services, online social networking services, video-sharing platform services, virtual assistants or online search engines, irrespective of the technological means used for such presentation, organisation or communication and irrespective of whether only one result is presented or communicated.”*

The DMA (Article 6(1)) also addresses self-preferencing in a broader sense, as it is concerned with the privileged access and use of data as way to treat first-party products and services more favourably.⁷⁸ Furthermore, the required use of choice screens by a gatekeeper’s operating system

⁷⁶ An example for an investment in an e-commerce setting is the long-term rental of a storage facility.

⁷⁷ Such rules may even help the gatekeeper platform in the long run as it may solve a gatekeeper’s self-commitment problem. In other words, it may help the gatekeeper to maintain a healthy and attractive eco-system, as it protects third-party users from unfair treatment. The problem with such asymmetric regulation in the case of self-commitment problems is that entrants offering substitutes to core platform services are not subject to this regulation and, therefore, are in a worse position to convince third-party providers to join. Such a self-commitment problem exists if a platform cannot credibly promise third-party sellers that it presents first-party products and services more favourably. Absent such self-commitment, there is the risk that such regulation increases entry costs for firms offering substitutes to core platform services. This would work against contestability of platform services.

⁷⁸ Recital 46 of the DMA says: *“In certain circumstances, a gatekeeper has a dual role as an undertaking providing core platform services, whereby it provides a core platform service, and possibly other services provided together with, or in support of, that core platform service to its business users, while also competing or intending to compete with those same business users in the provision of the same or similar services or products to the same end users. In those circumstances, a gatekeeper can take advantage of its dual role to use data, generated or provided by its business users in the context of activities by those business users when using the core platform services or the services provided together with, or in support of, those core platform services, for the purpose of its own services or products. The data of the*



(regarding online search engine, virtual assistant and web browser in Art 6(3)(iii) and software applications and software application stores in Art 6(4)(i)) are provisions against self-preferencing by the gatekeeper (as explained in the CERRE companion issue paper switching tools and choice screen). In this issue paper, we acknowledge self-preferencing practices in a broad sense, but focus on the provision in Article 6(5).⁷⁹

2.2 What is a Separate Service or Product under Article 6(5)?

The first question for Article 6(5) is what constitutes a separate service or product. There is no definition in the DMA that helps in answering this question. Where may ambiguities arise? Consider the Google search engine. Its purpose is to present (and thereby rank) search results after a systematic search of the internet in response to a user's web search query. The general question becomes: should only material presented in the organic search results be considered as a product or service or should also material such as Google's knowledge panels (information boxes that appear on the Google search engine after certain search queries for people, places, and organizations, for instance) count as a gatekeeper's product or service for the purposes of the DMA?

To assess whether a particular offer by the gatekeeper is subject to the Article 6(5), the following specific questions may be helpful:

- Does the offer have a **distinct destination** (such as an app)?
- Are there **alternative providers that make a comparable offer on a self-standing basis** (or have there been such instances in the past or would they be likely to emerge in the future)? To assess whether an alternative offer is a comparable offer, one would have to understand whether the user experience with the offer can be seen as comparable to the one with alternative offers.

2.3 What is a First-Party Offer and What is a Third-Party Offer?

A broad interpretation of Article 6(5) would be that the prohibition of a more favourable treatment of a gatekeeper's products or services compared to third-party offers **applies both on the end user and the business user side** since no specific statement is made about the users receiving the offer.⁸⁰

- Regarding end users, an example would be a more favourable treatment of AmazonBasics products compared to third-party offers in the ranking presented to them (scenario 1). Here,

business user can also include any data generated by or provided during the activities of its end users. This can be the case, for instance, where a gatekeeper provides an online marketplace or a software application store to business users, and at the same time provides services as an undertaking providing online retail services or software application. To prevent gatekeepers from unfairly benefitting from their dual role, it is necessary to ensure that they do not use any aggregated or non-aggregated data, which could include anonymised and personal data that is not publicly available to provide similar services to those of their business users. That obligation should apply to the gatekeeper as a whole, including but not limited to its business unit that competes with the business users of a core platform service." Discriminatory access to data such that data are used in the provision of first-party products that cannot be used by third-party sellers can be considered to be self-preferencing in a broad sense.

⁷⁹ We mention contributions in the economics literature about self-preferencing related to data advantages.

⁸⁰ While it is useful to distinguish the different sides of a multi-sided platform, it is important to keep in mind that neither end users nor business users are necessarily a homogeneous group. In particular, there may exist different types of business users whose interest may not be aligned.



the gatekeeper offers its own services or products to end user and operates a gatekeeper for end users to reach these services or products as well as similar services and products provided by other business users.

- Regarding business users, if an e-commerce platform operates as a pure marketplace in a particular product category, self-preferencing may play out as follows: it may offer its own fulfilment (or payment) service as well as third-party fulfilment (or payment) services. If it treats its own service more favourably than third-party fulfilment services in its ranking given to the sellers on the platform this can also be seen as an instance of self-preferencing and thus fall under Article 6(5) (scenario 2).
- The more favourable treatment of the gatekeeper's services that are offered to business users may also happen indirectly through self-preferencing on the end user side (scenario 3): if a seller on a marketplace knows that its offer will receive a more favourable ranking if it uses fulfilment by the gatekeeper (such as Amazon), this may also be seen as an instance of self-preferencing and fall under Article 6(5) because a vertically integrated service is treated more favourably than a third-party service. For example, this would be the case if a seller is more likely to appear in the buy box of Amazon when it uses the 'Fulfilment by Amazon' service.

These three scenarios are illustrated in Figure 1, where vertically integrated offers are shown as a square and substitute third-party offers as a circle. Scenario 1 applies to products or services offered to end users and is clearly within the scope of Article 6(5); scenarios 2 and 3 feature products or services that the gatekeeper offers to business users, which are offered to them as part of a bundle with their own product or service to end users.

When implementing the DMA, the **European Commission will have to decide whether to include also scenarios 2 and 3. An argument against including scenarios 2 could be that first-party and third-party services are offered to business users, and end users are not exposed to "manipulated" rankings.** However, in this scenario end users are still clearly part of the picture given that the business users are active on the platform only because they can reach end users.

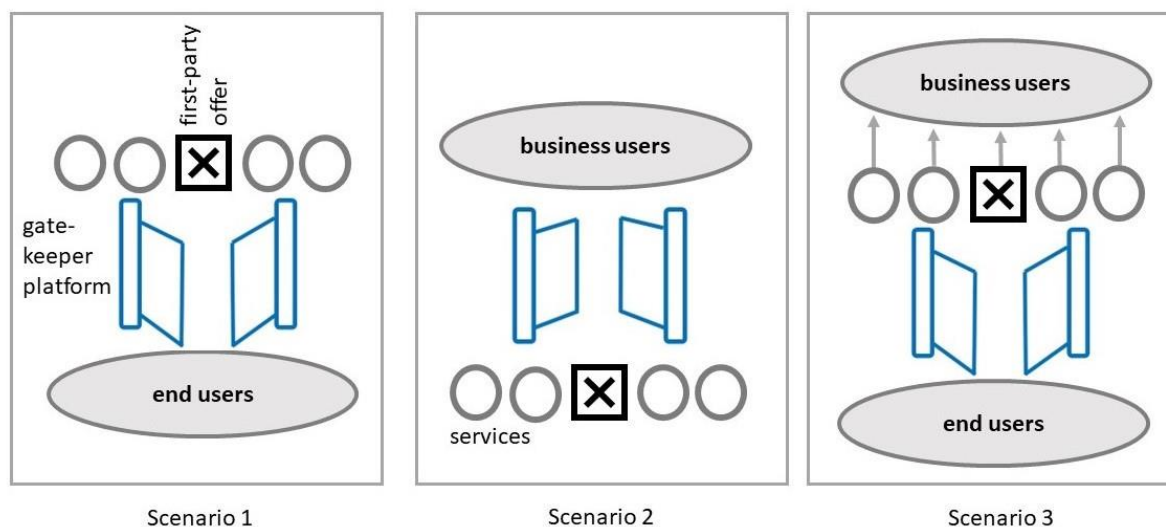


Figure 1: Scenarios with self-preferencing

The use of self-preferencing and other forms of steering can **also be seen as means for the platform to indirectly ensure a certain behaviour of business users when directly imposing such behaviour is prohibited elsewhere in Articles 5 or 6 of the DMA** (in particular, Article 5(3-8)). For example, Recital 43 states that:

“In order to avoid a situation in which gatekeepers indirectly impose on business users their own services provided together with, or in support of, core platform services, gatekeepers should also be prohibited from requiring end users to use such services, when that requirement would be imposed in the context of the service provided to end users by the business user using the core platform service of the gatekeeper.”

Self-preferencing and other distortions of recommendations as a means to enforce a certain behaviour by business users fall under Article 13 of the DMA that deals with “anti-circumvention”. In particular, Article 13(6) says:

“The gatekeeper shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6 and 7, or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users and business user’s autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.”

A final consideration for distinguishing a first-party and a third-party offer is the ownership of a company. A fully vertically integrated offer by a gatekeeper clearly constitutes a service or product “*offered by the gatekeeper itself.*” Suppose instead that a gatekeeper platform holds a stake in another undertaking that competes with third parties without any cross ownership. Under which conditions does the gatekeeper’s more favourable treatment of the former relative to the latter fall under Article 6(5)? According to Recital 52 the prohibition of self-preferences applies to “*products or services it*



offers itself or through a business user which it controls." This requires an understanding of what constitutes control.

2.4 How to Determine the Absence of Self-Preferencing?

A more favourable treatment of first-party products or services may mean that the gatekeeper charges different fees or uses non-price strategies to treat them differently from third-party products or services.

Differential fees (conditional on the ranking position) indicate differential treatment. Even if the same fee is charged, this does not necessarily imply that this creates a level-playing field, as first-party fees are transfers within the same company. Hence, while self-preferencing consisting of lower fees for first-party content is, in principle, easy to observe, it is not obvious whether symmetric fees should be seen as sufficient to be compliant with the prohibition of self-preferencing with respect to the price dimension. It could indeed be argued that symmetric high fees charged to third parties are a means to steer users to first-party offers.

Overall, it is unclear to what extent fees associated with rankings are subject to Article 6(5) and, if so, whether charging high symmetric fees could be a violation of Article 6(5). The Commission will have to clarify whether and to what extent a gatekeeper's pricing of ranked items falls within the meaning of Article 6(5). While high or differential fees may fall under different provisions of the DMA, **Article 6(5) could be restricted to the design of rankings as a non-price strategy** (which does not preclude the possibility that a third party has to make a payment to be ranked).

The application of Art. 6(5) to non-price strategies is facilitated by Recital 51:

"Gatekeepers are often vertically integrated and offer certain products or services to end users through their own core platform services, or through a business user over which they exercise control which frequently leads to conflicts of interest. This can include the situation whereby a gatekeeper provides its own online intermediation services through an online search engine. When offering those products or services on the core platform service, gatekeepers can reserve a better position, in terms of ranking, and related indexing and crawling, for their own offering than that of the products or services of third parties also operating on that core platform service."

The recital provides specific examples, which are possibly motivated by abuse cases at the European Commission.

"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."

In addition to search engines, the recital also refers to application stores, content platforms (video sharing, for example), social networks and e-commerce platforms.



“Other instances are those of software applications which are distributed through software application stores, or videos distributed through a video-sharing platform, or products or services that are given prominence and display in the newsfeed of an online social networking service, or products or services ranked in search results or displayed on an online marketplace, or products or services offered through a virtual assistant. Such reserving of a better position of gatekeeper’s own offering can take place even before ranking following a query, such as during crawling and indexing. For example, already during crawling, as a discovery process by which new and updated content is being found, as well as indexing, which entails storing and organising of the content found during the crawling process, the gatekeeper can favour its own content over that of third parties.”

Noteworthy is that Article 6(5) mentions not only rankings but also *“related indexing and crawling.”* As Recital 51 suggests, this has been done because self-preferencing may be achieved through indexing and crawling. To take an extreme example, if Google Search does not crawl or index sites that are rivals to its own then these rivals’ sites will not be ranked. However, outside such an extreme case, how will the European Commission be able to assess whether indexing and crawling is transparent, fair, and non-discriminatory?

The general concern appears to be that self-preferencing puts third-party providers at a disadvantage, which may lead to a lack of contestability regarding third-party content and services.

Recital 61 notes:

“In those circumstances, the gatekeeper is in a dual-role position as intermediary for third party undertakings and as undertaking directly providing products or services. Consequently, such gatekeepers have the ability to undermine directly the contestability for those products or services on those core platform services, to the detriment of business users which are not controlled by the gatekeeper.”

Recital 52 of the DMA continues:

“... the gatekeeper should not engage in any form of differentiated or preferential treatment in ranking on the core platform service, and related indexing and crawling, 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, the conditions that apply to such ranking should also be generally fair and transparent. Ranking should in this context cover all forms of relative prominence, including display, rating, linking or voice results and should also include instances where a core platform service presents or communicates only one result to the end user. To ensure that this obligation is effective and cannot be circumvented, it should also apply to any measure that has an equivalent effect to the differentiated or preferential treatment in ranking...”

Including instances in which only one result is presented, fits the Amazon Buy Box as well as voice assistants, where it is rather cumbersome for end users to be presented more than one choice at a time.



It is worth noting, however, that **it can be challenging to detect self-preferencing bias as opposed to legitimate differential treatment**. Differential treatment may be legitimate because of quality or match value differences between first-party and third-party offers. Detection can be particularly challenging when rankings are based on self-learning algorithms. Digital platforms may benefit from guidance by the European Commission about what kind of evidence is required to justify differential treatment of similar offers. For example, Amazon may be able to provide evidence that end users typically prefer products from sellers that use ‘Fulfilment by Amazon’. To what extent would such evidence justify more favourable treatment of products with ‘Fulfilment by Amazon’ (when assigning the buy box) and thus show its compliance with Article 6(5)?

To summarise, when applying Art 6(5), the **European Commission must make a judgement on the meaning and scope of self-preferencing; and has a discretionary power as to which possible/potential violations of the prohibition it will examine at all**. Moreover, since gatekeeper platforms have to show compliance, the European Commission may want to provide guidance on practices that are, and those that are not, compliant. Even though Article 6(5) is framed as a general prohibition, **economic analysis can help to distinguish between self-preferencing bias and legitimate differential treatment of different offers**. Economic analysis **may also play a useful role when considering the specification of the prohibition**, by evaluating the effects of different measures and whether they are in line with the overall objectives of the DMA. This is in line with the principles of proportionality and effectiveness, as some restrictions are more severe than others and may lead to worse outcomes for third-party business users, end users, and society at large. At the same time, the use of economics to specify the DMA prohibition does not imply the re-introduction of an antitrust efficiency defense, which has been explicitly excluded under the DMA.⁸¹

⁸¹ DMA, Recital 10.



3. SELECTED INTERNATIONAL COMPARISON: APPROACHES TO DEAL WITH SELF-PREFERENCING

The issue of self-preferencing has appeared in several jurisdictions. Most noteworthy is the new competition tool in Section 19a of the German Competition Act that came into force at the beginning of 2021, which opens the way to prohibit self-preferencing practices by platforms considered to be of “paramount significance for competition across markets” on a case-by-case basis. In the UK, while competition law has not been modified, through the use of market studies and market investigations⁸² there is a competition policy tool available to address self-preferencing (that does not require running an abuse case). The market study on mobile ecosystems is mentioned below as an example. Finally, we comment on the US.

3.1 Self-Preferencing in the German Competition Act (GWB)

An interesting comparison is the treatment of self-preferencing in the quasi-regulatory tool of Section 19a in the German Competition Act regarding platforms that are of “paramount significance for competition across markets”. According to Section 19a, subsection (2) of the GWB,

“the Bundeskartellamt may prohibit such undertaking from

1. favouring its own offers over the offers of its competitors when mediating access to supply and sales markets, in particular

a) presenting its own offers in a more favourable manner;

b) exclusively pre-installing its own offers on devices or integrating them in any other way in offers provided by the undertaking”⁸³

Presenting own offers more favourably is regarded as a (potentially) abusive foreclosure because this may prevent third-party providers from developing and marketing innovative offers and thus restricts ‘competition on the merits’ (Franck and Peitz, 2021, p. 519).

If a behaviour falls under this category of self-preferencing, this indicates an anticompetitive potential, but does not fall under a per se prohibition. It must **only be prohibited on a case-by-case basis after a careful balancing of potential competitive and welfare effects** (Franck and Peitz, 2021, p. 521). As Franck and Peitz (2021, p. 526) conclude, “the appropriate application of section 19a of the Competition Act requires a detailed case-by-case analysis, including a thorough evaluation of the market position and the scrutinised conduct of the addressed undertaking and, more specifically, allows the latter to justify its behaviour and to invoke an efficiency defence in doing so.”

⁸² For institutional details, see e.g. Wish (2022).

⁸³ The pre-installation of apps is covered by Art. 6(3) in the DMA (see also recitals 49-53), which differs from Section 19a, subsection (2)(b) GWB.



3.2 Self-Preferencing According to the CMA

In its market study on mobile ecosystems, the Competition and Markets Authority (CMA) develops a broad definition of self-preferencing practices in the context of such ecosystems and expresses the following concerns:

“The main ways in which Apple and Google may be able to self-preference their own apps or services are:

- *biasing consumer choice: using choice architecture to make consumers more likely to choose their products;*
- *giving their own products a non-replicable quality advantage: either by degrading rivals’ quality or by improving their own products in ways that are not accessible to rivals (e.g. better integration with the platform);*
- *raising rivals’ costs: through the fees charged for use of their platforms (which they don’t pay themselves) or through making it more costly in other ways to access the platform compared to their own products; and*
- *using information gained from app developers by virtue of their positions as gatekeepers: which may in the long run harm third-party developers’ incentives to innovate.”* (CMA, 2022, p. 185)

The third type of practice concerns the gatekeeper’s price decision, the other three relate to non-price strategies. However, this is not a general definition of self-preferencing practices but is context-specific. Article 6(5) of the DMA corresponds to biasing consumer choice.

3.3 A Look Across the Atlantic

In the United States, there is an **ongoing debate in Congress on whether to prohibit the dual mode for certain platforms**, which would be a clean, but draconian intervention in response to self-preferencing. The Ending Platform Monopolies Act was introduced in the U.S. House of Representatives in June 2021. According to this Act, large platforms will be prohibited from selling first-party products or apps in competition with third-party sellers or developers on their marketplaces. The American Innovation and Choice Online Act (AICO),⁸⁴ introduced in the U.S. Senate, would **restrict self-preferencing practices** of large digital platforms. The Open App Markets Act (OAMA), also introduced in the U.S. Senate, targets mobile app stores and operating systems,

⁸⁴ American Innovation and Choice Online Act, S. 2992, 117th Cong., version from February 3, 2022. Available at: <https://www.congress.gov/bill/117th-congress/senate-bill/2992/text>. Several types of self-preferencing practices are considered unlawful in this act. This includes the following practices: “*prefer the products, services, or lines of business of the covered platform operator over those of another business user on the covered platform in a manner that would materially harm competition*” (Sec. 3.a.1) and “*in connection with any covered platform user interface, including search or ranking functionality offered by the covered platform, treat the products, services, or lines of business of the covered platform operator more favorably relative to those of another business user than under standards mandating the neutral, fair, and nondiscriminatory treatment of all business users*” (Sec. 3.a.9).



prohibits some specific self-preferencing practices, and goes against “walled gardens” in which all app transactions must run through a single app store.⁸⁵ For a critical assessment, see Hovenkamp (2022).

Self-preferencing has also received some attention in antitrust proceedings both by the agencies and private lawsuits. In 2013, the **FTC settled with Google in its investigation of Google Search**. It found that: *“A key issue for the Commission was to determine whether Google changed its search results primarily to exclude actual or potential competitors and inhibit the competitive process, or on the other hand, to improve the quality of its search product and the overall user experience [...] The totality of the evidence indicates that, in the main, Google adopted the design changes [...] to improve the quality of its search results, and that any negative impact on actual or potential competitors was incidental to that purpose.”*⁸⁶ (Later in this issue paper we provide some examples from Europe.)

An example of a private lawsuit is the ongoing case brought by online video platform **Rumble against Google** in which the former alleges that Google is engaged in anticompetitive behaviour by self-preferencing own content in its organic search: Rumble claims that Google manipulates *“algorithms (and/or other means and mechanisms) by which searched-for-video results are listed, Google [...] [ensures] that the videos on YouTube are listed first, and that those of its competitors, such as Rumble, are listed way down the list on the first page of the search results, or not on the first page at all.”*⁸⁷ Google’s motion to dismiss the case was denied on July 29, 2022.

⁸⁵ Open App Markets Act, S. 2710, 117th Cong., amendment from February 22, 2022. Available at: <https://www.congress.gov/bill/117th-congress/senate-bill/2710/text>. According to the Act, *“A covered company shall not provide unequal treatment of apps in an app store through unreasonably preferencing or ranking the apps of the covered company or any of its business partners over those of other apps in organic search results ... Unreasonably preferencing (A) includes applying ranking schemes or algorithms that prioritize apps based on a criterion of ownership interest by the covered company or its business partners; and (B) does not include clearly disclosed advertising.”*

⁸⁶ Federal Trade Commission, Statement of the Federal Trade Commission Regarding Google’s Search Practices, In the Matter of Google Inc., FTC File number 111-0163; January 3, 2013, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commission-regarding-googles-search-practices/130103brillgooglesearchstmt.pdf.

⁸⁷ U.S. District Court Northern District of California, Rumble v. Google, Order Denying Motion to Dismiss and Strike, Case No. 21-cv-00229-HSG, p.2.



4. CASES OF SELF-PREFERENCING IN EU AND MEMBER STATES

The prohibition of self-preferencing has been motivated by past experiences.⁸⁸ In the impact assessment study commissioned by the European Commission, Sunderland et al. (2020, Annex 1) give several examples of self-preferencing in rankings and listings as unfair practices, which are reported in Table 1.⁸⁹

Table 1: Examples of self-preferencing according to Sunderland et al. (2020)

AMAZON	<ul style="list-style-type: none"> Investigation by the Italian National Competition Authority (NCA) (influencing listings for companies using Amazon fulfilment)
APPLE	<ul style="list-style-type: none"> Preferential display/advertising of Apple Music
GOOGLE	<ul style="list-style-type: none"> Google shopping case (influencing listings), job search feature, concerns over travel listings Pre-installation of Chrome on Android Refusal to list competing app on auto services (Italian NCA)

This illustrates the concern with self-preferencing from the outset, but sheds little light on what exactly is the issue and what are meaningful remedies. To see concrete examples of self-preferencing in practice and how agencies have dealt with them under competition law, it is useful to mention a few cases in the EU as examples (this is not a complete list).

4.1 Cases at the European Commission

A few competition cases at the European Commission address self-preferencing. What are they about?

In 2017 the European Commission fined Google with 2.4 billion Euro for hampering competition through **self-preferencing its Google Shopping offers** (case COMP/AT.39740). The European Commission wrote: *“Google has systematically given prominent placement to its own comparison shopping service: Google’s comparison shopping results are displayed, in a rich format, at the top of the search results, or sometimes in a reserved space on the right-hand side. They are placed above the results that Google’s generic search algorithms consider most relevant. This happens whenever a consumer types a product-related query into the Google general search engine, in relation to which Google wants to show comparison shopping results. This means that Google’s comparison shopping*

⁸⁸ For a discussion of case law in the EU, see Ibáñez Colomo (2020).

⁸⁹ The authors wrote: “The prevalence of unfair practices by large gatekeeper platforms is evidenced not only in the number of cases that have been investigated by competition and other authorities, but also from common themes raised by interviewees and in case studies prepared in the context of this study.”



*service is not subject to Google's generic search algorithms.*⁹⁰ They continue as follows: “Evidence shows that even the most highly ranked rival comparison shopping service appears on average only on page four of Google's search results, and others appear even further down. In practice, this means consumers very rarely see rival comparison shopping services in Google's search results.” The European Commission thus considers Google's self-preferencing behaviour to be anticompetitive leverage of its dominant position in general search into comparison shopping.⁹¹

In November 2020 the European Commission started an antitrust proceeding against **Amazon regarding self-preferencing when assigning its buy box** (case COMP/AT.40703). The Commission is concerned about the “conditions and criteria that govern the selection mechanism of the Buy Box that prominently shows the offer of one single seller for a chosen product on Amazon's websites, with the possibility for consumers to directly purchase that product”⁹² Amazon may favour its own products or third-party sellers that make use of the ‘Fulfilment by Amazon’ (FBA) service. In July 2022 Amazon made a commitment proposal to the European Commission that addressed, among others, the Commission's concern about self-preferencing when assigning the buy box, which Amazon calls a Featured Offer. Amazon offers the following: “if a Featured Offer is displayed, Amazon will apply non-discriminatory conditions and criteria for the purposes of determining which Offer, whether from Amazon Retail or Sellers (including Sellers using FBA), will be displayed as the Featured Offer [...] Amazon will remove Prime as a relevant criterion for the selections of the Featured Offer.”⁹³ This case shows that in a standard antitrust proceeding it is possible to obtain a commitment offer as a remedy to address alleged self-preferencing. However, some questions remain. First, it is unclear how effective such a commitment will be. Here, one may argue that the DMA offers better monitoring possibilities. And second, it is also unclear whether Amazon would have been equally forthcoming if the DMA was not about to be enacted.

4.2 Cases in Member States

Several EU Member States have run or are running their own investigations that include concerns about self-preferencing practices. The Amazon case initiated by the European Commission applies to the whole European Union except Italy, the reason being that Italy initiated its own case against Amazon earlier. The **Italian NCA reached a decision in its case against Amazon** in November 2021.⁹⁴

The directly affected parties are Amazon.it, third-party sellers on the marketplace, and independent logistics service providers offering its services to third-party sellers. As Lombardi (2022) puts it, “currently, a third-party seller active on Amazon can manage the logistics of its products in two ways. It can independently operate the storage, logistics, and delivery; or outsource it to an independent operator. This operator can be Amazon itself, or another firm. If the seller decides to use Amazon's logistics network (ALN), they are requested to purchase a service called ‘Fulfilled by Amazon’ (FBA). If

⁹⁰ Quote from “Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service – factsheet,” 27 July 2017. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1785

⁹¹ For some discussion including the effectiveness of the remedies, see Bourreau and Krämer (2019).

⁹² Quote from https://ec.europa.eu/competition/antitrust/cases/dec_docs/40703/40703_67_4.pdf

⁹³ Amazon, Case COMP/AT.40462 and Case COMP/AT-40703. Commitment Proposal. July 7, 2022.

⁹⁴ Italian Antitrust Authority decision A528, 30 November 2021. This case is summarised by Lombardi (2022).



they entrust an independent logistics firm instead, Amazon defines the operation as a ‘Merchant Fulfilment Network’ (MFN). FBA is an integrated logistics service that includes: (i) warehousing and inventory management for retailers at Amazon’s distribution centres; (ii) fulfilment of orders received on Amazon.it, including packaging and labelling; (iii) shipping, transportation, and delivery; (iv) returns management; and (v) customer service.” In more general terms, Amazon engages in mixed bundling, as third-party sellers can access the marketplace by buying the bundle of marketplace access and FBA or just buying marketplace access from Amazon and logistics services elsewhere. The issue of self-preferencing arises in the way Amazon treats third-party sellers with FBA compared to those without it. Lombardi (2022) writes: “The advantages of FBA are, in particular: (i) non-application of performance metrics to third-party sellers; (ii) obtaining the Prime badge; (iii) higher probability of being awarded the buy box; (iv) possibility to participate in special events and offers; and (v) eligibility for ‘Free Shipping via Amazon’.” With those advantages afforded to third-party sellers opting for FBA, Amazon might leverage its dominant power as a marketplace provider to monopolize the market for e-commerce logistics services. This may also make entry and scaling up of competing marketplaces more difficult.

In 2018, the **German Bundeskartellamt also opened proceedings against Amazon** for a number of reasons (Case B2 – 88/18); the case was closed in 2019 after Amazon changed some of its practices, including some which fall under the label of self-preferencing.⁹⁵ In light of the question how to deal with the prohibition of self-preferencing, the following statement by the Bundeskartellamt is noteworthy: “The Bundeskartellamt sees that there is a considerable risk of misuse, misrepresentation and manipulation of ratings, which is detrimental to both customers and for competing sellers. Amazon has shown a strong and justifiable interest in combating such inauthentic reviews (“fake reviews”). The Office has therefore refrained from making further demands ...” A possible conclusion is that a careful assessment of practices that may treat first-party and third-party offers differently is needed and that it is to be avoided that a prohibition of self-preferencing increases the problem of fake reviews.⁹⁶

In 2019, the **Dutch NCA completed a market study on mobile app stores** and several instances of self-preferencing are mentioned in the report.⁹⁷ As documented in that report, Apple claims that “... favouring their own apps over third-party apps would not be rational, even though they pre-install their own apps on their own devices. If a third-party offers a higher quality app, Apple has no incentive to hinder the app in any way. Apple earns the majority of its money from devices, and therefore wants to offer the best services possible to its users.” (p. 84) While discriminatory pre-installation and access to APIs can be seen as self-preferencing practices in a broad sense, they do not fall under Article 6(5)

⁹⁵ In its case summary, the Bundeskartellamt writes (own translation) : “With regard to product reviews, sellers have criticised the fact that product reviews obtained via third-party providers – so-called review clubs - are no longer posted or deleted from the platform, while the reviews generated by Amazon itself via its own review programme “Vine” continue to be published, although here too the reviewers are not paid directly but at least receive the test product free of charge. Since the Vine programme has so far only been Vendors, i.e. the suppliers of Amazon Retail, the Office saw this as a disadvantage for the marketplace dealers and a leverage effect to supply Amazon Retail. This applies in particular to new products for which no other for which no other admissible customer reviews - e.g. via verified purchases - are available. At the instigation of the Bundeskartellamt, Amazon will therefore promptly open the Vine programme for marketplace traders who are trademark right holders or authorised representatives and gradually expand the capacities required for this.”

⁹⁶ In 2020 the Bundeskartellamt completed a sector inquiry on reviews and ratings. However, self-preferencing was not part of the investigation.

⁹⁷ Netherlands Authority for Consumers & Markets, Market study into mobile app stores. Case no.: ACM/18/032693, April 11, 2019.



of the DMA, but can be addressed by other DMA obligations, particular Articles 6(3) and 6(4) (and they do fall under the broader provision of Section 19a of the German Competition Act). The report also mentioned the importance of the visibility of apps in the app store but did not dig deeper.

Lastly, in June 2022, the German Bundeskartellamt opened proceedings under Section 19a against Apple about its tracking rules that appear to discriminate between first-party and third-party apps within its “App Tracking Transparency Framework”. According to the Bundeskartellamt, *“Apple’s rules have raised the initial suspicion of self-preferencing and/or impediment of other companies.”*⁹⁸

⁹⁸ Bundeskartellamt, press release “Bundeskartellamt reviews Apple’s tracking rules for third-party apps,” 14 June 2022.



5. INTERPRETING THE DMA PROHIBITION: THE ECONOMICS OF SELF-PREFERENCING

The case against self-preferencing may look clear from a theory point of view to the extent that it amounts to unequal treatment of equal offers. As such, **several economists have taken the view that self-preferencing should, in general, be prohibited**. For instance, Cabral et al. (2021, p. 14) have written: *“We would suggest that any form of discrimination against third parties be deemed unlawful. In other words, we believe self-preferencing is a natural candidate for the ‘blacklist’ of practices to be deemed anti-competitive and ‘per se’ disallowed.”* Such an unequivocal statement from a diverse set of academic economists is quite remarkable.⁹⁹ In their report to Commissioner Vestager, another group of academics (only one of whom is an economist) are more careful: *“In a market with particularly high barriers to entry and where the platform serves as an intermediation infrastructure of particular relevance, we propose that, to the extent that the platform performs a regulatory function, it should bear the burden of proving that self-preferencing has no long-run exclusionary effects on product markets.”* (Crémer et al., 2019, p. 7)

Economists have provided formal frameworks that allow to assess the incentives of platforms to enter the dual mode and the welfare effect of such a change of business model. Furthermore, formal frameworks can help to understand the platform’s incentives to favour certain sellers (including first-party products and services) and what are the competitive and welfare effects of such practices. Earlier work on tying and refusals to deal can also shed light on the effects of self-preferencing. Furthermore, empirical work can identify instances of practice that may be classified as self-preferencing (it partly has done so) and, possibly, work out what have been the consequences of such behaviour.

5.1 First- and Third-Party Offers: The Economics of the Dual Mode

Before taking a look at self-preferencing as a non-price strategy, it is useful to reflect on the role of first-party offers in shaping competition on the platform.

If the platform sells first-party products it is said to operate in *dual mode*. In the policy debate, sometimes the prohibition of this dual mode has been advocated (for instance, Khan, 2017, 2019) and this has received some support in the House in the US.¹⁰⁰ With such a prohibition in place, the platform has to either become a pure retailer or drop first-party offers and become a pure marketplace. An analysis of the economic forces at play reveals that **a prohibition increases consumer welfare under some conditions but does the opposite under others**.

Consider a setting in which a platform charges sellers for the transactions on a platform. A possible defence for the practice of introducing first-party offers is that a platform may want to provide an anchor for retail prices of third-party sellers. This is of particular relevance in markets with little

⁹⁹ The same set of authors acknowledge difficulties when trying to implement such a prohibition.

¹⁰⁰ According to the Ending Platform Monopolies Act, which was introduced in the U.S. House of Representatives in June 2021, large platforms will be prohibited from selling first-party products or apps in competition with third-party sellers or developers on their marketplaces.



competition between third-party sellers.¹⁰¹ In this case, the platform as a guardian of the ecosystem may be worried about consumers receiving a bad deal and therefore introduce a first-party product to stimulate competition. This may be a more attractive option for the platform than lowering fees charged to sellers; in particular, if such fee reductions are not fully passed through to consumers. In such a case, a platform is particularly inclined to introduce those first-party offers for which it has a cost or quality advantage over third-party sellers.

Economic theory has looked at a number of market environments. Take the formal setting proposed by Anderson and Bedre-Defolie (2021), as it delivers a clear-cut result. A monopoly firm can operate as a pure retailer, as a platform running a marketplace with third-party sellers, or as a platform in dual mode running a marketplace on which it also sells products as a retailer itself. A platform in dual mode sets the retail price of its own product and a percentage transaction fee; third-party sellers observe these prices and decide whether to enter and, if so, set their retail prices; finally, buyers make purchasing decisions. In that setting, prohibiting the dual mode increases consumer surplus if and only if the prohibition leads to a pure marketplace.¹⁰²

If the marketplace operates for product categories in which innovative sellers may appear, the marketplace helps with the discovery process by consumers and limits the market power of an innovative seller. In the formal model developed by Hagiu et al. (2022), this implies that the dual mode always gives higher consumer welfare than the pure marketplace. Furthermore, a ban on the dual mode never increases consumer welfare.¹⁰³ While the prohibition of the dual mode is not considered in the DMA, burdensome remedies to combat self-preferencing and legal risks may lead platforms to opt out of the dual mode altogether.¹⁰⁴

Instead of prohibiting the dual mode, a regulator may prefer to impose a cap on the fee the platform can charge to sellers.¹⁰⁵ Such an intervention is common practice in a number of network industries and may be worth considering in the case of gatekeeper platforms.¹⁰⁶ While less intrusive than a prohibition of the dual mode, it is a challenge for the regulator to appropriately choose the rate, as the optimal rate differs across product and service categories. What is more, the platform may be able to circumvent this cap by imposing charges somewhere else in the value chain – creating a whack-a-mole problem – it may use non-price instruments and direct consumers to more profitable sellers if

¹⁰¹ Take as an extreme case a situation of full seller collusion and step demand, which implies that sellers will charge the monopoly price that is independent of the level of the fee charged by the platform.

¹⁰² In recent empirical work, Crawford et al. (2022) empirically assess the effect of Amazon's retail entry competing against third parties offering the same product. They find that entry is correlated with high growth and a low degree of competition. Overall, they read their findings as Amazon internalizing externalities, which makes the platform more attractive to consumers. A different market expansion effect can arise if a platform invites entry of successful offline brands (see Jin et al. 2022).

¹⁰³ Other contributions include Hagiu and Spulber (2013) and Etro (2021a). Etro (2021b) and Jeon and Rey (2021) investigate how the platform's monetization model affects its incentives to enter with first-party content and the incentives of third-party developers.

¹⁰⁴ Short of abandoning the dual mode, the gatekeeper may replace factor-based ratings by ratings that are determined via a payment-based mechanism (if this is seen as compliant); for example, Amazon's buy box could be assigned via an auction. Such a change raises challenges of its own, see Feasey and Krämer (2019, Section 4.3).

¹⁰⁵ Fee regulation as a remedy to competition concerns in dual mode has been formally investigated by Hervas-Drane and Shelegia (2022) and Wang and Wright (2022).

¹⁰⁶ As an instance of selective fee regulation applied to digital platforms, several US cities capped fees charged to independent restaurants by on-demand delivery platforms at 15%. See Li and Wang (2021) for details.



fee regulation is applied selectively,¹⁰⁷ and it may change its business model and rely more on advertising. These regulation-induced changes may thus play out to the detriment of consumers. At this point, the DMA does not explicitly mention price regulation. However, two qualifications are due. First, Article 6(12) of the DMA imposes FRAND access to app stores, online search engines, and social networks, which is a weak form of price regulation. Second, regulatory pressure on transaction fees may come from abuse cases and thereby, rest within the competition policy realm. It is worth noting that any public pressure on the fees a platform can charge to sellers increases the incentives of platforms to engage in practices of self-preferencing using non-price instruments.

When operating in the dual mode, the platform may use information on the success of third-party sellers to decide in which product category to enter.¹⁰⁸ Some researchers have looked at the dynamic effects this might have. First, a third party may anticipate the platform's imitation decision in case of high demand and hide information related to demand (Jiang et al., 2011). Alternatively, third-party sellers may reduce investment¹⁰⁹ or opt for product categories in which it is known that demand is low so that the risk of the platform entering with a first-party product is also low. To address the concern of underinvestment and distorted entry by third-party sellers because of the imitation threat, a possible remedy is to ban the platform (or at least its first-party division) from having access to any private information generated by the third-party seller (see Hagiu et al., 2022). However, a platform with access to this information may operate more efficiently and just banning the first-party division from accessing this information may be difficult to enforce. Another possible remedy is to prohibit the platform from entering new product categories with first-party products for a certain amount of time (see Madsen and Vellodi, 2022, for a formal analysis). While relevant in the broad context of self-preferencing, these insights have no bearing in relation to Article 6(5).

5.2 Competitive Effects of Self-Preferencing

Recent contributions of economic theory have shed light on the incentives of platforms to steer consumers to first-party products.¹¹⁰ When we talk of favouring own products and services it is important to define what a neutral platform practice (that is, a neutral ranking or neutral recommendation) would be. If end user benefit is the ultimate goal, the consumer welfare standard applied to end users appears to be the right criterion to follow.¹¹¹ Then, **the prohibition of self-preferencing would mean that a platform is prohibited from using practices that steer users to first-party products when this is not in the interest of end users.** For example, if a consumer could get a lower price for the same service quality from a third-party seller, then steering consumers towards a first-party product would violate the self-preferencing prohibition. The issue gets more complicated

¹⁰⁷ In the case of fee caps for independent restaurants on on-demand delivery platforms, Li and Wang (2021) find that chain restaurants, which after the introduction of caps continue to pay high fees, benefit from this intervention, while independent restaurants that were supposed to benefit from the regulation, lose. This can be seen as an indication that the platform responded by favouring chain restaurants after the regulation took effect and, thus, steering more consumers towards chain restaurants.

¹⁰⁸ Platforms such as Amazon marketplace generate information which products or product categories are particularly successful. Zhu and Liu (2018) provide empirical evidence that Amazon is more likely to enter as a first-party seller into more-successful product spaces.

¹⁰⁹ For some evidence in the mobile app market, see Wen and Zhu (2019).

¹¹⁰ The literature started with de Cornière and Taylor (2014). More recent contributions include Drugov and Jeon (2017), Bourreau and Gaudin (2022), de Cornière and Taylor (2019), Padilla et al. (2022), Zenny (2022).

¹¹¹ The consumer welfare standard is not limited to taking only price effects into account.



when products or services are differentiated, and consumers have different tastes about those products or services. For example, if some consumers have a strong taste for quick delivery, while others do not, it becomes difficult to assess when actual recommendations violate the self-preferencing prohibition (see also Section 2). What is more, what is in the interest of consumers in the short run may not be in their long-run interest: By recommending new products and services (which may be first-party or third-party offers) the platform may learn about correlations in consumer tastes (Che and Hörner, 2018). When the platform deviates from consumer-optimal rankings and recommendations given the current information, consumers may overall benefit due to the additional information gathering by platforms. This begs the question how to define neutral rankings and recommendations and, thus, the absence of self-preferencing.

Absent any restriction on fees, before trying to figure out when and how platforms engage in self-preferencing and what are the effects on consumer welfare, one may ask in the spirit of the Chicago School why at all there could be consumer welfare-reducing self-preferencing. Suppose that a platform in dual mode sells its own products and runs a marketplace for third-party sellers. Clearly, this platform has the option to drop the marketplace and operate under full vertical integration. In this case it would earn monopoly rents on its vertically integrated products. Thus, if it decides to open a marketplace (even when heavily using self-preferencing), the platform must gain from this (at least in the long run). Operating in dual mode, the platform may guide consumers to its own product more often than what is in the interest of consumers, at given prices. We would call this self-preferencing. However, the platform could also increase its fee charged to sellers.¹¹² Sellers will at least partially pass this fee increase on to consumers. By doing so, the platform reduces the degree of self-preferencing when keeping its recommendation policy unchanged and increases its profit.

The **trade-off faced by the platform** can be explained differently. Suppose that the platform aims at offering an expected net benefit to a consumer. It has **three instruments** to do so: **the retail price of its own product; the fee charged to sellers; and its steering policy that can be thought of as affecting the visibility of third-party products.** With reduced visibility of third-party products, consumers will sometimes buy the first-party product even though, at given prices, consumers would prefer to buy from a third-party seller. When further reducing visibility, which increases the profit from selling the first-party product, but reduces the profit that stem from the fee charged to sellers, the platform has to compensate the consumer somehow to keep the consumer's net benefit unchanged.

Why would a platform in dual mode “manipulate” recommendations when it could increase its fee charged to sellers? Economists have engaged formal models to better understand the incentives of a platform to provide recommendations.¹¹³ **Incentives for self-preferencing are particularly strong in**

¹¹² For a related discussion, see Feasey and Krämer (2019, sections 2.2 and 2.3).

¹¹³ Several contributions provide formal arguments that platforms as pure intermediaries may provide recommendations that are not in the best interest of consumers. For work in the context of search engines, see Hagiu and Jullien (2011, 2014) and de Cornière and Taylor (2014). More broadly, see Heidhues et al. (2020), Lee (2021), and Peitz and Sobolev (2022). For overviews that address the incentives of a platform which recommendations to give, see Belleflamme and Peitz (2018, 2021). Hagiu et al (2022) provide a formal argument in the dual mode setting (used e.g. by Amazon and Apple App Store). They show that self-preferencing allows the platform to address the problem of bypass that otherwise limits the fees it can charge third parties. Thus, they show that self-preferencing can result in higher fees and prices.



cases in which the platform is not free to change the fee it charges to sellers. Most obviously, this is the case if that fee is zero. An example is the Google Shopping case (see above) in which there are no fees for organic search results and, therefore, strong incentives for Google to bias organic search results in favour of first-party offers.

An important observation is that even a platform that only runs a marketplace and does not provide own products and services does not necessarily provide recommendations in the best interest of consumers (of course, it will not ignore consumer benefits altogether). This is most easily seen when the platform does not charge users directly and only extracts some of the surplus generated by sellers. In the context of search engines, this has been noted by Brin and Page in 1998: *“we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers”* (Brin and Page, 2012, p. 3832). Furthermore, sellers may differ in their ability to extract rents from consumers (who will be active on the platform in any case) and therefore a platform may favour those sellers that are better at extracting such surplus. Hence, it is an illusion to think that prohibiting the platform favouring its own products will necessarily result in recommendations that are in the best interest of consumers.

5.3 Economists Empirically Assessing Self-Preferencing in the Real World

Few economic studies have gathered evidence on self-preferencing. While more empirical work is needed, **there are strong indications that some platforms engage in practices that may be called self-preferencing, but that this is not always consumer welfare detrimental.** These and future works may help the European Commission in developing a more refined view on which practices it will eventually classify to constitute self-preferencing (by distinguishing between which practices are harmful and which ones are beneficial to consumers).

Chen and Tsai (2022) look at Amazon’s recommendations through its ‘Frequently Bought Together’ algorithm distinguishing between products sold by Amazon as a retailer, by sellers as part of the ‘Fulfilment by Amazon’ (FBA) program, and non-FBA sellers. The authors conclude that the steering via Amazon’s FBT algorithm is driven by seller identity rather than consumer preference. In other words, Amazon manipulated the FBT algorithm in such a way that a given product is more likely to be recommended if it is available through Amazon as a retailer (controlling for seller characteristics).

Other work has looked at Amazon’s algorithm that assigns a particular offer to its buy box, which is a powerful instrument to guide consumers.¹¹⁴ Lee and Musolff (2021) empirically evaluate the effect of Amazon’s use of the buy box on consumer welfare using high-frequency data with the help of a structural model. They do find evidence of self-preferencing by Amazon. However, this self-preferencing increases consumer welfare because, everything else given, consumers appear to prefer the product sold by Amazon instead of a third-party seller. Lee and Musolff (2021) also endogenize

¹¹⁴ According to the U.S. Senate Judiciary Committee, “Amazon can give itself favorable treatment relative to competing sellers. It has done so through its control over the Buy Box.”



the entry and exit of sellers and find that, in the long-run, the impact of self-preferencing on consumer welfare is negligible relative to the short-run effect (it remains positive though).

Overall, Lee and Musolff (2021) find strong evidence of self-preferencing, which may be seen as water on the mills of policy makers and competition authorities going after Amazon. However, as they clearly show, self-preferencing may be a good thing for consumers.

An interesting feature is that Amazon does not always assign the buy box. Lee and Musolff (2021) attribute this to situations in which no attractive offers are available, which can be seen as a mechanism to encourage third-party sellers to make more attractive offers. Hunold et al. (2022) take a closer look at this buy box suppression. They observe that the buy box is always assigned when Amazon is one of the sellers, while this is not the case in 39% of all instances in which only third-party sellers offer the product. As they infer, Amazon's algorithm in charge of assigning the buy box has the feature that the associated probability is higher when third-party sellers that offer a certain quality are present and when the best price is lower. The key finding is that, if Amazon were to apply the same standard to itself, it should not assign the buy box in about 13% of instances when it is present.

Self-preferencing has also been found in the context of hotel booking. This has appeared at two layers of the value chain. First, self-preferencing has been shown in the way meta search engines such as TripAdvisor recommend hotel offers on different hotel booking portals. The issue of self-preferencing arises in this context because several meta search engines are owned by hotel booking portals (Booking.com acquired Kayak in 2013, for instance). Cure et al. (2022) find that the online hotel-booking portals belonging to the holding company of Booking.com have a higher probability to be visible in the meta search and to be highlighted than competing portals.¹¹⁵

Second, self-preferencing may refer to the way hotel booking platforms rank different hotels. Hunold et al. (2020) provide empirical evidence that hotels rank worse on hotel booking portals if their price is lower on competing channels (on hotel website or competing hotel booking portals).¹¹⁶ Here, the ranking algorithm appears to respond to the fact that consumers are more likely to bypass the portal and book elsewhere if they find lower prices outside the portal. The portal offers consumers discovery tools and a booking service and charges hotels for transactions between hotel and consumer. A hotel that is more expensive elsewhere (and, in the extreme, exclusive to the platform) is attractive for the portal because for (almost) any hotel booking the portal's own booking service will be consumed. By contrast, a hotel that offers better terms elsewhere is less attractive for the portal, because with a positive probability the portal's booking service will not be consumed. Thus, by favouring the former over the latter hotel, the portal increases the likelihood that its own booking service will be consumed. This amounts to self-preferencing (similar to Amazon favouring FBA sellers), and such differential treatment of different hotels is not in the best interest of consumers.

¹¹⁵ This is the outcome of linear regressions with fixed effects. Furthermore, the authors find that hotels appear on average about eight positions further down the list in the Kayak search results when the hotel price is lowest on an online hotel-booking portal belonging to the Expedia conglomerate.

¹¹⁶ For a discussion, see Belleflamme and Peitz (2021, pp. 208-209).



It is important to note that recommendations based on conversion rates may lead to such an outcome. In general, a higher conversion rate suggests that a hotel is a better match and thus recommending products with higher conversion rates appears to benefit consumers. However, when consumers find lower prices for a hotel elsewhere, a low conversion rate does not indicate that consumers are less interested in this hotel. An algorithm that works in the best interest of consumers would have to take such lower-priced offers outside the platform into account and rank hotels with such offers better than an algorithm that is only based on conversion rates.¹¹⁷

Yet another instance of a platform as a recommender that affects consumer choice is Spotify. As Aguiar and Waldfogel (2021) empirically show, Spotify's popular playlists (some of them algorithmic, others curated) have a strong influence on music streaming. Apart from other reasons for biased recommendations, self-preferencing could be of concern given that major music labels hold minority stakes in Spotify. However, Aguiar and Waldfogel do not find evidence that Spotify is biasing music consumption towards major labels.

¹¹⁷ As this example demonstrates, when deciding whether a practice constitutes self-preferencing, the European Commission may have to take a stance whether a gatekeeper platform can be forced to use certain data as input in their recommendation algorithm (in the concrete example, this would be the prices charged by hotels outside the platform).



6. CONCLUSION

Self-preferencing sounds wrong. Stating that an interested party should not be the referee sounds obvious. However, **platforms in dual mode are concerned about the well-functioning of the ecosystem they manage. A regulator imposing a certain behaviour on platforms, which may amount to picking a particular market design, runs the risk of not acting in the best interest of consumers, especially in the long term, which is the ultimate goal of market contestability.**

The prohibition on self-preferencing as formulated in Article 6(5) of the DMA requires context. The European Commission and the courts would therefore be well-advised **not to use this prohibition as carte blanche and engage in mechanistic enforcement.** Instead, the DMA could be **used to identify those acts of self-preferencing that are likely to be against market contestability and the long-term interest of consumers, and use guidance from economics to specify adequately, under Article 8 of the DMA, the self-preferencing prohibition.**¹¹⁸ This requires an understanding of when consumers consider a first-party offer superior to similar third-party offers. Giving prominence to a superior first-party offer should not be seen in conflict with Art 6(5), as such behaviour coincides with the one of a gatekeeper who acts in the best interest of consumers. Recent cases under competition law may provide further insights about possible harms and benefits, as well as the appropriate choice of remedies, and economic analysis can provide a better understanding of which practices under which circumstance are likely to be consumer welfare decreasing.

Platforms can make life difficult for third-party sellers by **using price and non-price instruments.** Thus, in the context of self-preferencing, an effective policy against foreclosure and refusal to deal may **require a combination of Articles 6(5) and 6(12).** Specific commitments must be seen in a broader context to avoid circumvention through other means.

¹¹⁸ For a discussion of remedies, see Feasey and Krämer (2019). As explained above, the use of economics to specify the DMA prohibition does not imply the re-introduction of an antitrust efficiency defense which is explicitly excluded under the DMA.



REFERENCES

- Aguiar, L. and J. Waldfogel (2021). Platforms, power, and promotion: Evidence from Spotify playlists. *Journal of Industrial Economics*, 69, 653-691.
- Anderson, S. and Ö. Bedre-Defolie (2021). Hybrid platform model. CEPR Discussion Paper No. DP5694.
- Belleflamme, P. and M. Peitz (2018). Inside the engine room of digital platforms: Reviews, ratings and recommendations. In: J. J. Ganuza and G. Llobet (eds.). *Economic Analysis of the Digital Revolution*, Funcas Social and Economic Studies n° 4, Funcas.
- Belleflamme, P. and M. Peitz (2021). *The Economics of Platforms: Concepts and Strategy*. Cambridge University Press.
- Bourreau, M. and G. Gaudin (2022). Streaming platform and strategic recommendation bias. *Journal of Economics & Management Strategy*, 31, 25-47.
- Brin, S. and L. Page (2012). Reprint of 'The anatomy of a large-scale hypertextual web search engine'. *Computer Networks*, 56, 3825-3833.
- Cabral, L., J. Haucap, G. Parker, G. Petropoulos, T. Valletti, and M. Van Alstyne (2021). The EU Digital Markets Act: A Report from a panel of economic experts. Publications Office of the European Union, JRC122910.
- Che, Y.-K. and J. Hörner (2018). Recommender systems as mechanisms for social learning. *Quarterly Journal of Economics*, 133, 871-925.
- Chen, N. and H.-T. Tsai (2022). Steering via algorithmic recommendations. Unpublished manuscript.
- CMA (2022). *Mobile Ecosystem: Market Study Final Report*. 10 June 2022.
- Crawford, G., M. Courthood, R. Seibel, and S. Zuzek (2022). Amazon entry on Amazon Marketplace. CEPR Discussion Paper DP17531.
- Crémer, J., Y.-A. de Montjoye, and H. Schweitzer (2019). *Competition Policy of the Digital Era - Final Report*. Publications Office of the European Union.
- Cure, M., M. Hunold, R. Kesler, U. Laitenberger, and T. Larrieu (2022). Vertical integration of platforms and product prominence. *Quantitative Marketing and Economics*, published online.
- de Cornière, A. and G. Taylor (2014). Integration and search engine bias. *Rand Journal of Economics*, 45, 576-597.
- de Cornière, A. and G. Taylor (2019). A model of biased intermediation. *Rand Journal of Economics*, 50, 854-882.
- Drugov, M. and D.-S. Jeon (2017). Vertical integration and algorithm bias. Unpublished manuscript.



Etro, F. (2021a). Product selection in online marketplaces. *Journal of Economics & Management Strategy*, 30, 1-25.

Etro, F. (2021b). Device-funded vs ad-funded platforms. *International Journal of Industrial Organization*, 75, 102711.

Feasey, R. and J. Krämer (2019). Implementing effective remedies for anti-competitive intermediation bias on vertically integrated platforms. CERRE report.

Fletcher, A. (2022). DMA switching tools and choice screens. CERRE issue paper.

Franck, J.-U. and M. Peitz (2021). Digital platforms and the new 19a tool in the German Competition Act. *Journal of European Competition Law & Practice* 12, 513-528.

Hagiu, A. and B. Jullien (2011). Why do intermediaries divert search? *Rand Journal of Economics*, 42, 337-362.

Hagiu, A., and B. Jullien (2014). Search diversion and platform competition. *International Journal of Industrial Organization*, 33, 48–60.

Hagiu, A. and D. Spulber (2013). First-party content and coordination in two-sided markets. *Management Science*, 59, 933-949.

Hagiu, A., T.-H. Teh, and J. Wright (2022). Should platforms be allowed to sell on their own marketplaces? *Rand Journal of Economics*, 53, 297-327.

Heidhues, P., M. Köster, and B. Kőszegi (2020). Steering fallible consumers. Unpublished manuscript.

Hervas-Drane, A. and S. Shelegia (2022). Retailer-led marketplaces. CEPR Discussion Paper No. DP17351.

Hovenkamp, E. (2022). Proposed antitrust reforms in Big Tech: What do they imply for competition and innovation? *CPI Antitrust Chronicle*, July 13, 2022.

Hunold, M., R. Kesler, and U. Laitenberger (2020). Rankings of online travel agents, channel pricing, and consumer protection. *Marketing Science*, 39, 92-116.

Hunold, M., U. Laitenberger, and G. Thébaudin (2022). Bye-box: An analysis of non-promotion on the Amazon marketplace. Unpublished manuscript.

Ibáñez Colomo, P. (2020). Self-preferencing: Yet another epithet in need of limiting principles. *World Competition*, 43, 417-446.

Jeon, D.-S. and P. Rey (2021). Platform competition, ad valorem commissions and app development. Unpublished manuscript, Toulouse School of Economics.

Jiang, B., K. Jerath, and K. Srinivasan (2011). Firm strategies in the “mid tail” of platform-based retailing. *Marketing Science*, 30, 757-775.



Jin, G. Z., Z. Lu, X. Zhou and L. Fang (2022). Flagship entry in online marketplaces. Unpublished manuscript.

Khan, L. (2017). Amazon's antitrust paradox. *Yale Law Journal*, 126, 710-805.

Khan, L. (2019). The separation of platforms and commerce. *Columbia Law Review*, 119, 973-1093.

Lee, C. (2021). Optimal recommender system design. Unpublished manuscript, University of Pennsylvania.

Li, Z. and G. Wang (2021). Regulating powerful platforms: Evidence from commission fee caps in on-demand services. Unpublished manuscript.

Lombardi, C. (2022). The Italian Competition Authority's Decision in the Amazon Logistics Case: Self-preferencing and Beyond. CPI Column, April 11, 2022.

Madsen, E. and N. Vellodi (2022). Insider imitation. Unpublished manuscript.

Padilla, J., J. Perkins, and S. Piccolo (2022). Self-preferencing in markets with vertically integrated gatekeeper platforms. *Journal of Industrial Economics*, 70, 371-395.

Peitz, M. and A. Sobolev (2022). Inflated recommendations. CEPR Discussion Paper No. DP17260.

Sunderland, J., F. Herrera, S. Esteves, I. Godlovitch, L. Wiewiorra, S. Taş, P. Kroon, M. Stronzik, D. Baischew, L. Nett, S. Tenbrock, S. Strube Martins, A. de Streel, J. Kalliala, J. Huerta Bravo, W. Maxwell, and A. Renda (2020). Digital Markets Act Impact Assessment support study. Publications Office of the European Union.

Wang, C. and J. Wright (2022). Regulating platform fees. Unpublished manuscript.

Whish, R. (2022). Market investigations in the UK and beyond. In: M. Motta, M. Peitz, and H. Schweitzer (eds.). *Market investigations: A new competition tool for Europe?* Cambridge University Press.

Wen, W. and F. Zhu (2019). Threat of platform-owner entry and complementor responses: Evidence from the mobile app market. *Strategic Management Journal*, 40, 1336-1367.

Zenny, Y. (2022) Platform encroachment and own-content bias. *Journal of Industrial Economics*, forthcoming.

Zhu, F. and Q. Liu (2018). Competing with complementors: An empirical look at Amazon.com. *Strategic Management Journal*, 39, 2618-2642.



DATA ACCESS PROVISIONS IN THE DMA

Jan Krämer



TABLE OF CONTENTS

INTRODUCTION	119
1. DATA PORTABILITY FOR END USERS AND BUSINESS USERS	120
1.1 Scope of Data Access.....	121
1.1.1 Data portability for end users	121
1.1.2 Data portability for business users	122
1.2 Consumer Consent	123
1.2.1 Regarding data portability by end users	123
1.2.2 Regarding data portability by business users	124
1.3 Tools to Facilitate Data Portability	125
1.4 Effective and High Quality Data Access	127
2. DATA ACCESS FOR SEARCH ENGINES	129
2.1 Tension Between Privacy and Contestability	129
2.1.1 Technical means.....	130
2.1.2 Institutional means: Data trusts and data sandboxing (in-situ access).....	131
2.1.3 Data portability as a complement to anonymisation	132
2.2 Which Data Could/Should be Provided?	133
2.3 Who Can Receive Access to Search Data?.....	136
2.4 Fair, Reasonable, and Non-discriminatory Access	137
2.4.1 Providing non-discriminatory data access	137
2.4.2 What is the appropriate price for access under FRAND terms ?	138
REFERENCES	141



INTRODUCTION

Data, especially data on consumer behaviour, is an essential input factor in the digital economy. It facilitates and improves personalization, product designs, recommendations and predictions, and targeted advertising, among other things. In this vein, data-driven advantages can spur positive feedback-loops (data-driven network effects) which in turn create barriers to entry. The DMA foresees several provisions whereby gatekeepers need to share data which were created by users while using the gatekeeper's core platform service. Such data must be shared with end users (**Article 6(9)**) and business users (**Article 6(10)**) who were involved in creating the data through real-time and continuous data portability. Moreover, data that was created by users while using an online search engine, must be shared with other online search engines (**Article 6(11)**).

The DMA has two main goals: contestability and fairness. However, the data access provisions mentioned above seem to be especially motivated by the goal of contestability. This is expressed, for example in Recital 3 (emphasis added): “Contestability is reduced in particular due to the existence of very high barriers to entry or exit, including high investment costs, which cannot, or not easily, be recuperated in case of exit, *and the absence of, or reduced access to, some key inputs in the digital economy, such as data.*” Moreover, Recital 32 states that “The features of core platform services in the digital sector, such as network effects, strong economies of scale, and *benefits from data have limited the contestability of those services and the related ecosystems.*”

This view is strengthened by the specific recitals relating to the above provisions. In relation to data portability by business users and end users, Recital 59 explains that the provision is necessary “to ensure that gatekeepers do not undermine the contestability of core platform services, or the innovation potential of the dynamic digital sector, by restricting switching or multi-homing”. Likewise, Recital 61, relating to access to search and query data, highlights that “access by gatekeepers to such ranking, query, click and view data constitutes an important barrier to entry and expansion, which undermines the contestability of online search engines.”

However, Recital 34 also makes clear that “contestability and fairness are intertwined”. Moreover, Recital 33 states the notion of fairness includes that “business users should have the ability to adequately capture the benefits resulting from their innovative or other efforts”. One can argue that the goal of fairness therefore includes that business users receive access to the data that was created through their efforts using a core platform service.

In this issue paper, the provisions of the DMA on data portability and data access to search and query data of search engines are considered in more detail, in particular with regard to open questions concerning their implementation in view of the stated goal of contestability.



1. DATA PORTABILITY FOR END USERS AND BUSINESS USERS

Albeit data portability is already a fundamental right of users under the **General Data Protection Regulation (GDPR) (Article 20)**, this right is augmented in the context of contestability by the DMA.

Article 6(9)

The gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data.

There are three main differences between Article 20 of the GDPR and Article 6(9) of the DMA. First, of course, the GDPR applies horizontally to all data controllers, whereas the **DMA only applies to gatekeepers**. Thus, enhanced data portability is only available at a very limited number of firms. However, by Article 17(4) also emerging gatekeepers, which do not yet meet the thresholds for gatekeepers laid out in Article 3, can be mandated to offer such enhanced data portability (including data portability for business users as discussed below).

Second, and most importantly, consumers must be provided **data access continuously and in real-time**, likely through APIs. The GDPR only calls for one-off data transfers provided in “a structured, commonly used and machine-readable format”, and data controllers have up to 30 days to provide the data. This often tedious and slow process, where the data may be outdated by the time they are received, has been considered one of the main reasons why data portability under the GDPR is not used widely to date, and thus not an effective instrument to spur competition and innovation (Krämer et al. 2020). At the same time, it should be acknowledged that continuous and real-time data portability is much more complex to implement than a one-off data transfer and raises additional technical feasibility issues that need to be considered in the implementation of this provision.

Third, the gatekeeper must provide “**tools to facilitate the effective exercise of data portability**”. This is worth discussing, and we will return to this below.

In addition, the DMA also extends the idea of data portability to business users as follows:

Article 6(10)

The gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users. With regard to personal data, the gatekeeper shall provide for such access to, and use of, personal data only where the data are directly connected with the use effectuated by the



end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users opt in to such sharing by giving their consent.

1.1 Scope of Data Access

1.1.1 Data portability for end users

The scope of data that is ‘provided’ by an end users, and thus subject to data portability, is already contentious under the GDPR’s data portability right (cp. Krämer et al. 2020). One can roughly distinguish between volunteered, observed, and derived data (Crémer et al. 2019). *Volunteered data* is explicitly and intentionally revealed by a user (an email-address or ‘likes’, for instance). *Observed data* is obtained from the usage of a device, website, or service and the user may or may not be aware that such data is collected (location data or clickstream data, for example). *Inferred data* is derived through refinement and recombination from volunteered and observed data, such as by use of data analytics such as clustering, filtering or prediction.

Article 20 GDPR clearly includes volunteered data, while it is commonly understood that inferred data is not included. With respect to observed data, it is currently not completely clear how far the users’ right to port data goes, and whether and to what extent it is covered by the right to data portability. However, in its “Guidelines on the right to data portability” the European Data Protection Board (EDPB) defines provided data as those data “provided by the data subject by virtue of the use of the service or device”. The EDPB also suggests that this can include data that was explicitly provided by the data subject (“volunteered data”) as well as data that was implicitly provided by the data subject (“observed data”).¹¹⁹ But the question remains how far reaching one can interpret the scope of ‘observed data’.

Accordingly, as the DMA is using the same language as the GDPR and, in Recital 59, clearly labels its data portability provision as a complement to that under the GDPR, the same ambiguity on the precise scope of data portability now extends to the DMA. Given that Recital 59 also refers to the “innovation potential” and, as laid out above, seeks to promote contestability in the context of data portability, a wider scope of observed data could be assumed. This could, for instance, also include clickstream data of consumers then. In reverse, the DMA must also be interpreted in light of the proportionality of its obligations and in view of IP rights, data security, and privacy-related innovation. While we have already pointed to the ambiguity of the scope of observed data to be included in a portability request under GDPR, the **similar language in the DMA suggests that the same scope as under GDPR should also apply to the DMA. That would exclude derived data from portability requests under the DMA.**

While it is clear that only raw data can be ported, under a generous interpretation of ‘provided’ data (especially with regard to ‘observed’ data), it is **reasonable to ask how much context to the ported data needs to be provided** so that data subjects (and third parties to which the data is ported) can truly assess the information content of that data. For example, in the context of clickstream data, such

¹¹⁹ See https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf



data is meaningless unless the content that was consumed or which ads were clicked on is also shared. But the contextual information (for instance the content or the ad) was of course not ‘provided’ by the user, although the user engaged with that content. So, should contextual information be in scope of data portability? What are the objective legal, economic, or technical reasons not to make location, tracking, and clickstream data available? For example, are concerns about data security and about a possible loss of reputation due to data leakage or misuse at the end of the receiving data controller admissible? Given that data needs to be shared in real-time and continuously, potentially vast amounts of data are subject to data portability if such a wider scope is assumed. When exactly is technical infeasibility admissible as a defence for a data rich firm in the digital economy? Generally, Article 34 of the GDPR requires a data controller to put in place appropriate security measures for all personal data in its possession, including that which it is provided further to the rights of access and portability. The DMA needs to be consistent with those requirements.

Finally, one may ask if the answer to these questions should factor in at all what the intended use of the data is, or where consumers are porting the data to. If the goal of this provision is just to facilitate switching and multihoming, then it may be **justified to limit data portability to the personal data required to enable switching and multihoming**, but no more. For example, which ads the consumer clicked on may well be personal data (and as such eligible for portability under GDPR), but not be material for switching to another service provider offering a similar service, and thus must not be provided under the end user’s DMA portability right (in a real-time and continuous manner). If such a logic were admissible, then there would be difficult case-by-case decisions to make on which data are material for switching. For example, even though the alternative provider may not require the clickstream data on ads for improving its service offering directly, that information may nevertheless improve the service quality indirectly, as it helps to increase ad revenues, which can be re-invested in service quality. Further, viable alternative providers may not yet exist at the time where the Commission needs to specify the scope of the data portability provision for a given gatekeeper, and then it would have to anticipate which data may be useful for switching to a future (innovative) service provider. This seems challenging.

In conclusion, a **wider scope of the data to be ported, independent of the use and the destination of the data, seems preferable**.

1.1.2 Data portability for business users

Generally, the same issues on scope also arise in the context of data portability for business users, especially relating to personal data of end users engaging with the product or service of the business user.

In addition, it is noteworthy that, in relation to Article 6(10), Recital 60 seems to allow for some ‘*adversarial portability*’ by business users. That is “a gatekeeper should not use any contractual or other restrictions to prevent business users from accessing relevant data”. This could be understood as a free pass for business users to use web scraping or other tools not directly provided or authorised by the gatekeeper in order to access the information that the gatekeeper may provide to those business users via its own website or other interfaces. This would mean **that whatever data the gatekeeper chooses to make available to the business user via its own interfaces (such as**



performance metrics, aggregate user data, and so on) in any form, could be in scope for data portability by business users. Although the data must be ‘relevant’, this does not seem to put a strong restriction. If the data were not ‘relevant’ to the business user, then it probably would not have been provided to them via some interface in the first place. Moreover, the judgment on whether data is ‘relevant’ to a business users can only be made on a case-by-case basis and must also anticipate future business users.

Another issue of the scope of data portability relates to the definition of a “business users’ product or service”. Business users are only entitled to port data that was created in relation to their product or service. *But what if a business user is just one of many on a platform that offer the identical product or service?* Say a business user offers a product on an online marketplace and is listed as one of many sellers of that very product. The online marketplace shows the product only once (for instance in a search result or on a dedicated product page), and from there it links to several business users from which the product can be bought. Which of the many business users is entitled to the data that was created through the engagement of an end user with that product in the online marketplace? Only the business user which was listed as the “default” buy option? All business users, albeit some may have offered the product at a price that would not have led to an engagement by the end users in the first place? This issue may not arise in contexts where the product or service offered through the core platform service is uniquely linked to a specific business user, but as the example highlights, in the case of some core platform services that linkage between product and business user is not unique.

KEY QUESTIONS

- What is the **scope of observed user data that needs to be provided** for end users pursuant to a portability request? In particular, does contextual information on the data need to be provided to make data portability effective?
- Can the gatekeeper bring forward a **technical feasibility constraint**, given that data needs to be ported in real time.
- Is ‘**adversarial portability**’ allowed for business users under the DMA?
- Are there **limits** to data portability of a given business users **when the business user’s products or services** are offered by several business users?

1.2 Consumer Consent

1.2.1 Regarding data portability by end users

In the context of real-time and continuous data portability, consumers should be able to give their **consent on a fine-granular level** regarding which data is to be potentially transferred. All-or-nothing transfers are often not necessary, and would create more transaction costs, both technically (network



load or space requirements, for example) as well as economically (larger privacy concerns). The granularity of consent should be part of the regulator's specification procedure in relation to the data portability obligations. Of course, gatekeepers shall not influence consent or dissent by offering commercial incentives or disincentives.

A particular concern in the context of data portability is a potential conflict with the *rights of other data subjects*. Consumers may want to port data that has been co-created (for instance, chat protocols) or is shared by others via a core platform service (for example, pictures of (several) data subjects), or is otherwise linked to others (such as address books, or pictures where other people are tagged). In this case, the platform service may be required to ask for consent to include such data in a data portability request. Otherwise, the gatekeeper may just exclude such data from data portability diminishing its value, especially with regard to the intended goal of facilitating switching and multi-homing for end users. Thus, next to the end user's consent to initiate a data portability request, **end users may also need to consent (possibly in advance) to other users' data portability requests.**

Neither the DMA nor GDPR currently provide guidance on this issue, that is, who is responsible for obtaining consent from others, or whether a data portability request can be limited to only that portion of the data which is not affected by rights of others.

It should also be understood that obtaining consent doesn't shield the parties involved from compliance with the GDPR, which includes compliance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability. The GDPR imposes obligations on all actors of the data supply chain and the data ecosystem – the gatekeeper, the recipient of the data, and other business partners.

1.2.2 Regarding data portability by business users

In the context of data portability by business users an additional complication (in comparison to data portability by end users) arises from the fact that non-personal (aggregate) data and personal data relating to some end user must be differentiated. For example, an end user may have provided his or her gender and age via the core platform service to the business user. While the business user may be entitled to port aggregate information about its users' demographics, the information about a specific user is only accessible if the user has opted into data portability for that very business user. That is, **each business user must ask each of its users whether they agree to data portability.** There are at least two implementation issues associated with this:

First, **when is the consumer being asked for consent?** To exemplify this issue take the following case. Say a user browses through an online marketplace, looking at various products. The age and gender of that user is known to the online marketplace, and it can thus be linked to the clickstream data that the user is generating while browsing. The user enters a keyword and is presented a list of products. After looking at some products in that listing, the user eventually buys a product. When should a user be prompted for consent, and with regard to which personal data? Should the user consent already when clicking on the product page, possibly to each business user who provides that product individually? That would clearly be valuable for business users, as they may determine from the clickstreams why a consumer has not bought. However, this would also clearly not be practical and



quickly render the online marketplace unusable from an end user’s perspective. Should the user then only be asked for consent if he or she has bought a product? Article 6(10) only seems to require ‘engagement’, but does not further specify whether there is a threshold to what qualifies as ‘engagement’. And which data should that consent then cover? The whole customer journey leading up to that sale? Only the customer journey on the product page of the product that was eventually bought? And does that data only include observed data (say which reviews the customer has read on the product page), or also personal data provided by the user to the core platform service in advance to the customer journey (age and gender in this example), but which has not been provided in the customer journey leading up to that sale or as part of the sales process?

Second, **how is consent being obtained?** Through the business user (via channels outside of the core platform service) or via the core platform service directly? Recital 60 notes that the gatekeeper “should enable business users to obtain consent of their end users”. This seems to suggest that gatekeepers need to implement tools directly through the core platform service that enable business users to obtain consent. Say, in the online marketplace example, a consumer can tick a box before concluding a purchase as to whether his or her data can be ported to the business user. That would require at least one additional click for users – in a context where every click leading up to a final purchase can be one click too many. Are gatekeepers then allowed to have consumers opt in to data portability for all business user interactions that they encounter using the core platform service at once? This seems overly broad and may not be in line with the notion of informed consent under GDPR that is required also under the DMA (as noted in Recital 60 when referencing Regulation (EU) 2016/679 and Directive 2002/58/EC). Relatedly, can a business user ask for consumer consent to portability for all the core platform services that it may operate on, or does this need to be obtained per core platform service?

KEY QUESTIONS

- How fine **granular must the consent** for data portability obtained be, and should it include consent to data portability requests of others?
- What is the **threshold for ‘engagement’** in order for a business user to be entitled to data portability?
- Does end **user consent** to portability need to be obtained for each business user, or for each core platform service separately?

1.3 Tools to Facilitate Data Portability

Interestingly, Article 6(9) relating to data portability by end users requires gatekeepers to provide end users with “tools to facilitate the effective exercise of such data portability” free of charge. This is worth discussing for several reasons.



First, it is noteworthy that this obligation to provide ‘tools’ does not exist for data portability by business users, probably since business users are expected to have their own ‘tools’ for that purpose – or because third-party tools are being developed and offered to business users. By contrast, as mentioned above, business users are provided with an implicit authorisation to make use of ‘adversarial data portability’, which is not the case in relation to portability by end users.

One may **wonder why end users seemingly do not have the right to use ‘adversarial data portability’, but instead need to rely on the tools provided by the gatekeeper.** This matters, because users may have access to more data through their user interface when using the core platform service than what may fall under the scope of personal data portability (see above for a discussion on the scope of data portability requests). One may also expect that third-party tools that pull data from the user interface are being in case this was legitimised by the DMA. In fact, those tools often already exist, but have been shut off by some of the possible gatekeepers.¹²⁰ One important objection against such adversarial data portability may be that some of the data that is being shown to users via their user interface is in fact not their personal data, at least not theirs alone, as it also touches on rights of others (cf. discussion above on consent). For example, they may see personal pictures of others, or chat protocols that have been co-created with others. Although a user may see this personal data of others, and others may have shared it with the whole world, this does not mean that the data can be legally ported. There has already been controversy about this issue in context to data portability under the GDPR (Graef 2020; Krämer et al. 2020) and the debate is still not resolved. In this regard, the use of tools provided by the gatekeeper to exercise data portability, instead of adversarial data portability, can also be understood as a means to be able to control the lawfulness of data portability better. A gatekeeper can ask consumers for their consent to the porting of their personal data that they shared with others (such as personal photos that they publicly uploaded) in order to ensure that only such data are being ported (through the tool).

Second, there may also be an unintended consequence in relation to the tools provided for data portability. Data portability, especially continuous and real-time data portability, can spur the emergence of Personal Information Management Systems (PIMS) (cf. Krämer, Senellart & de Streef 2020), which are believed to be an important pillar for consumer empowerment in the digital economy (EDPS 2020). PIMS are envisaged to facilitate consumers’ data control and the exercise of their rights to data portability, including accessing, storing, visualisation, and possibly monetisation of their data. PIMS may also allow for (automated) consent management across services. While the technical details and economics of PIMS are beyond the scope of this report, it is important to note that the **DMA’s provision to offer tools for data portability to consumers may lead to a crowding out of independent PIMS.** Such PIMS may then be provided by gatekeepers instead of independent third parties.

Ultimately, the tools provided by gatekeepers may not only facilitate data portability from their core platform service to another provider, but also data portability requests between various services more generally. In fact, in 2018 some of the major tech firms, under the lead of Google, already started an

¹²⁰ An example is the tool ‘Ad Observer’ that has been developed by researchers from New York University to study misinformation on Facebook. See <https://www.nytimes.com/2021/08/10/opinion/facebook-misinformation.html>



open source project, called the **Data Transfer Project**¹²¹, with exactly this purpose. While the project has not progressed significantly since then, the DMA may spur its development. This should be scrutinised closely, as otherwise this may unintentionally equip gatekeepers with even more sources to consumer data.

KEY QUESTIONS

- Must consumers rely on the **tools provided by gatekeepers** to exercise their right to continuous and real-time data portability under the DMA?
- Can **third-party** tools also access the data with the same performance and quality?

1.4 Effective and High Quality Data Access

Both Article 6(9) and 6(10) require the implementation of data portability to be *effective*. Beyond the points already mentioned, what could effective data portability mean? Recital 59 suggests that effectivity could relate to the *format* in which the data are accessible (through the interfaces or ‘tools’ provided by the gatekeeper), as it notes that such data shall be “effectively accessed and used by the end user”. Moreover, ‘effective’ could also entail that data transfers are safe to use for end users. That is, the data transfer needs to be **secure**, minimizing risks for data leakage to parties not involved in the transfer, data modification or loss of data;

Effectiveness of data portability can also relate to aspects of transparency and adherence to common standards. Thus, **where possible, data portability should make use of open standards and protocols, which are free to use and transparent for developers** (see, for instance, Furman et al, 2019, pp.71-74). To this end, Article 48 of the DMA allows the regulator to request European standardisation bodies to develop standards for portability. This is also elaborated on in Recital 96: “The implementation of some of the gatekeepers’ obligations, such as those related to data access, data portability or interoperability could be facilitated by the use of technical standards. In this respect, it should be possible for the Commission, where appropriate and necessary, to request European standardisation bodies to develop them.” Examples may be drawn from the Australian Consumer Data Right (CDR) initiative,¹²² which has also relied on a standardisation body.

However, the development of standards may require much time, and regulators will have to rely on effective implementations by the gatekeepers in the meantime. In any case, albeit challenging and time consuming, it will be important to **harmonise data formats and interfaces for data portability across the various gatekeepers** subjected to the DMA’s data portability provisions. Harmonisation and standardisation are important, because it allows third party tools, such as PIMS, to better

¹²¹ See: <https://datatransferproject.dev>

¹²² See <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>



integrate with the largest possible set of firms and thereby to facilitate switching and multihoming (cf. Krämer et al 2020). In other words, instead of having one tool per gatekeeper, it would be better to have one tool that is able to connect to all gatekeepers for the purposes of data portability.

As mentioned above, effective data portability also means that **consumer consent for data portability can be provided effectively**. This relates to the granularity of consent (see above), but may also include the possibility to give automated (rule-based) consent, for instance, through tools such as PIMS. It will have to be clarified, however, to what extent under what conditions such automated consent (that is, consent automatically derived from the users' explicitly provided privacy preferences) would qualify as "informed consent" under Article 7 GDPR.

Effectivity should also relate to *availability and performance* of the interface used for data portability. In the context of the Revised Payment Services Directive (PSD2 Directive), **performance and reliability was measured against the data provider's other consumer-oriented interfaces**.¹²³ This seems to be a reasonable approach also in the context of the DMA's data portability provisions.

Finally, it is also worth highlighting that **'high quality' of data portability** is explicitly mentioned, next to 'effectivity', only in Article 6(10), but not in Article 6(9). Recital 59 clarifies what may be meant by 'high quality' in relation to data portability: "Gatekeepers should also ensure, by means of appropriate and high quality technical measures, such as application programming interfaces, that end users or third parties authorised by end users can freely port the data continuously and in real time. This should apply also to any other data at different levels of aggregation necessary to effectively enable such portability." Does the mentioning of 'high quality' only in Article 6(10) mean the performance standards are possibly lower in relation to data portability by end users, relative to data portability by business users? This would not seem reasonable in light of the goals of the provision, that is to facilitate switching and multihoming. If this distinction in the 'quality' of data portability is indeed intended by the regulator, where should we then draw the line between 'high quality' and 'effectiveness' of data portability?

KEY QUESTIONS

- To what extent does data portability need to fulfil **security, availability, performance, and standardization** criteria in order to be 'effective'?
- Are the **criteria different** for end user data portability vs. business user data portability?

¹²³ See Article 32 as well as Recitals 23-25 in the Delegated Regulation (EU) 2018/389, amending the PSD2 Directive (EU) 2015/2366.



2. DATA ACCESS FOR SEARCH ENGINES

Online search engines are a particularly important service in the digital economy as they are usually the entry point of an online session. Scholars have long argued that the market for (general) online search engines may lack contestability due to strong data-driven network effects, and that data sharing may be an appropriate remedy (Argenton & Prüfer 2012). The DMA now includes a provision exactly to that effect.

Article 6(11)

The gatekeeper shall provide to any third-party undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click and view data that constitutes personal data shall be anonymised.

2.1 Tension Between Privacy and Contestability

The provision in Article 6(11) requires gatekeepers to provide ranking, query, click, and view data to third-party search engines with the explicit goals of fostering competition and contestability in relation to that gatekeeper. However, at the same time the provided data cannot contain personal data, which shall therefore be sufficiently anonymised. Recital 61 explains that the gatekeeper should “ensure the protection of the personal data of end users, including against possible re-identification risks, by appropriate means, such as anonymisation of such personal data, without substantially degrading the quality or usefulness of the data.”

However, there is **a tension between strong anonymisation and maintaining enough level of detail in the data that it is valuable** for third-parties such that they can derive better algorithms and predictions in order to contest the data provider. While it is clear that anonymisation needs to be effective, there is regularly a dispute over the boundary at which data is effectively anonymised, especially as technology and computing power progresses. In the extreme, data could be so strongly aggregated (for example, an average age for all users) that it is not useful anymore for deriving insights from the data. When implementing this provision, navigating this tension between aggregation and detail of the data will probably be the most difficult task for the regulator.

Some observers seem to question that it will ever be possible to balance this tension, as methods and tools for de-anonymisation are continuously being improved and even relatively little detail may already reveal a person’s identity (see, for instance, Rocher, Hendrickx, & de Montjoye 2019). It may likely require technical *and* institutional means to achieve this in the best possible way. Some possible approaches are discussed below, which may also be used in combination. However, no matter how the data sharing is implemented, anonymised user data will never have the same ‘depth’ as the original data set due to this trade-off. This also calls into question whether such data sharing is sufficient for a third-party to truly contest the incumbent who had provided this data. We will return to this below.



The risk of de-anonymisation in a particular data set depends crucially on the uniqueness of the attributes associated with different individuals. It is therefore generally not enough to just remove a personal identifier (for instance, the combination of full name, birthday, and place of birth) and to replace it with a pseudo-identifier (a unique combination of numbers and letters, for example). Although it might not be immediately obvious anymore who is associated with a given data record, the values of the remaining attributes in the data set (such as the combination of blood type, zip code, and age) may still uniquely identify an individual. This is the more likely the more unique the individual values are (a very rare blood type or a very high age, for instance). **'Anonymity' is therefore not a discrete zero-one concept but rather a statistical concept that relates to a particular probability that an individual may be re-identified.**

2.1.1 Technical means

K-anonymity

In computer science, two concepts are frequently used to describe the degree of anonymity in a given data set. The first concept is k-anonymity: **A data set is said to have k-anonymity if the information for each person contained in the data set cannot be distinguished from at least k-1 other persons who are also contained in the same data set.** Consequently, the larger k, the larger is the degree of anonymisation of a data set. K-anonymity can generally be achieved by suppression of attributes (for example, deleting name, dates, or address) or by generalisation of attributes (such as transforming names to initials, dates to years, and addresses to zip codes). K-anonymity usually does not involve any randomization of attributes and it can be seen that in large data sets, especially 'deep' data sets with many attributes, anonymity may nevertheless be compromised.

Differential privacy

A second, more recent and more sophisticated concept is differential privacy. Roughly speaking **differential privacy is not a discrete concept (as k-anonymity), but a probabilistic concept and requires randomization of attribute values (adding some random noise to GPS data, for instance).** The goal is to create a data set for which it is not possible (with some statistical guarantees) to know whether an individual's data is contained in the data set. This is important because de-anonymisation attacks typically match data from different data sets from which it is known that they contain a given individual. This can be achieved, for example, by running several similar queries to a data base, with the goal to obtain (anonymised) data sets that differ only by the entry of one person. While data sets with a k-anonymity property are susceptible to such attacks, data sets with differential privacy are not, due to randomization. There are several algorithms to achieve differential privacy, and this is subject to ongoing research in cryptography. In practice it may be difficult and computationally burdensome to achieve differential privacy, especially if data is shared in a continuous manner. A more practical approach is therefore **not to store accurate data about individuals at all, but to add some noise already when data is collected.** This is a technique that is already applied by Apple and Google for select applications in iOS/macOS and Chrome,¹²⁴ but it is not known whether it also applies in relation to online search engines. This also highlights that differential privacy is not just a theoretical option,

¹²⁴ Green, M. (2016). What is differential privacy? <https://blog.cryptographyengineering.com/2016/06/15/what-is-differential-privacy/>



but can indeed be applied in the context of large-scale data collection as is typical for prominent digital services. This may also mean, however, that regulated firms may not only be mandated to share their data, but also mandated to collect (or rather *not* collect) their data in a certain way, in order to enable privacy-preserving sharing of that data later.

Synthetic data

The anonymisation of search logs while preserving useful information is a relatively recent and emerging field of research (Hong et al. 2009), but also a domain of computer science in which progress is being made quickly. **Promising developments seem to be the creation of ‘synthetic search logs’** which contain plausible search sequences, but are created from a machine learning model and do not relate to an actual person (see, for instance, Krishnan et al. 2020).

2.1.2 Institutional means: Data trusts and data sandboxing (in-situ access)

Next to such technical means, there are also institutional means to protect privacy, which can also be combined. A common institutional proposal is to establish a trusted data intermediary (*data trust*). To ensure this, the trust needs to be independent from the regulated entity, of course. The main idea is that **user data (from the various entities that are mandated to share data) is collected by a data trust in its original raw and detailed form (see, for example, Graef & Prüfer 2021). The trust could then combine the data and anonymise it properly.** Such anonymisation of the joint data set directly would be preferred over anonymisation of separate data sets at the source, because it would reduce the risk of de-anonymisation through re-matching of the different data sets, each of which may have different attributes omitted or generalised.

Moreover, the data trust may not need to reveal any raw data directly but **could act as a data sandbox** instead. This means that third-parties would need to submit their algorithm for analysing the data to the trust, who would then run it on their behalf on the detailed raw data. The third-party would receive back the trained algorithm, but never see the raw data itself. Data sandboxing could also be applied at the original data source directly (Graef & Prüfer 2021), which is then referred to as *in-situ access* (Martens et al 2021).

It is however **not clear whether access of the data only through data trusts and data sandboxing is sufficient** to allow access seekers to combine the provided data with their own in order to really be able to obtain a novel dataset – which, as argued above, would probably be necessary in order to be truly able to contest the incumbent. Otherwise, the shared data will just be an (inferior) subsample of the data that is available to the incumbent.

In addition, there are several practical issues with data trusts and data sandboxes, especially when applied to vast amounts of data, as those collected by online search engines. For all practical purposes **a data trust would require an enormous infrastructure** to be able to store, aggregate and anonymise the data (continuously) in any meaningful way. For example, Google Search alone processes over 80,000 search queries every second on average, which translates to almost 7 billion searches per



day.¹²⁵ It seems one would have to duplicate much of the gatekeeper's data centre infrastructure to achieve this. Who would then finance and operate this, and be liable in case of failure or data breaches? Would this be in line with the Commission's sustainability goals?

Likewise, data sandboxing is an intriguing theoretical idea, but it would require an even larger infrastructure to have sufficient computing power required for running probably complex algorithms on the data. Since these would operate on the detailed raw data, it would also require enormous effort and expertise to make sure that the algorithms do not compromise privacy. It seems to be a formidable task for the regulator to police this – that is, to ensure that the data are neither too highly aggregated (so they don't prove useful), nor too little aggregated (so they may compromise privacy).

If algorithms are run directly on the infrastructure and raw data of the original data controller (in-situ access), then this would also **put a significant computational burden and cost on the regulated firm**. In turn, this would warrant some financial compensation (discussed in more detail below in relation to FRAND access provisions). It also needs to be feared that the original data controller would be able to acquire business sensitive information about the third-parties through the algorithms that are run on its infrastructure.

Nevertheless, regulators may want to entertain the idea that data trusts or data sandboxing (at a data trust or via an in-situ access) **may be feasible if confined to subsets of the data, particularly with a focus on recency**. In the short term only in-situ access seems practical, as the gatekeeper already has an appropriately sized infrastructure in place. In this case scrutiny must be placed on the confidentiality of the competitors' algorithms. In addition, in-situ access does not alleviate privacy risks completely, as data requests may be so specific that they can be matched to individuals and anonymisation techniques (cp. to the concept of 'differential privacy' above) must be applied nevertheless.

2.1.3 Data portability as a complement to anonymisation

Finally, it is worth highlighting that there may be a fruitful interaction between the data portability provisions and anonymisation in this context.

Gatekeepers operating an online search engine and being subjected to Article 6(11) are also subjected to Article 6(9) and 6(10). As the number of business users are defined by the commercial websites listed by an online search engine (see Appendix to the DMA), this potentially gives a large number of business users portability rights vis-à-vis a search engine. **Depending on the scope of access under this portability right (see above), this could also include query and click data, and – if the end user has consented to it – personal data.**

Likewise, the user could directly transfer (continuously and in real-time!) personal data (which should include clickstream data, as discussed above) under his or her portability right to a third party, such as a search engine. Of course, only a subset of the end users will ever make use of this. Thus, the ported

¹²⁵ Internet Live Stats, 2020, <https://www.internetlivestats.com/one-second/#google-band>



data are not representative by any means, but provide more ‘depth’ to the data than what can be shared through Article 6(11), and thus data portability can act as a complement (but not as a substitute) to it.

However, in contrast to the data portability provisions discussed above, the search engine data to be shared under Article 6(11) does not need to be shared in real-time and continuously. This would also not be possible while at the same time, anonymisation techniques shall be applied. However, regulators should still put an emphasis on recency of the data to be shared, including an appropriate frequency at which the data is to be updated.

KEY QUESTIONS

- What is the appropriate **institutional means** (data trusts, data sandboxing/in-situ access, APIs) through which search engine data shall be shared in order to balance contestability goals and privacy?
- How far reaching are the powers of the EC to impose a certain means and/or to impose a **certain data collection procedure to facilitate sufficiently anonymised** yet useful data sharing?

2.2 Which Data Could/Should be Provided?

In general search, the data bottleneck lies in the search queries, associated context information, and behavioural data on how users interacted with the search results (Krämer et al. 2021). The data bottleneck is not, however, the web index (that is, the register of all websites), as this data can be more easily duplicated by (potential) competitors.

Any shared data must therefore at least contain information about the search queries that users have presented to the search engine provider. This already brings about one central difficulty. **Search queries are inherently personal** and can reveal significant information about an individual. They may also reveal a person’s identity relatively easily. A famous example is the case of Ms. Arnold, who was identified from a list containing 20 million web search queries conducted by a total of 657.000 Americans over the period of just three months. Although the data set was released by AOL in a pseudo-anonymised way (evidently not respecting k-anonymity or differential privacy), she was re-identified based on her search queries alone (Barbaro & Zeller 2006).

Since web queries are based on text, it is not as straightforward to add some noise to the search terms without rendering them useless (cf. ‘differential privacy’). Moreover, as has been pointed out by the CMA’s study on ‘Online platforms and digital advertising market’ (CMA 2020, p. 12)¹²⁶ as well as recent

¹²⁶ Also specifically Appendix I of that study. Available at https://assets.publishing.service.gov.uk/media/5fe4957c8fa8f56aeff87c12/Appendix_I_-_search_quality_v.3_WEB_.pdf



research (Klein et al. 2022), it is precisely the rare search terms that are particularly valuable for training a prediction model improving ranking quality.

The risk of re-identification is less pronounced if one would not associate specific search queries with a unique user identifier, which allows to associate different searches of an individual over a period of time. However, without such a user identifier, the data set loses traceability, for instance, on the search process of an individual, which is an important for improving for the quality of search engines.

A second major challenge is to define the scope of the contextual information relating to the search results page properly. Aggregate, or even individual search query data is only one part of the relevant information that users reveal to a search engine. The other part is how they have interacted with the search results page, for example, which links were clicked subsequent to a given search and in which order. But sometimes it may be even more informative which links consumers did *not* click and thus did not find relevant after a given search. For a proper assessment of clicks, it would also be necessary to know which other elements were shown on the search results page in addition to the organic search results. For a long time now, Google's search results page does not only contain "10 blue links" anymore, but in addition, and depending on the search query, sponsored search results and other 'boxed' elements such as a news carousel, flight search, a shopping comparison, or an immediate answer to the search query are displayed. In fact, an increasing percentage of search sessions end with the search results page, and consumers never follow up and click on a search result. It is estimated that so called Zero-Click Searches amounted to about 50% of all searches on Google.com in June 2019 (Fishkin 2019). Likewise, research has shown that clicks on organic search results are heavily influenced by whether and how sponsored search results and 'boxed' results are presented (Edelman and Lai, 2016).

Evidently, the search results page (ranking) is already inferred data of the search engine, and forcing the release of detailed information about the search results page pertaining for every query would probably go too far with regards to the proportionality principle under EU Law and Art. 8.(1) DMA, as it would undermine past and future innovation efforts. Based on this data, third parties may be able to reverse-engineer the gatekeepers ranking algorithm. However, it may be justified to release such information for samples of queries, or to limit the details of the data relating to the search results page. One could release, for example, only the first clicked result.

In order to advance the discussion on the appropriate scope of shared search logs, Krämer et al. (2021) suggested to think in three main categories: i) data on the query itself, ii) data on the search results page, and iii) data on the user. The below table exemplifies which pieces of information can belong to each category.

**Table 1: Categories and scope of search data to be considered for sharing**

DATA ON QUERY	DATA ON THE SEARCH RESULT PAGE (SERP)	DATA ON THE USER
Keywords (such as raw search string, synthetic search string)	Clicked URLs (first clicked result, last clicked result, all clicked results)	Unique identifier
Timestamp (week, day, hour, seconds)	Zero-Click search (yes/no)	Device metadata (for instance, mobile/ desktop, browser metadata)
Connected queries in the same session	Results ranking (top 3, top 5, top 10)	Location data (IP-address, GPS)
	Layout of the SERP (sponsored results, one-boxes)	Other available user attributes (age and gender from account data, for example)

This is certainly not a complete list, but it invites policy makers to think how different data, each at various level of granularity (listed in parentheses), can be mixed and matched from the different categories, and this would result in significantly different data sets that may be shared.

Another issue relates to the **impact that the legal geographical reach of the DMA may have on the scope of data that can be provided**. Can the DMA only ever demand relevant data to be shared that was collected in the EU, or provided by citizens of the EU? Or can it demand from gatekeepers operating in the EU that all of their relevant search and query data, no matter where and from whom it is collected, and no matter where it is stored, fall under the scope of the DMA's sharing obligation? Given the fact that data-driven learning and improvements of the search algorithm provided to EU citizens is also (at least potentially) determined by data that was provided outside of the EU, the latter may be justified.



KEY QUESTIONS

- What is the **precise scope** of data to be shared with respect to the detail on the query, the search results page, and the user?
- What is the **scale of data to be shared** (for instance, full or random samples, only data from within the EU)?
- What is the appropriate **timeliness of the data** (frequency of updates and recency of the data)?

2.3 Who Can Receive Access to Search Data?

The answer to this question may seem obvious at first, as Article 6(11) limits access to other ‘search engines’. However, this calls into question what exactly the purpose of this obligation is, how narrowly defined the ‘search market’ is, and whether one should evaluate the seriousness of the access seeker to contest the access provider.

First, does the access seeker have to be in the area of general search, or can it be also in more narrow search markets, such as product search or location search? **The definition of an ‘online search engine’ in the DMA suggests that only general search engines are subject to the access obligation,**¹²⁷ but does this also extend to the access seeking search engine? This interpretation is very important. If the scope of third parties that can seek access is rather small and limited to other search engines, then the goal of this provision would clearly be to enable other general search engines to contest the gatekeeper. In this case, what if an undertaking just cooks up a general search engine in order to receive data ‘as a search engine’, but use that data for a totally different business really? Should there be a vetting procedure determining the seriousness to contest the incumbent by an access seeker. This seems problematic. And if not, is this worrisome with respect to contestability? As search engine data may well be repurposed to innovate and pursue different types of services, this would be welcomed from an innovation point of view, and this could also provide a stepping stone for entry of new digital firms (not necessarily in the search market), which may ultimately be able to become a sizable competitor and thus to increase contestability in digital markets. If, however, access is indeed limited to other search engines in the narrow sense, then this innovation and competition potential coming from search data is forfeited. In reverse, if the scope is meant to be rather wide, why has it been limited to ‘search engines’ in Article 6(11)?

Relatedly, is it realistic that a third-party search engine takes the main search engine head on and tries to improve its search algorithm with the ambition to take over the leading position in the general

¹²⁷ The definition of an ‘online search engine’ is borrowed from the Platform-to-Business Regulation (EU 2019/1150), Article 2(5), where it is noted that « ‘online search engine’ means a digital service that allows users to input queries in order to perform searches of, in principle, **all websites**, or all websites in a particular language, on the basis of a query **on any subject** in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found; » [emphasis added].



search market? Since Article 6(10) limits access to search engines, the DMA seems to rather assume this narrow view of contestability *à la Baumol* (1986). However, there is reason to **doubt that such frontal contestability is feasible**. As detailed above, the access provider will only be able to make a fraction of its data trove ever available to third parties, due to technical limitations and due to privacy reasons. Moreover, significant investments in (duplication of) infrastructure are necessary to lead this market. Competing search engines deliberately try to differentiate themselves, for instance, in the dimension of privacy or sustainability. However, many competing search engines also rely on syndication agreements with other search engines (especially with Microsoft's Bing) for search results, which also limits their potential to differentiate themselves.

Suppose contestability in the narrow sense is desired and realistic, then the main search engine is supposed to be challenged by a not yet leading search engine. However, the thresholds for the number of users and business users at which a search engine qualifies as a core platform services are relatively low. This is especially so because business users do not necessarily have to actively sign up with the search engine, but only have to appear in the search index and be listed as a search result. In consequence, also not yet leading search engines may well have to provide access to its search and query data to third parties under the DMA, including to the main engine, as there is no restriction in Article 6(11) or anywhere else in the DMA that would prevent gatekeepers to access data by other gatekeepers made available under the DMA.¹²⁸ If contestability of the main search engine is indeed the short term goal of Article 6(11), which seems to be the most likely interpretation, such reciprocal data access may rather weaken than strengthen the position of the most likely challenger.

2.4 Fair, Reasonable, and Non-discriminatory Access

Gatekeepers do not have to provide access for free, as in the data portability provisions, but have to provide access on FRAND terms. It is worth considering the two main parts of FRAND access separately, that is, “non-discriminatory” and “fair and reasonable”. The former relates to who shall receive access and whether each data seekers receives the same data. The latter relates to an appropriate price for such access. Both are very challenging problems on their own and discussed in turn.

2.4.1 Providing non-discriminatory data access

One interpretation of ‘non-discriminatory’ could be that access has to be non-discriminatory in the sense that every third-party search engine should receive the same type of data. Another interpretation is that the gatekeeper must offer a menu of data access possibilities, and the third-party search engines can choose their appropriate access service from that menu. Both interpretations bear issues, as discussed below.

Different search engines have different needs for data, depending on their specific business model and value proposition. If a new search engine were to take on Google, then it would first need to pick at least one area (say product search, or people search) where it can potentially offer a true improvement over the incumbent's offering. But to that end, the access seeker would need to be able

¹²⁸ This is remarkably different to the draft proposal of the Data Act, where gatekeepers are supposed to be denied from accessing data made available under the Act.



to specify what kinds of data are most useful to it, or at least to be able to pick from a comprehensive menu of option.

In this regard, the access provision under Article 6(11) bears some specific challenges typically not present in other cases where FRAND access is required. That is, providing more detail in one dimension, almost certainly requires –through the need for anonymisation and technical limitations – to reduce detail in another dimension of the data.

- If the interpretation of FRAND is that every search engine shall receive the same data, then such tailoring of data access would not be possible. The access provider must then offer a one-size-fits-all access, which ultimately may not be truly helpful for anyone to be able to challenge the incumbent.
- If the interpretation is that access seekers can pick from a menu of options, then there may likely be issues with identifying the right specification of those options, and there certainly are additional challenges for anonymisation. Who is then to determine the kind of data access options? Can access seekers specify what kind of data they would want or can the gatekeeper determine what options are appropriate?

In the latter case, the gatekeeper likely has distorted incentives and in consequence is not likely to provide the most useful data to potential competitors. In the former case, the preferred data choice of access seekers must still meet anonymisation requirements and is thus limited. More fundamentally, if a menu of data sets is offered, each of which by itself would satisfy anonymisation requirements, then the data set that can be derived from combining these individuals data sets is much less likely to still satisfy the same anonymisation requirements. This would mean that access seekers could be limited to picking only one of the data access options offered (assuming that is sufficient to prevent recombination). Or, what would be worse for ‘contestability’, each individual data set must be more strongly anonymised (leaving less detail to the data), so that even if the menu of data sets is combined, sufficient anonymisation can be preserved.

2.4.2 What is the appropriate price for access under FRAND terms ?

Finally, the determination of a ‘fair and reasonable’ access price is a central issue of the FRAND access terms. In general, the **determination of a ‘fair and reasonable’ price is going to be heavily influenced by the implementation questions discussed above**, such as whether data is provided through a data trust, via data sandboxing (in-situ), what the scope of the data is, and how many data access options are to be provided. Thus, it seems advisable to achieve clarity on the other implementation questions first, before setting a price for access.

Next, a common understanding must be reached on the meaning of ‘fair and reasonable’ in this context. The price should be fair and reasonable not only to the access seekers, but also to the access provider. To this end, it can be useful to think in two broad price components:



- 1) the direct costs of providing access, which may be determined through accounting measures or (as is the case in telecom markets) through an engineering cost model
- 2) a mark-up, which is determined by economic considerations, such as a risk and innovation premium, or opportunity costs.

Such a ‘cost-plus’ breakdown of the access pricing is roughly also the approach that is used in other regulated network industries where some mandated access regimes with price regulation are in place, such as energy markets and telecoms. However, the lessons from these industries are that it is a formidable task to determine an appropriate price, and it took many years to achieve this.¹²⁹ **Much depends on the precise goal of the access regime.** The ‘efficient’ access price is going to be different depending on whether one wants to preserve innovation incentives of the incumbent (in this case the mark up and price should be higher), or whether one wants to promote entry (in which case the price should be lower). A notable difference to those regulated network industries is also that regulators were looking for an ‘efficient’ price, and not a ‘fair and reasonable’ price. In a FRAND regime, the price is not supposed to be unilaterally set by the regulator, but to be negotiated between access provider and access seeker.

Both parts, the determination of the direct costs, as well as the determination of the mark-up have their own challenges. With respect to direct costs, investments in IT infrastructure are typically lumpy and there exist large economies of scale and scope, which make it difficult to attribute costs to any specific activity. Moreover, marginal costs may be zero. In telecoms the concept of ‘incremental costs’ was therefore introduced, which measured the difference in cost at a supra-marginal level. Here the gatekeeper would have to demonstrate the costs that actually arise from providing access, and whether these costs occur only once (for setting up the access regime), repeatedly (which each new data set made available), or continuously (as access is being sought). Certainly gatekeepers have an incentive to inflate costs and to pursue clever accounting to prove it. These reasons have led regulators in the energy and telecom domains to use non-accounting/non-self-reporting methods of determining the costs over the years.

With respect to the appropriate **mark-up, the challenge is to balance innovation and sabotage incentives of the gatekeeper with those of the access seekers.** If the mark-up is low, the access provider may invest less in innovation of the service through which it was able to collect superior data, or it may innovate less in its ability to collect data. However, these innovation risks seem to be rather low in the context of gatekeepers under the DMA, especially a search engine, as these firms are financially very strong and have an inherently strong incentive to collect data. This may justify a lower mark-up. What seems to be more relevant are risks of sabotage, that is, efforts of the access provider to impede the quality of the data access (for instance, through providing lower quality data, or reducing the performance of the interface). A higher mark-up would reduce those incentives. Ultimately, according to the famous Efficient Component Pricing Rule (ECPR), the access provider

¹²⁹ For example, in telecom markets instead of looking at historic cost values, a complex “forward looking long-run incremental cost approach” (FLIRC) was devised, which built on inputs from an engineering model that would determine the cost that a hypothetically efficient incumbent would have using the currently available efficient technology. In energy markets, efficient costs are often determined through benchmarking – a procedure that is only available if there are several comparable firms in the market.



would have no incentives to sabotage anymore if the mark-up compensates exactly for the opportunity costs of providing access. However, as the goal is to make the market more contestable, a mark-up according to the theoretical concept of the ECPR is certainly too high – but provides an upper bound. In reverse, if contestability and entry is to be achieved, then a lower mark-up is justified, including a mark-up of zero.¹³⁰

Given all these issues with the determination of the cost-based component, the vast infrastructure that potential gatekeepers like Google or Microsoft have available, (which can be used to provide access); and arguing that the mark-up should be zero anyway in order to promote competition and contestability, one may ask whether the ‘fair and reasonable’ should not be zero after all. Instead of keeping innovation incentives intact through a price, one may also seek to be mindful in this regard with respect to which data ought to be shared. For example, as argued above, forcing the gatekeeper to reveal the combination of full search term and the full search results page (ranking) seems problematic from an innovation perspective. At the same time, the data provided needs to be ‘effective’ to facilitate contestability, which requires more than just the search terms (see above on which data should be provided).

In conclusion, given the complexity of issues that arise in this context, it seems unlikely that the access provider and access seekers can ever succeed in negotiating a FRAND access between themselves. Thus, the **Commission needs to provide some guidance on the key trade-offs** mentioned, and yet, it is likely that ultimately the issues need to be resolved in courts. This means, access may not be provided for years to come, unless the Commission is willing to impose interim measures. However, also in this case, a specification has to be made and trade-offs have to be addressed.

KEY QUESTIONS

- What is the **process by which data access options** are determined? Who can pick data to be provided and how many different access options must be made available?
- Can a price of zero be **‘fair and reasonable’**?

¹³⁰ In telecoms, this is known as Pure LRIC, where access providers receive only a compensation for the direct costs of access, but not a mark-up.



REFERENCES

Argenton, C., & Prüfer, J. (2012). Search engine competition with network externalities. *Journal of Competition Law and Economics*, 8(1), 73-105.

Attoresi, M., Moraes, T. & Zerdick, T. (2020). EDPS TechDispatch on Personal Information Management Systems. Available at: https://edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf

Barbaro, M. and Zeller, T. (2006). A Face is Exposed for AOL Searcher No. 4417749. *New York Times*. Available at: <https://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&r=0>

Baumol, W. J. (1986). Contestable markets: an uprising in the theory of industry structure. *Microtheory: applications and origins*, 40-54.

Competition and Markets Authority [CMA] (2020). Online platforms and digital advertising market study. Available at: <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>

Crémer, J., de Montjoye, Y. A., & Schweitzer, H. (2019). Competition for the digital era. Report for the European Commission.

Edelman, B., & Lai, Z. (2016). Design of search engine services: Channel interdependence in search engine results. *Journal of Marketing Research*, 53(6), 881-900.

Fishkin, R. (2019). Less than Half of Google Searches Now Result in a Click. SparkToro. Available at: <https://sparktoro.com/blog/less-than-half-of-google-searches-now-result-in-a-click/>

Furman, J., Coyle, D., Fletcher, A., McAuley, D., & Marsden, P. (2019). Unlocking digital competition: Report of the digital competition expert panel. Government of the United Kingdom. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/un_locking_digital_competition_furman_review_web.pdf

Graef, I. (2020). The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation- Competition Policy International, *Antitrust Chronicle* November 2020 (II), Available at SSRN: <https://ssrn.com/abstract=3740185>

Graef, I., & Prüfer, J. (2021). Governance of data sharing: A law & economics proposal. *Research Policy*, 50(9), 104330.

Hong, Y., He, X., Vaidya, J., Adam, N., & Atluri, V. (2009, November). Effective anonymisation of query logs. In *Proceedings of the 18th ACM conference on Information and knowledge management* (pp. 1465-1468).

Klein, T. J., Kurmangaliyeva, M., Prüfer, J., & Prüfer, P. (2022). How important are user-generated data for search result quality? Experimental evidence. Tilburg University Working Paper.



Krämer, J., Senellart, P., & de Streel, A. (2020). Making data portability more effective for the digital economy: Economic implications and regulatory challenges. CERRE Policy Report. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866495

Krämer, J., Schnurr, D., & Micova, S. B. (2020). The role of data for digital markets contestability: case studies and data access remedies. CERRE Policy Report.

Krishnan, U., Moffat, A., Zobel, J., & Billerbeck, B. (2020, April). Generation of Synthetic Query Auto Completion Logs. In European Conference on Information Retrieval (pp. 621-635). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-45439-5_41

Martens, B., Parker, G., Petropoulos, G., & Van Alstyne, M. W. (2021). Towards efficient information sharing in network markets. TILEC Discussion Paper No. DP2021-014, Available at SSRN: <https://ssrn.com/abstract=3956256> or <http://dx.doi.org/10.2139/ssrn.3956256>

Rocher, L., Hendrickx, J. M., & De Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nature communications, 10(1), 1-9. Available at: <https://www.nature.com/articles/s41467-019-10933-3>

cerre

Centre on Regulation in Europe



DMA HORIZONTAL AND VERTICAL INTEROPERABILITY OBLIGATIONS

Marc Bourreau



TABLE OF CONTENTS

INTRODUCTION	145
1. HORIZONTAL INTEROPERABILITY	146
1.1 The Obligation and its Objective.....	146
1.1.1 The DMA’s horizontal interoperability obligation	146
1.1.2 The Objective of the obligation.....	147
1.2 Interpretation and Implementation Issues.....	147
1.2.1 Usefulness and effectiveness of the horizontal interoperability obligation.....	147
1.2.2 Geographical scope.....	148
1.2.3 Trade-off between effectiveness and complexity or implementation costs: Basic standard functionalities	149
1.2.4 Trade-off between interoperability and privacy or security: Possible licensing regime .	150
1.2.5 Conditions of access: Price and reference offers.....	152
2. VERTICAL INTEROPERABILITY	154
2.1 The Obligation and its Objective.....	154
2.1.1 The two DMA vertical interoperability obligations.....	154
2.1.2 The objective of the obligations.....	155
2.1.3 Dual role of gatekeepers and risk of foreclosure.....	155
2.2 Interpretation and Implementation Issues.....	156
2.1.4 Dealing with access requests	156
2.1.5 Equivalence of input when proportionate.....	157
2.1.6 Definition of interfaces	157
2.1.7 Concerns about security and integrity: License for access seekers.....	158
2.1.8 Economic conditions for access	159
REFERENCES	161



INTRODUCTION

Digital markets have reached high degrees of concentration, limiting inter- and intra-platform competition. One instrument which has been introduced in the Digital Markets Act (DMA) to enhance competition and improve contestability, is to mandate the interoperability of platforms. Different products or services are interoperable if they can ‘work together,’ meaning that some functionalities they have in common can be used indifferently across them via appropriate information exchange.

The DMA introduces two forms of interoperability: (i) *horizontal interoperability*, limited to messaging services (‘number-independent interpersonal communications services’ (NIICS)) via Article 7; and (ii) *vertical interoperability*, via an access obligation to essential functionalities of operating systems or hardware capabilities of a given device (Article 6.7) and the possibility to install third-party app stores and sideload apps (Article 6.4). Horizontal interoperability allows network effects to be shared among competitors and aims at levelling the playing field between small and large players. Vertical interoperability allows innovative complementors to enter the market and compete on a level playing field with a gatekeeper controlling an essential input, such as an essential functionality of an operating system or hardware device.

In what follows, we first discuss the provisions regarding horizontal interoperability, and second, we review those that concern vertical interoperability.



1. HORIZONTAL INTEROPERABILITY

1.1 The Obligation and its Objective

1.1.1 The DMA's horizontal interoperability obligation

In the DMA, horizontal interoperability corresponds to an **access obligation for gatekeepers providing messaging services** (NIICS):

“a gatekeeper [providing] number-independent interpersonal communications services (...) shall make the basic functionalities of its number-independent interpersonal communications services interoperable with the number-independent interpersonal communications services of another provider (...) by providing the necessary technical interfaces or similar solutions that facilitate interoperability, upon request, and free of charge.” (Art. 7(1))

Thus, this access obligation concerns only a subset of the functionalities of the messaging services offered by gatekeepers, the so-called **“basic functionalities”** defined in Article 7(2), as we shall discuss below. Access is provided upon request from an access seeker and is **free of charge**.

Note that such an access obligation for NIICS **already existed in a different form in the European Electronic Communications Code (EECC)**,¹³¹ in Article 61(2.c) of that legislation. Under this code, the national telecommunications regulators may impose on the providers of number-independent interpersonal communications services obligations to make their services interoperable, including by relying on standards, if (i) those providers reach a significant level of coverage and user uptake; (ii) the Commission has found an appreciable threat to end-to-end connectivity between end-users and has adopted implementing measures specifying the nature and scope of any obligations that may be imposed by the national authorities; and (iii) the obligations imposed are necessary and proportionate to ensure interoperability of interpersonal communications services.¹³²

However, the DMA transforms this possibility introduced by the EECC for national regulatory authorities “to impose” interoperability under some conditions,¹³³ into an actual obligation for the designated gatekeepers. At the same time, the EECC seems to open the door to full interoperability, whereas the DMA considers only partial interoperability (for a given set of “basic functionalities”).

¹³¹ Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ [2018] L 321/36.

¹³² EECC, art 61(2c). As noted by the Commission services, this need could arise from a significant decline in usage of the number-based communications system, so that the public interest in end-to-end connectivity can no longer be assured through that system – either because a single NIICS becomes the predominant mode of interpersonal communications or because of market fragmentation with a large number of different, non-interoperable communications applications: European Commission, *Review of the Electronic Communications Regulatory Framework* (Executive Summary 2: Electronic communications services and end-user rights, 2016) p. 3. http://ec.europa.eu/information_society/newsroom/image/document/2016-52/executive_summary_2_-_services_40995.pdf (accessed November 8, 2022).

¹³³ There are three conditions to impose horizontal interoperability under the EECC that are not in the DMA: (1) the communications services must have reached a significant level of coverage and user up-take; (2) the Commission determines that there is an appreciable threat to end-to-end connectivity between end users; and (3) the obligations imposed are necessary and proportionate to ensure the interoperability of interpersonal communications services.



1.1.2 *The Objective of the obligation*

The main objective pursued with horizontal interoperability is to **improve contestability**, one of the two overarching aims of the DMA:

“The lack of interoperability allows gatekeepers that provide number-independent interpersonal communications services to benefit from strong network effects, which contributes to the weakening of contestability.” (Rec. 64)

This is the standard rationale for interoperability in network industries. Without interoperability, network effects are firm-specific and proprietary. Therefore, firms have strong incentives to expand their proprietary network to offer larger network benefits to users than their rivals. In an extreme scenario, the market may tip in favour of one firm, and market contestability will be limited. By contrast, with interoperability, network effects are shared between rivals and constitute a public good. Competition can emerge and develop along other dimensions than network effects, like service quality or innovative functionalities.

Horizontal interoperability may also spur competition between ecosystems more widely, in a context where one of the barriers to switching ecosystems is perceived to be the loss of connection with family and friends within the same ecosystem as the core messaging app.

1.2 Interpretation and Implementation Issues

1.2.1 *Usefulness and effectiveness of the horizontal interoperability obligation*

The **standard argument in favour of horizontal interoperability is that it levels the playing field between small and large players** and, by doing so, increases competition and contestability (see, for example, Scott Morton et al., 2021). In the academic economics literature, the reference study that comes to this conclusion is the paper by Crémer, Rey and Tirole (2000) on the impact of interoperability on competition between small and large networks. The authors show that interoperability increases network effects for all users because it allows them to communicate both on- and off-net. As services become more valuable due to larger network effects, irrespective of the supplier, the market expands, which benefits all market players. At the same time, the competitive advantage of large players in terms of network effects is reduced due to interoperability, since users of small networks have access to (almost) the same network as users of large networks. Thus, interoperability levels the playing field between small and large players, reduces entry barriers and, improves market contestability.

This standard argument **ignores the possible interplay between interoperability and multihoming**. Empirical evidence shows that multihoming is widespread in the market for messaging services. For instance, according to a survey conducted by WIK (2022) in Germany in 2021, 75% of users of messaging services multihome.¹³⁴ If we consider only messaging services from different providers, the extent of multihoming is lower, but still significant; the study finds that 61% of users multihome messengers from different suppliers. Therefore, there exists some competition between messaging

¹³⁴ Analysys Mason provides similar empirical evidence for the UK (see: “The Digital Markets Act proposes messaging interoperability, but this is easier said than done,” Analysys Mason, April 2022).



platforms via multihoming.¹³⁵ However, interoperability may substitute for multihoming since it allows users to access all networks at lower costs,¹³⁶ possibly with a quality loss.¹³⁷ Therefore, from a policy perspective, interoperability and multihoming may represent two substitute means to enhance competition and improve contestability in digital markets.

Bourreau and Krämer (2022) develop a theoretical model of competition between an incumbent platform and a more efficient entrant, where the market tends to tip due to strong network effects. They show that mandated interoperability can reduce contestability, that is, the likelihood that the more efficient entrant supplants the incumbent in the long term (the optimal outcome since the entrant is more efficient). The reason for this result is that interoperability reduces multihoming. However, multihoming allows the entrant to survive in the market dominated by the incumbent until it has an opportunity to grow, reach a critical mass of users and displace the incumbent.¹³⁸ In conclusion, left aside from the implementation challenges that we discuss below, the ability of horizontal interoperability to improve contestability cannot be taken for granted.

With these reservations in mind, it is striking that some major competitors, such as Signal and Threema, have announced that they are not keen to use the interoperability provision.¹³⁹ In particular, Julia Weiss, spokesperson of Threema, declared that “[i]nteroperability would cement the monopoly of the top dogs, instead of breaking it up. If existing users of free messenger A with bad privacy practices could communicate with users of privacy-conscious paid messenger B, they will not pay money for messenger B, effectively depriving it of its only source of revenue.”

Therefore, it would make sense to **monitor the market shares and the extent of multihoming** for messaging services following the implementation of horizontal interoperability to check if this provision has the intended effect. Another relevant indicator to evaluate the effectiveness of the measure would be the volume of traffic going through the interfaces implemented for interoperability.

1.2.2 Geographical scope

An important question of interpretation of the horizontal interoperability provision in the DMA concerns its geographical scope. **Does it only require that a user in the European Union (EU) should be able to communicate with any other user also based in the EU? Or is it a more global obligation** requiring every user to connect to every other user, including outside of the EU? In our view, the general objective of effectiveness in the DMA dictates that *global* network effects should be shared for the interoperability provision to have its intended effect in terms of competition and contestability. Therefore, our reading is that messaging users of gatekeepers within the EU must be

¹³⁵ While users can multihome, the market is still very concentrated around a few main applications. According to a BEREC study, the main messaging applications identified by 84% of EU consumers belong to only one company (Meta); see BEREC (2021), p. 42.

¹³⁶ Multihoming may entail additional (transaction) costs for users, such as additional learning costs or the costs of maintaining and managing contacts across several platforms. Typically, horizontal interoperability allows users to save these costs.

¹³⁷ Since interoperability is partial (i.e., it applies only to a set of “basic functionalities”), the quality of interaction is lower than with multihoming, where the complete set of functionalities can be used.

¹³⁸ See also Bourreau, Krämer and Buiten (2022).

¹³⁹ See, “Europe’s Digital Markets Act Takes a Hammer to Big Tech,” Wired, March 2022, <https://www.wired.com/story/digital-markets-act-messaging/>.



able to talk to any user in the world. In any case, the geographical scope of the provision has to be clarified.

1.2.3 *Trade-off between effectiveness and complexity or implementation costs: Basic standard functionalities*

The interoperability obligation in the DMA applies only to a set of “basic functionalities” defined in Article 7(2) to the extent that “*the gatekeeper itself provides [them] to its own end users.*” At the start, the “basic functionalities” consist of one-to-one text messaging and sharing of images, voice messages, videos and other files. These interoperable functionalities should be available to group messaging within two years. Then, within four years, voice and video calls should also be made interoperable. Thus, interoperability is only partial, not full. The interoperability requirement applies only to some “standard” functionalities, leaving other “non-standard” functionalities aside. This partial level of interoperability reflects a **trade-off between the provision’s effectiveness on the one hand, and complexity, implementation costs, and possibilities of differentiation on the other.**

A higher level of interoperability (for example, more functionalities being interoperable) would make it more effective in promoting competition and reducing entry barriers. Indeed, the levelling effect of interoperability between the dominant gatekeepers and their competitors (or potential competitors) is more pronounced if a larger set of functionalities becomes interoperable. With partial interoperability, competition is still shaped by the network effects specific to each firm. Since they have a larger network, incumbent players may keep a competitive advantage.¹⁴⁰ However, providing a higher level of interoperability is likely to increase the complexity and costs of implementation, for instance, when more specific or complex features are considered. It can also reduce the possibilities of differentiation as the set of “non-standard” functionalities shrinks. This can harm innovation for new features and lead to less choice and variety for end users eventually, a concern raised in various policy reports (such as, by the CMA (2020); by the German Monopoly Commission (2021); and, by the German Federal Network Agency (2021)). Thus, **it makes sense to apply the interoperability requirement only to a subset of “basic functionalities.”**

The DMA precisely specifies a minimum set of “basic functionalities”.¹⁴¹ However, we think that solving this trade-off (for example, by picking the functionalities with the strongest impact on competition, while keeping complexity and implementation costs at a reasonable level) may lead to **a different set of interoperable “basic functionalities” for each messaging service** concerned by the regulation. For instance, voice calls may be the key “basic functionalities” to interoperate for some services, while it could be text messaging for others. The DMA does not allow for this kind of flexibility in defining “basic functionalities” on a case-by-case basis.

Besides, how can this list of interoperable “basic functionalities” be **adapted if usage evolves towards ‘new’ types of messaging functionalities**, making the ‘old’ functionalities obsolete? For instance, some messaging apps have shifted towards self-deleting media, while some users now communicate mainly

¹⁴⁰ The same problem arose in telecommunications, where interconnection did not eliminate the significance of network effects. Large players could exploit their network effects by imposing differentiated on-net and off-net prices, making it more attractive for users to join a large network.

¹⁴¹ The European Commission can extend this list.



via emojis or GIFs. If the provisions are not adapted fast enough, there is a risk that interoperability quickly becomes ineffective in levelling the playing field between small and large players. Article 12(3) of the DMA mentions the possibility for the Commission to conduct a market investigation to identify the “*need to keep [the interoperability] obligations up to date.*” However, the question is whether this kind of procedure can keep up with the fast pace of innovation in the digital sector. On the other hand, if any new innovative functionality introduced by a gatekeeper is made interoperable immediately, innovation incentives will be substantially harmed.

1.2.4 Trade-off between interoperability and privacy or security: Possible licensing regime

The DMA states that horizontal interoperability obligations should not reduce security or privacy for end users:

*“The **level of security**, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users **shall be preserved** across the interoperable services.”* (Art. 7(3))

*“The gatekeeper shall collect and exchange with the provider of number-independent interpersonal communications services that makes a request for interoperability **only the personal data of end users that is strictly necessary** to provide effective interoperability.”* (Art. 7(8))

However, **achieving interoperability without affecting security or privacy is challenging**. Consider the two possible approaches to develop interoperable messaging services:

- Providing access to Application Programming Interfaces (APIs) that the gatekeepers may already use for their own systems; and
- Adopting and implementing a universal open and secure (encryption) standard.

The second approach (standardisation) would be best suited for new (interoperable) messaging services, and it could provide a similar level of security as that of existing proprietary messaging services (such as, with end-to-end encryption). However, the messaging services of gatekeepers concerned by the regulation already exist and rely on different technologies. Standardising existing services *ex-post* would be highly complex, time-consuming, and costly (not to speak of the strong resistance from the firms).

Recital 96 of the DMA acknowledges that the implementation of interoperability “*could be facilitated by the use of technical standards*” and that “*it should be possible for the Commission, where appropriate and necessary, to request European standardisation bodies to develop them.*” However, the DMA does not go as far as obliging gatekeepers to adopt such standards if they are already developed. Since there are important potential downsides associated with *ex-post* standardisation (such as, the costs of switching to a new architecture for service providers or reduced innovation incentives), we do not consider it desirable that there is such an actual obligation.



Without a universal encryption standard, interfaces must be introduced to interoperate messaging services, which corresponds to the first approach outlined above. Experts tend to agree that, in this case, achieving **end-to-end encryption across multiple applications is not possible**.¹⁴² In particular, interoperability may require sharing of encryption keys outside of individual apps, raising questions about which apps are eligible to access the keys. Security issues become even more complex with group chat and voice or video calls (see, for example, WIK, 2022).

Besides, platforms may have to constantly update their interfaces to improve security or cope with threats as they arise. Any access seeker would have to keep up with these changes to make interoperability effective, increasing complexity and implementation costs. Alternatively, access providers would have to slow down the pace of innovation in fear of breaking access for existing access seekers.

Therefore, implementing interoperability involves a trade-off in terms of security. In this context, it seems crucial to **consider the incentives of all parties (both access providers and access seekers) to maintain a sufficiently high level of security for users**. Indeed, each party may have an insufficient incentive to offer secure communication since it may not fully bear the costs of a security breach (external effects).

Similarly, interoperability may harm end-user privacy even if “*only the personal data of end users that is strictly necessary to provide effective interoperability*” is exchanged. For instance, imagine a malevolent messaging service interconnecting with a gatekeeper. Any data exchange, even if kept to the strict minimum necessary, would lead to consumer harm. More generally, personal data used to provide effective interoperability may be (re)used for other purposes, with possible consumer harm.

Finally, note that Article 7(7) of the DMA requires that end users must be “*free to decide whether to make use of the interoperable basic functionalities*.” Besides, Article 7(8) requires that the “*collection and exchange of the personal data of end users*” necessary to provide effective interoperability complies with the GDPR and the e-Privacy Directive. To comply with these two requirements, an **opt-in regime for interoperability is likely to be necessary**. Though it may increase the complexity of implementation, an opt-in regime allows each individual user to balance the potential benefits and costs (such as, in terms of privacy or security) of interoperability.

Mitigating security or privacy risks advocates for **screening potential access seekers, with the question of how trustworthy** a given access seeker is. The DMA allows any messaging service provider to request access free of charge to the messaging service of a gatekeeper based on the reference offer; this includes both existing competing messaging services and potential entrants (for example, any “*provider offering or intending to offer such services in the Union*” – Article 7(1)). However, the DMA introduces some potential safeguards.

First, the gatekeeper is obliged to accept only “**reasonable**” requests for interoperability:

¹⁴² See WIK, (2022) for a comprehensive analysis. See also Wired, (2022), ‘Forcing WhatsApp and iMessage to Work Together Is Doomed to Fail’. Available at: <https://www.wired.com/story/dma-interoperability-messaging-imessage-whatsapp/> The Verge, (2022), ‘Security experts say new EU rules will damage WhatsApp encryption’. Available at: <https://www.theverge.com/2022/3/28/23000148/eu-dma-damage-whatsapp-encryption-privacy>



“The gatekeeper shall comply with any reasonable request for interoperability within 3 months after receiving that request by rendering the requested basic functionalities operational.”
(Art. 7(5))

Nevertheless, what “reasonable” precisely means is not defined. The rest of the text suggests that it is, in particular, a question of **security**:

“The Commission may, exceptionally (...) extend the time limits for compliance (...) where the gatekeeper demonstrates that this is necessary to ensure effective interoperability and to maintain the necessary level of security, including end-to-end encryption, where applicable.”
(Art. 7(6)).

Whether a request is “reasonable” will probably be evaluated on a case-by-case basis and depend on the gatekeeper or the type of functionality. However, it would be appropriate to define what is a “reasonable” request in general. For instance, the access seeker could have to meet some security and privacy standards to make an access request possible to satisfy, given the gatekeeper’s technical architecture, for the request to be deemed “reasonable.”

Second, the gatekeeper is entitled to take measures to **maintain the integrity of its network** whenever interoperability raises privacy and security risks:

*“The gatekeeper shall not be prevented from taking measures to ensure that third-party providers of number-independent interpersonal communications services requesting interoperability do not **endanger the integrity, security and privacy** of its services, provided that such measures are strictly necessary and proportionate and are duly justified by the gatekeeper.”* (Art. 7(9)).

The DMA seems to imply that the access provider screens which access seekers are eligible for access. This may raise competition problems, as there could be a thin line between what is appropriate to ensure a safe environment for privacy and/or security, and possible anticompetitive discrimination.

To alleviate these problems, another possibility would be that a **regulatory body or a third party (such as, an independent industry body) grants access licenses based on objective criteria**, as Bourreau, Krämer and Buiten (2022) argue. For instance, the access seeker may have to demonstrate that it meets certain standards in terms of security or privacy protection. To avoid strategic obstruction, we recommend this latter approach.

1.2.5 *Conditions of access: Price and reference offers*

Gatekeepers may have a strong incentive to resist interoperability and adopt various sabotage tactics to make it ineffective. Indeed, allowing for interoperability may be costly due to increased competition (the “levelling effect”), but it may also entail direct costs for its implementation. The DMA does not consider covering these direct costs - interoperability must be offered **“free of charge.”** On the one hand, free access reduces entry barriers for potential entrants. On the other, it gives an incentive to resist the access provision or degrade the quality of access. In comparison, access prices have always been at least cost-oriented in the telecommunications sector.



To avoid these problems (such as, the degradation of the quality of access), the **precise technical terms of the reference offers will be crucial** for the provision's success. The DMA does not specify what the reference offer must contain, but it introduces the possibility of consulting BEREC. Nonetheless, the evaluation or auditing of reference offers for a very diverse set of messaging services could be a complicated and time-consuming task, leading to further delays in the practical implementation of the interoperability obligation.

Finally, the DMA is silent on the pace of revisions of reference offers. For instance, the reference offers for interconnection in telecommunications are typically revised annually. Given the fast pace of innovation in digital technologies, the gatekeepers may have to update the technical details for interoperability at a relatively fast pace. This raises various questions, such as how well in advance the access seekers should be informed of the forthcoming changes.



2. VERTICAL INTEROPERABILITY

2.1 The Obligation and its Objective

2.1.1 *The two DMA vertical interoperability obligations*

Vertical interoperability allows services at different levels of the digital value chain to work together. The DMA introduces two vertical interoperability requirements: (i) the sideloading of applications and app stores (Article 6(4)); and (ii) access to essential functionalities of operating systems (Article 6(7)).

The *first* vertical interoperability provision allows end users to **sideload apps and app stores**. It means that users can run different app stores on the same operating system or download an app without using the gatekeeper's app store:

“The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper.” (Art. 6(4)).

The *second* vertical interoperability requirement introduced in the DMA concerns **access to essential hardware or software functionalities of the operating system** that are used by the gatekeepers for their own products or services (such as, near-field-communication hardware and software components for contactless payments):

“The gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant (...) as are available to services or hardware provided by the gatekeeper.” (Art. 6(7))

Article 6(7) states that gatekeepers must give access to *“the same hardware and software features accessed or controlled via the operating system or virtual assistant (...) as are available to services or hardware provided by the gatekeeper.”* Recital 55 restricts this access provision to *“competing service or hardware providers”* which need such access *“to be able to provide a competitive offering to end users,”* hence, third parties competing with the gatekeeper's complementary products and services.

The terms of **access to these essential “features” have a technical and an economic dimension.**

- The technical access conditions must detail precisely which features and functionalities are given access to; how security and integrity are being maintained; performance criteria for the interface; how changes to the interfaces can be implemented, and how such changes are notified to the access seekers.
- Economic access conditions specify who is eligible to access, and what the appropriate access pricing scheme should be (if any).



Besides, third parties should have the possibility to invite (“**prompt**”) end users to set their app or app store as their default, which is related to the user switching tool analysed in a companion CERRE issue paper. Finally, some security safeguards are introduced (see below).

2.1.2 *The objective of the obligations*

In principle, vertical interoperability **facilitates the entry of complementors** by providing them access to essential components they cannot easily replicate.¹⁴³ It also allows them to compete on a level playing field with the products and services offered by the gatekeepers that rely on those components. Finally, for some complementors, such entry can represent a stepping stone, a successful niche entry allowing them to later expand into other product and service areas.

Regarding sideloading, Recital 50 states that restrictions to the ability of end-users “*to install and effectively use third party software applications or software application stores on hardware or operating systems of [a] gatekeeper (...) should be prohibited as **unfair** and liable to weaken the **contestability** of core platform services*” as this limits third parties’ ability to use alternative distribution channels and reduces end users’ choice set.

In its Recital 54, the DMA acknowledges that the gatekeepers’ control over essential hardware and operating systems’ components may harm competition by limiting user switching:

*“Gatekeepers can also technically limit the ability of end users to effectively switch between different undertakings providing internet access service, in particular through their control over hardware or operating systems. This **distorts the level playing field** for internet access services and ultimately harms end users.”* (Rec. 54)

In this context, vertical interoperability can level the playing field between gatekeepers and potential rivals:

*“[C]ompeting service or hardware providers (...) require equally effective interoperability with, and access for the purposes of interoperability to, the same hardware or software features to be able to provide a **competitive offering** to end users.”* (Rec. 55)

2.1.3 *Dual role of gatekeepers and risk of foreclosure*

Article 6(4) allows third-party application developers to use alternative and cheaper distribution channels. This should facilitate entry by reducing entry costs for developers, which will be able to pick the distribution channel most suited to their business. Facilitated entry should then translate into increased consumer choice. The main concerns relate to integrity and security; we will return to these problems below.

Article 6(7) deals with a more complex problem, when gatekeepers control an operating system (OS) or a device and offer products or services that rely on specific functionalities of these systems:

¹⁴³ For an analysis of the essential components in the mobile ecosystems, see Feasey and Krämer (2021).



*“Gatekeepers can (...) have a **dual role** as developers of operating systems and device manufacturers, including any technical functionality that such a device may have. For example, a gatekeeper that is a manufacturer of a device can restrict access to some of the functionalities in that device (...), which can be required for the effective provision of a service provided together with, or in support of, the core platform service by the gatekeeper as well as by any potential third party undertaking providing such service.” (Rec. 56)*

Vertical integration may increase efficiency, for instance, by eliminating double marginalisation or fixing the hold-up problem (see Copenhagen Economics (2020), and Bourreau and Krämer (2022)). However, **due to their “dual role,”** gatekeepers may also have the ability and incentive to use their control over the essential functionalities of their OS or device to **restrict competition** in the downstream markets for products or services relying on those functionalities, as Recital 57 outlines:

“If dual roles are used in a manner that prevents alternative service and hardware providers from having access under equal conditions to the same operating system, hardware or software features that are available or used by the gatekeeper in the provision of its own complementary or supporting services or hardware, this could significantly undermine innovation by such alternative providers, as well as choice for end users.”

Thus, the aim of the obligations detailed in Article 6(7) is *“to allow competing third parties to interconnect through interfaces or similar solutions to the respective features as effectively as the gatekeeper’s own services or hardware.”* (Rec. 57)

Indeed, in a context where a firm controls an essential input (which cannot be replicated or bypassed) while being active in the downstream market, this firm may have the incentive to foreclose its downstream competitors. Various strategies may have this effect, such as refusal of access, margin squeeze (whereby the integrated firm does not leave enough economic space for rivals to be active), sabotage of the upstream input (such as, the provision of a degraded version of the input to downstream rivals), discriminatory information disclosure, and so on.

Vertical separation would be one possible remedy, but the DMA adopts another approach, with (non-discriminatory and free-of-charge) access provision to the essential input for downstream rivals. Therefore, the key question for the implementation of the vertical interoperability provision contained in Article 6(7) relates to the access terms.

2.2 Interpretation and Implementation Issues

2.1.4 Dealing with access requests

The vertical interoperability provision is broad. A gatekeeper shall give access to any functionalities *“accessed or controlled via the operating system or virtual assistant (...) as are available to services or hardware”* that it provides (Art. 6(7)).

Therefore, the gatekeeper may receive several access requests for different essential functionalities. This contrasts with telecommunications, for instance, where interconnection requests concern only a few network elements (such as, the local loop).



Therefore, there should be a process for handling those requests efficiently. As with the other aspects of access provision, one possible approach would be to **allow the gatekeeper to define this process under regulatory oversight**.

2.1.5 *Equivalence of input when proportionate*

To mitigate the risk of foreclosure discussed above, we argue that the general guiding principle for such access provision should be the ‘equivalence of input’ when this is respecting the principle of ‘proportionality’; that is, the entrant should have access to the same functionalities, and on the same terms, as the vertically integrated gatekeeper, for its own complementary products and services relying on the essential features. When it is not proportionate, an equivalence of output may alternatively be imposed.

This approach has been used in regulated industries like telecommunications to define the technical and economic conditions for access.¹⁴⁴ It is consistent with Recital 55, which states that:

*“[C]ompeting service or hardware providers (...) require **equally effective** interoperability with, and access for the purposes of interoperability to, the same hardware or software features to be able to provide a competitive offering to end users.”* (Rec. 55)

The ‘equivalence of input’ principle requires monitoring to verify that the access provider satisfies the principle. In telecommunications, it is a time-consuming task, requiring regular audits. However, telecommunications networks are standardised, which facilitates learning and regulators’ job. The digital technologies potentially concerned by the vertical interoperability provisions are much more diverse, making the monitoring of the ‘equivalence of input’ particularly complex and time-consuming. One possibility would be to have a first level of monitoring, where access providers would submit their process in their annual compliance reports. In the case of business user complaints, more stringent forms of monitoring (such as, via audits) could be introduced.

2.1.6 *Definition of interfaces*

The “effective interoperability” or “access” to the hardware and software features controlled by the gatekeeper requires the definition of relevant hardware or software interfaces. A relevant question is, who should define the interfaces?

The first possibility is that the **gatekeeper itself designs the interconnection access interface and provides access in a non-discriminatory way**. From a technical perspective, this approach seems efficient as the platform is better placed to design the interface as it has developed the hardware or software technology. Besides, the platform can update the interface smoothly when technical changes are needed and can also take the necessary measures to ensure integrity and security. However, this approach also provides the platform with the ability to impede access in various ways and foreclose its competitors in the complementary product and service markets. Such sabotage tactics may be difficult and time-consuming to monitor.

¹⁴⁴ For instance, see Commission Recommendation 2013/466 of 11 September 2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment, O.J. [2013] L 251/13.



An alternative approach would consist in **developing an open interface standard**. Recital 96 of the DMA acknowledges that *“the implementation of some of the gatekeepers’ obligations, such as those related to data access, data portability or interoperability could be facilitated by the use of technical standards.”* However, the standardisation of interfaces may take a lot of time, and it may be complex to reach a consensus among market players with different (and sometimes conflicting) incentives.

Therefore, we think the best (and most appropriate) approach is the first, where the gatekeeper manages access and interfaces. In case of complaints and concerns about possible non-compliance, the regulator would investigate the technical specifications of the access interface.

2.1.7 *Concerns about security and integrity: License for access seekers*

Vertical interoperability may raise concerns regarding the security and integrity of hardware and software systems, and more broadly user safety. Therefore, the DMA acknowledges that the gatekeeper is entitled to take the necessary measures to ensure security and integrity:

*“The gatekeeper shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the **integrity** of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper.”* (Art. 6(7))

*“The gatekeeper shall not be prevented from taking 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 measures go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.”* (Art. 6(4))

*“Furthermore, the gatekeeper shall not be prevented from applying measures and settings other than default settings, enabling end users to effectively protect **security** in relation to third-party software applications or software application stores, provided that such measures and settings go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.”* (Art. 6(4))

Those measures (which can be *“technical”* or *“contractual”* according to Recital 50) must be strictly necessary, proportionate and duly justified. Recital 50 adds that the gatekeeper must demonstrate *“that there are no less-restrictive means to safeguard the integrity of the hardware or operating system.”* Besides, those measures cannot consist of *“default setting”* or *“pre-installation”* (Rec. 50).

As with horizontal interoperability, the gatekeeper decides which measures are necessary to protect the integrity of its system if they are *“proportionate”* and *“duly justified.”* This seems efficient as the gatekeeper knows its technology best. However, the gatekeeper is vertically integrated and therefore, it may have the ability and incentive to take technical measures that not only protect security and integrity, but also harm potential rivals. Therefore, a regulator should monitor the security measures introduced by the gatekeeper, which may be particularly complex and time-consuming.



To protect the integrity and security of hardware and software systems (in all dimensions: product integrity, user safety, and so on), it would make sense to offer access only to players that comply with certain security or privacy standards. **To screen access seekers, access licenses** could be granted based on objective criteria and revoked in case of misconduct.

One possible approach would be to allow the gatekeeper to grant access licenses based on public and objective criteria. Another possible approach would be to confer this role to the regulator or an independent third party. Finally, there could be a middle ground where the **gatekeeper grants access, but if the access seeker is denied access, it can appeal to the regulator**. In any case, it seems necessary that the regulator scrutinises the process to avoid the gatekeeper refusing reasonable access requests. Therefore, the two last approaches seem preferable to the first one.

However, the DMA does not indicate whether access seekers can be screened, for instance, *via* access licenses. Article 6(7) states that the gatekeeper must offer access to *“the same hardware and software features accessed or controlled via the operating system or virtual assistant (...) as are available to services or hardware provided by the gatekeeper”* for *“providers of services and providers of hardware.”* Similarly, Article 6(4) states that the gatekeeper must *“allow and technically enable the installation and effective use of third-party software applications or software application stores (...)”*. In both articles, it seems that no screening is done.

However, the gatekeeper is entitled to take the necessary measures to *“ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features”* that it provides (Article 6(7)) and that *“third party software applications or software application stores do not endanger the integrity of [its] hardware or operating system (...)”* (Article 6(4)). Therefore, we recommend that granting access licenses based on objective criteria should be viewed as “necessary” and “proportionate” measures to ensure security.

2.1.8 *Economic conditions for access*

In network industries, firms typically pay a wholesale price to access infrastructure. This is the case in telecommunications, for instance, for interconnection and access to the local loop. The access price should be low enough to minimise entry barriers and encourage competition. At the same time, it should not be too low to avoid inefficient entry and low investment incentives for infrastructure owners and access seekers. Low access prices might also encourage infrastructure owners to engage in non-price discrimination.

In the context of the DMA, the legislator has decided that access to “hardware and software features” would be **provided “free of charge”** (Article 6(7)). This access price, seemingly set to zero, thus strikes a balance towards entry, competition, and innovation by complementors. However, such a low access price could attract inefficient entrants, and the incentives of gatekeepers to invest and maintain their functionalities may be harmed. Vertical access with low compensation may also reduce the gatekeeper’s innovation incentives.¹⁴⁵ Finally, it may encourage gatekeepers to adopt non-price

¹⁴⁵ See Bourreau and Krämer (2022) for a more in-depth discussion.



discrimination strategies. Therefore, we would rather recommend that the **costs of providing access for gatekeepers be covered, at least partly, by access seekers.**

In any case, the choice of “*free of charge*” access makes it particularly important to screen access seekers to avoid entry of inefficient entrants and closely monitor the access conditions offered by gatekeepers to access seekers, to avoid non-price discrimination.



REFERENCES

BEREC, (2021). 'Analysing EU consumer perceptions and behaviour on digital platforms for communication'. Analysis report. BoR (21), pg. 89.

Bourreau, M. & J. Krämer, (2022). 'Interoperability in Digital Markets: Boon or Bane for Market Contestability?' Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4172255

Bourreau, M., Krämer, J. & M. Buiten, (2022). 'Interoperability in Digital Markets', Centre on Regulation in Europe (CERRE) Report, available at: https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf

CMA, (2020). 'Online platforms and digital advertising. Market study final report.' Available at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_AL_T_TEXT.pdf

Copenhagen Economics, (2020). 'The economic rationale for vertical integration in the tech sector'. Available at: <https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/0/550/1606320780/copenhagen-economics-the-economic-rationale-for-vertical-integration-in-tech.pdf>

Crémer, J., Rey, P. & J. Tirole, (2000). 'Connectivity in the Commercial Internet'. *Journal of Industrial Economics*, Vol. 48(4), pp. 433-472.

Feasey, R. & J. Krämer, (2021). 'Device Neutrality: Openness, Non-Discrimination and Transparency on Mobile Devices for General Internet Access'. CERRE Report, available at: https://cerre.eu/wp-content/uploads/2021/06/CERRE_Device-neutrality_FINAL_June-2021.pdf

Monopoly Commission [Monopolkommission], (2021). 'Telekommunikation 2021: Wettbewerb im Umbruch'. 12. Sektorgutachten der Monopolkommission. Available at: [https://www.monopolkommission.de/index.php/de/gutachten/sektorgutachten-telekommunikation/375-12-sektorgutachten-telekommunikation-2021.html#:~:text=Sektorgutachten%20Telekommunikation%20\(2021\)%3A%20Wettbewerb%20im%20Umbruch,-Drucken&text=Die%20Monopolkommission%20stellt%20heute%20ihr,Glasfasernetze%20sollte%20wettbewerbskonform%20ausgerichtet%20werden.](https://www.monopolkommission.de/index.php/de/gutachten/sektorgutachten-telekommunikation/375-12-sektorgutachten-telekommunikation-2021.html#:~:text=Sektorgutachten%20Telekommunikation%20(2021)%3A%20Wettbewerb%20im%20Umbruch,-Drucken&text=Die%20Monopolkommission%20stellt%20heute%20ihr,Glasfasernetze%20sollte%20wettbewerbskonform%20ausgerichtet%20werden.)

Scott Morton, F. M., Crawford, G. S., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P., & Seim, K., (2021). 'Equitable Interoperability: the "Super Tool" of Digital Platform Governance'. Policy Discussion Paper No. 4, Digital Regulation Project, Yale Tobin Center for Economic Policy. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3923602

WIK, (2022). 'Interoperability regulations for digital services: Impact on competition, innovation and digital sovereignty especially for platform and communications services'. Study for the Federal Network Agency. Available at: <https://www.wik.org/en/veroeffentlichungen/studien/weitere-seiten/interoperability-regulations-for-digital-services>

cerre

Centre on Regulation in Europe



PROCEDURES AND INSTITUTIONS IN THE DMA

Giorgio Monti



TABLE OF CONTENTS

INTRODUCTION	164
1. THE SUPERVISORY STRUCTURE OF THE DMA	165
1.1 Compliance Reports	165
1.2 Self-assessment.....	167
1.3 Co-operative Compliance.....	167
1.4 Enhanced Supervision	168
1.5 Detection.....	169
1.6 The Challenges of Gatekeeper Supervision	169
2. ENFORCEMENT	171
2.1 Investigative Powers	171
2.2 Interim Measures.....	171
2.3 Non-compliance Decision	172
2.4 Fines	173
2.5 Judicial Review	174
2.6 Implementing Acts and Guidelines	174
3. RESPONSIVE REGULATION	175
4. RIGHTS AND INTERESTS	178
4.1 Fundamental Rights of Gatekeepers.....	178
4.2 Third Parties	178
5. PRIVATE ENFORCEMENT	182
6. INSTITUTIONAL DESIGN OF THE DMA	184
6.1 Co-operation with National Authorities	184
6.2 EU-level Co-operation	186



INTRODUCTION

The Digital Markets Act (DMA) creates a new system for the enforcement of European Union (EU) Law.¹⁴⁶ Normally, EU Law is enforced at national level, sometimes by mandating independent authorities that are tasked with the public enforcement of these rules and often relying just on private litigation. National authorities are complemented by EU-level networks that facilitate the sharing of information and identification of good practices as well as adopting soft laws that stimulate convergence. The one exception to this system has always been competition law where enforcement took place at national and European level in parallel, with the Commission dominating enforcement in the early years.¹⁴⁷ Supervision of systemically significant banks is now also centralised,¹⁴⁸ and some other policy fields like trade and the Common Agricultural Policy are also enforced at EU level. However, the bulk of EU rules affecting firms are enforced by national regulators or are left to private enforcement

The DMA instead creates a one-stop shop: designated gatekeepers are asked to inform the European Commission (the Commission) of how they envisage complying with the obligations that apply to them, and the Commission has exclusive competence to enforce the rules. With great power comes great responsibility, not least to ensure that enforcement is both effective and also safeguards the fundamental rights and interests of the gatekeepers, as well as third parties.

The DMA contains a second novelty, for it changes the enforcement culture that gatekeepers are used to under antitrust. It adopts a supervisory mechanism to secure compliance. While this is backed up by a traditional enforcement arsenal which draws on antitrust law, the relationship between gatekeepers and DGs COMP and CNECT is intended to be supervisory, where the compliance efforts of gatekeepers are kept under regular review. The extent to which this materialises depends on the way the Commission and gatekeepers implement the DMA.

This paper is organised in the following manner: We start by considering the supervisory architecture (section 1), followed by the formal enforcement setup (section 2). In section 3 I suggest how these two modes of regulation could be combined. We then discuss the rights of gatekeepers and third parties (section 4), the role of private enforcement (section 5), and the institutional design of the DMA (section 6).

It is worth bearing in mind that the DMA will be accompanied by a procedural regulation, which will likely be similar to that found in antitrust and merger control regulations. Where relevant the paper comments on this, in particular in section 4, and focuses on the procedures once the gatekeeper has been designated.

¹⁴⁶ Regulation 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

¹⁴⁷ Trends and developments are discussed in Monti and de Streel, *Improving EU institutional design to better supervise digital platforms*, (CERRE, 2022).

¹⁴⁸ Regulation 1024/2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions [2013] OJ L287/63.



1. THE SUPERVISORY STRUCTURE OF THE DMA

1.1 Compliance Reports

The DMA sets up a scheme where, after a gatekeeper has been designated, it is expected to comply with the obligations and prohibitions which apply to it and to report how it is complying to the Commission. The reporting obligation is found in Article 11(1). Six months after designation, ‘the gatekeeper shall provide a report describing in a detailed and transparent manner the measures it has implemented to ensure compliance with the obligations’ in Articles 5-7.

This is perhaps the most important aspect of the enforcement architecture because, when read together with Article 8(1) of the DMA, this report is what ensures and demonstrates compliance. The report must, on this reading, not only describe what the gatekeeper plans to do, but also to demonstrate that the compliance effort is ‘effective in achieving the objectives of this Regulation and of the relevant obligation.’¹⁴⁹ This places a heavy burden on the gatekeeper. This is compounded by the objectives of the DMA being open-ended, as was observed in the Compass Paper.¹⁵⁰ For example, when it comes to the obligation in Article 6(3) in terms of which the gatekeeper must ‘technically enable end users to easily un-install any software applications on the operating system of the gatekeeper’, then a compliance report may provide for technical and procedural steps taken in order to comply. The gatekeeper might in addition provide indicators of compliance, for example by regular submission of data about the number of apps that are uninstalled, if this data is easily available, or a report on the number of complaints or requests for assistance to uninstall an app. Gatekeepers will also be expected to explain how some of their contracts with business users have been modified to secure compliance. These contract modifications will also have to be notified to the businesses concerned.

However, given the vital role that the compliance report is expected to play, it is surprising that there are no penalties that are directly associated with Article 11.¹⁵¹ In contrast, when the Commission requests information prior to commencing enforcement, it may impose a fine when the gatekeeper provides incomplete, incorrect or misleading information or explanations.¹⁵² Conversely, the submission of an uninformative report is not sanctioned. Arguably, the Commission is able to issue a request for information, based on Article 21, however this is normally a step used to determine whether to commence infringement proceedings and not designed to stimulate *ex ante* the delivery of comprehensive reports.

There is also no clear procedure to govern what happens when the report is unclear, and how far the Commission may request clarifications at an early submission stage before proceeding to enforcement. Alternatively, the Commission could develop a policy whereby an incomplete report forms the basis for starting non-compliance proceedings.

It would thus be desirable if very early on, the Commission were to issue guidelines on the submission of these compliance reports to facilitate the work of gatekeepers as well as to facilitate the

¹⁴⁹ DMA, Article 8(1).

¹⁵⁰ De Streef, *DMA Compass*, (CERRE, 2022).

¹⁵¹ See DMA Article 30(3) which lists instances where a 1% fine for procedural infringements may be imposed.

¹⁵² DMA, Article 21.



supervisory task of the Commission.¹⁵³ These guidelines should be updated frequently as the Commission gains more experience with the contents of these reports. Moreover, after some years of implementation the Commission could suggest specific metrics and indicators that gatekeepers should have in place to demonstrate compliance. This removes the risk of discretionary assessments of compliance by spelling out what results are expected. Specifying results, rather than just processes of compliance, avoids the risk that compliance is only formal.

It is worth adding that what constitutes compliance may change over time: one would expect fewer consumers to uninstall apps in the short term, but after say five years one could expect a greater supply of apps that compete against the gatekeeper and consumers being more used to switching apps to reveal an increase in the number of users uninstalling apps. However, some caution is necessary. First, if the gatekeeper has complied with the DMA by following the formal or informal guidance offered by the Commission, then if the Commission considers that the market is not sufficiently contestable, no fines should be imposed: the gatekeeper has a reasonable expectation that it has complied. Second, the lack of contestability may not be due to the fact that there could be a more effective way to comply: the gatekeeper might just be offering better quality products. Third, just as what constitutes compliance might change, so does consumer behaviour online: it might be that business users and consumers find alternative routes to connect without necessarily relying on the market-opening requirements of the DMA. Finally, it may be that the reason for the lack of progress is that the DMA contains gaps or is inappropriately drawn, which is a signal that some rethinking of the obligation is necessary. As suggested in the final section, it is important that the Commission evaluates the results of DMA compliance early on to diagnose what changes may be needed.

Observe that a non-confidential summary version of the report must also be published and provided to the Commission. This will be made publicly available on the Commission website and it is likely that gatekeepers will also announce their compliance on their websites for the benefit of business users and consumers. This non-confidential summary version is very useful for third parties; however, its value can only be judged once we see how much detail is retained and how much of it is redacted. Generally, the report should be useful for business users to enter the market. This general principle can serve as a guide to determine if the summary is of satisfactory quality. The report can serve three functions: (i) The business user is able to work out how to engage with the gatekeeper on the new terms; (ii) Suppose the third-party is a client of the gatekeeper and considers that the compliance report reveals that the gatekeeper is in full compliance with the DMA. However, the third-party then observes that in its relations with the gatekeeper it does not do what it says in the report. This creates a clear evidentiary base to challenge the gatekeeper in the national courts; and (iii) Suppose that the third-party does not consider that the report demonstrates effective compliance. Here the third-party may notify the Commission, a national authority or bring legal action. As we discuss in section 4.2, a means of collecting third-party concerns should be designed.

¹⁵³ DMA, Article 46(1) empowers the implementation of an implementing act but a soft law document seems more helpful as it gives the gatekeeper more flexibility.



1.1 Self-assessment

In addition to the report, gatekeepers have to design a ‘compliance function’, a group of employees independent from the operational function of the gatekeeper, with one or more compliance officers.¹⁵⁴ This body monitors the compliance of the gatekeeper. Safeguards are set out to ensure this body is well-resourced, independent, and is able to carry out its functions. The idea behind this body is that it helps design and monitor compliance. It can advise management and employees about compliance so as to prevent breaches of the DMA and assess risks of non-compliance when the gatekeeper changes its policies. Compliance officers will likely play a key role in drafting and assessing the compliance report. It is not clear how costly this will be for gatekeepers and how significant a change it brings to what gatekeepers would have done anyway.

The compliance function serves a second function: it may monitor compliance with commitments and co-operate with the Commission. It is not clear what co-operation means – the compliance function office does not report to the Commission, nor is this body necessarily the most useful source of information when investigatory powers are used. In an investigation, the Commission will wish to obtain details from those responsible for the design or the marketing of the relevant gatekeeper service who will know better how the product functions.

1.2 Co-operative Compliance

When undertakings are faced with obligations in Articles 6 and 7, and are uncertain about how to comply after a self-assessment, they may request help from the Commission, based on Article 8, where two options are available:

1. **Regulatory dialogue** (Article 8(3)): the gatekeeper requests a discussion with the Commission by which it explains the measures it intends to implement, or has implemented, and asks for the Commission’s views.¹⁵⁵ The Commission is not required to engage in this form of dialogue. If the dialogue starts, the gatekeeper has to provide a reasoned submission explaining why the measures it plans or has adopted comply, and a non-confidential version thereof which will be shared with third parties.
2. **Specification decision** (Article 8(2)): the gatekeeper requests the opening of proceedings which may lead to the Commission adopting an implementing act specifying the measures that the gatekeeper must implement to comply effectively. The Commission may also, at its own initiative, open proceedings with a view to issuing a specification decision.

Regrettably, this provision of the DMA suffers from some drafting infelicities in Articles 8(5) and (6). I present the law as set out first, show the problems, and then suggest what was probably intended.

Article 8(5) applies to specification decisions and provides that the Commission is to communicate its preliminary findings to the gatekeeper and the measures it thinks should be taken to comply. Article 8(6) provides that after this the Commission shall publish a non-confidential summary of the case and the measures it considers taking so that third parties may comment. A specification decision then

¹⁵⁴ DMA, Art 28.

¹⁵⁵ This provision was watered down during the legislative process, the sole remaining mention of dialogue is found in DMA, Recital 65.



follows and certain safeguards with respect to the effectiveness of these decisions are found in Articles 8(7) and 8(8). Furthermore, the procedure that led to a specification decision may be reopened upon request (most likely by the parties) or at the Commission's own initiative when there has been a material change in the facts when the decision was based on wrong information, or when the measures specified are not effective.¹⁵⁶

These supplementary provisions only apply to specification decisions and not to the regulatory dialogue. We know how the dialogue starts, but there are no steps for how it may end. This may have been deliberate, with the European Parliament, in particular, preferring quick enforcement rather than risking that gatekeepers stall compliance during the dialogue. However, this seems to misunderstand the provision on dialogue: it is not designed to stop the clock for the gatekeeper. The gatekeeper is expected to comply according to the DMA timetable but may ask for clarification to ensure that it is doing what is required. What is needed are provisions that help explain how the regulatory dialogue is carried out. Perhaps these can be specified in guidelines or implementing acts. My sense is that a procedure analogous to the one for specification decisions should be followed: the non-confidential version of the proposed compliance issued by the gatekeeper can be market tested and third-party feedback can be obtained before the Commission takes a position. Putting third parties first in this procedure indicates that the Commission will then take these reflections into account when offering its informal advice. If the feedback received raises serious concerns, the Commission may initiate a specification decision. In this way, we can also see a way of sequencing these two possibilities for addressing the doubts gatekeepers raise.

However, it is also arguable that having both of these procedures is unnecessary as they appear to duplicate a very similar process by which gatekeeper doubts are clarified. This is discussed further in section 3 below.

1.3 Enhanced Supervision

Article 26(1) gives the Commission powers to take all 'the necessary actions to monitor the effective implementation and compliance with the obligations laid down in Articles 5, 6 and 7 and the decisions taken pursuant to Articles 8, 18, 24, 25 and 29.' My interpretation is that the powers created here only apply when the Commission has made a decision based on the Articles listed here (Article 8 are specification decisions on how the gatekeeper should comply, Article 18 refers to systematic non-compliance, Article 24 refers to interim measures, Article 25 is about commitment decisions, and Article 29 refers to con-compliance decisions).

The necessary actions suggested in Article 26 are that the gatekeeper must retain all documents necessary to assess compliance and that the Commission may appoint an independent external expert and auditor, as well as officials from national competition authorities (NCAs) to help the Commission monitor the obligations. These powers are specified because without these the Commission would

¹⁵⁶ DMA, Art 9(9).



not be able to appoint an external expert.¹⁵⁷ It is not clear who bears the costs of the work of the independent external expert.

It is also not clear what additional monitoring steps may be identified, but the Commission would have to prove that any added burden is necessary to secure compliance. The Commission would thus have to prove that there is no less restrictive alternative to monitor compliance. If we apply this to the power to appoint an external expert, the Commission would have to prove that the compliance reports and the compliance officer do not provide effective safeguards to secure compliance. It may also have to prove that private litigation would be insufficient to deter the gatekeeper from infringing the DMA. In other words, it seems that the barrier to adopting enhanced supervisory mechanisms is high. It may be easier to secure these in cases of recidivism or systematic non-compliance.

1.4 Detection

Given the obligation in Article 11 which requires a compliance report, this will likely be the first evidentiary base used by the Commission to enforce the DMA.

Other possible sources of information could be whistle-blowers who are protected by provisions of EU Law,¹⁵⁸ or third parties who complain about the measures described in the report or about the conduct of gatekeepers.¹⁵⁹ Third parties may be business users, competitors or end-users. They may inform national authorities or the Commission. The option of informing NCAs is probably there for small and medium enterprises (SMEs) or consumers who may feel more confident informing a national authority and writing in their native language.

However, neither national authorities nor the Commission have any obligation to follow up on the information. There is good reason for this: the experience in antitrust where the Commission has to motivate the decision not to pursue a complaint involves resources and is at times subjected to appeals to the General Court. The legislator clearly intended to avoid these costs.

1.5 The Challenges of Gatekeeper Supervision

This new way of securing compliance is designed to place the burden of showing compliance on the gatekeeper and to allow the Commission to observe the degree of compliance. This does not come without risks. The compliance reports have to be sufficiently transparent to avoid circumvention strategies being missed, and there should be processes by which third parties are able to bring concerns to the attention of the Commission at all stages of the procedure.

Transparency of the process is also essential to ensure that this is legitimate: the Commission for example could have a central repository containing all specification decisions. The Commission can also consult other bodies, for example, the EU platform observatory to secure additional information

¹⁵⁷ *Microsoft v Commission* Case T-201/04, EU:T:2007:289, paras 1251-1279.

¹⁵⁸ Article 43 and Article 51, amending Directive 2019/1937 on the protection of persons who report breaches of Union law [2019] OJ L305/17.

¹⁵⁹ DMA, Article 27.



about the market. The process of supervision is necessarily a process of learning how the market and technology function and of keeping up with developments. Supervision is a dynamic exercise.

There is also a capacity challenge: while much of the evidentiary burden is placed on gatekeepers, there is a risk that supervision of all gatekeeper obligations is impossible. Here, the Commission will have to identify criteria for priorities. Capacity challenges also mean that there is a risk that gatekeepers may offer ineffective remedies, considering that there is a chance their conduct may not be scrutinised. As we discuss in section 6, some assistance may be obtained from national competition authorities.

Third parties can add useful information, but there is also a risk that third parties are not entirely representative of business users and so their comments should be assessed carefully, requiring evidence from them to substantiate their concerns.¹⁶⁰ This obviously adds to the burden of the Commission. Here a useful step has been taken by the German government, seeking to elicit information from a variety of parties.¹⁶¹ National authorities could serve as a place where complaints and concerns are filtered. Arguably the European Competition Network can be a site where NCAs can discuss best practices in receiving third-party notifications under the DMA: systematic evidence collection can help enforcement.

¹⁶⁰ C. Goujard, 'Big Tech accused of shady lobbying in EU Parliament', Politico, 14 October 2022.

¹⁶¹ Start of the Digital Markets Act: Economic Affairs Ministry launches consultation on experience with digital platforms, Press Release, (13/10/2022).



2. ENFORCEMENT

In order to reach a decision that the parties are not in compliance, impose a fine, or issue a specification decision under Article 8 (discussed in section 1 above), the Commission shall adopt a decision opening proceeding.¹⁶² However, it may use the investigative powers described below before opening proceedings.

2.1 Investigative Powers

First, the Commission may request information from the gatekeeper, including access to data, algorithms, and information about testing, and it may request explanations about these items.¹⁶³ Second, the Commission may carry out interviews and take statements. It may interview gatekeepers but it is also empowered to interview others.¹⁶⁴ Importantly, it seems that any report of interviews with third parties needs to be made available to the gatekeeper as this may contain exculpatory evidence.¹⁶⁵ This requirement might well deter some complainants from accepting an interview. Third, the Commission is empowered to carry out inspections of an undertaking.¹⁶⁶ This power is similar to that found in antitrust, but with specifications about the importance of digital evidence, thus inspectors are empowered to have access to and explanations of the undertaking's 'organisation, functioning, IT system, algorithms, data-handling and business practices and to record or document the explanations given by any technical means.'¹⁶⁷

In antitrust, the exercise of these powers has been reviewed by the Court of Justice which has specified how these powers may be exercised, while respecting the fundamental rights of those under investigation, such as the right to silence. It seems that the case-law in antitrust can serve as a guide on how to ensure that these powers are exercised in a manner consistent with the gatekeeper's fundamental rights. In addition to secondary legislation, perhaps a Manual of DMA procedures/best practices could be written up and modelled on a similar manual for the application of EU competition law.

2.2 Interim Measures

Interim measures may be adopted by implementing an act in case there is a risk of serious and irreparable damage for business users or end users of gatekeepers. If we look at the experience of the Commission in using interim measures in antitrust, three points stand out:

¹⁶² DMA, Article 20(1).

¹⁶³ Article 21(1). This may be by simple request or by decision. Under the latter, the party is subjected to periodic penalty payments for delay. Fines accrue for the supply of incomplete, incorrect or misleading information or explanations.

¹⁶⁴ DMA, Article 22.

¹⁶⁵ *Intel v Commission*, C-413/14 P, EU:C:2017:632, paras. 79-107.

¹⁶⁶ DMA, Art 23.

¹⁶⁷ DMA, Art 23(2)(d).



- They have been used very infrequently although it has been argued that this is a policy choice and not mandated by the restrictive test which has to be satisfied ('risk of serious and irreparable damage'),¹⁶⁸
- When they are applied, the remedy is specified with a greater degree of precision than in final decisions. This virtue should be retained but it may prove damaging to the gatekeeper if the method of compliance required ends up being more extensive than that which is necessary. Perhaps the gatekeeper can (as in non-compliance decisions discussed below) be asked to formulate a compliance report, however, this might risk delaying the imposition of interim measures; and
- A number of cases end once interim measures are implemented, suggesting that this intervention is sufficient to secure compliance. However, in antitrust law, there is no follow-up and it would be desirable that under the DMA, when an interim order is not followed-up with a decision, the gatekeeper, in revising the compliance report, refers to the procedures that led to the interim measures and shows how these have been integrated into its compliance.

2.3 Non-compliance Decision

If the gatekeeper does not comply with one or more of the following, a non-compliance decision will be issued: (a) the obligations in Articles 5, 6 and 7; (b) specification decisions; (c) systematic non-compliance (d) interim measures; (e) breaches of commitments that are made legally binding.

There is no deadline for reaching this decision but the Commission should endeavour to adopt a decision within 12 months of the opening of proceedings under Article 20.¹⁶⁹ Given the complexity of some of the issues, this may appear overly optimistic, but recall that there may have been many contacts between the Commission and the gatekeeper before the commencement of proceedings. Before adopting a non-compliance decision, the Commission is obliged to communicate its preliminary findings to the gatekeeper and explain the measures it intends to take or expects the gatekeeper to take.¹⁷⁰

There are two other parties who are **consulted**: the decision must be submitted to the comitology committee for an opinion (discussed below in section 5), and the Commission may consult third parties.¹⁷¹ Consultation of third parties is discussed in section 4 below.

A non-compliance decision contains a prohibition and a deadline for the gatekeeper to provide explanations on how it plans to comply. The gatekeeper is required to provide the Commission with a description of the measures that it has taken to comply.¹⁷² This is very important when compared with antitrust law where decisions normally do not specify remedies. Observe how the burden for designing the remedy falls on the gatekeeper. There are two aspects of this procedure that are missing. The first is the option to market test the remedies proposed by the parties. It is not clear why

¹⁶⁸ Ruiz (2020)

¹⁶⁹ DMA, Art 29(2).

¹⁷⁰ DMA, Article 29(3).

¹⁷¹ DMA, Article 29(4).

¹⁷² DMA, Article 29(5) and (6).



this is not available here when it is for commitment decisions. The second is that it is not clear what happens if the measures proposed by the gatekeeper are not in compliance. One answer might be that if the Commission is dissatisfied, it commences infringement proceedings again with a view to issuing a second non-infringement decision. This does not seem to be an efficient way of securing compliance. The alternative is to negotiate with the parties to obtain an amendment to the measures proposed. The weakness of this is the absence of transparency in the bargaining process.

2.4 Fines

There are three instances when a fine may be imposed.

- For non-compliance decisions, the maximum fine is 10% of worldwide turnover in the year before the finding that the gatekeeper, whether intentionally or negligently fails to comply with: (a) obligations in Art 5, 6 and 7; (b) specification decisions; (c) systematic non-compliance (d) interim measures; (e) breaches of commitments that are made legally binding.¹⁷³
- The Commission may impose a fine of up to 20% of turnover if the gatekeeper has committed the same or similar infringement of an obligation in arts 5, 6 and 7 in relation to the same core platform where a non-compliance decision was already adopted in the previous 8 years.¹⁷⁴ The thinking here is to penalise recidivism.
- Fines of 1% of turnover apply for breaches of procedural obligations.¹⁷⁵

Fines for substantive infringements are based on the gravity, duration and recurrence. In antitrust, the Commission issued Guidelines to increase the transparency of its fining policy.¹⁷⁶ It is recommended that a similar guideline should be introduced here. The antitrust guidelines include provisions allowing fines to be increased for aggravating factors and reduced for mitigating factors. This may also be something to consider under the DMA: a gatekeeper who selectively infringes its obligation vis-à-vis undertakings who are likely to steal its market share while treating others in a manner which complies with the DMA may reveal greater exclusionary risk, while a gatekeeper whose compliance is delayed by technical factors might escape with a reduced penalty.

The implication of imposing large fines is that it turns the DMA into a ‘criminal law’ for the purposes of the European Convention of Human Rights. This means not only that the Commission must respect the fundamental rights of the undertakings it investigates, but also that judicial review must be carried out by a court with full jurisdiction. It means that the General Court is required to scrutinize infringement decisions very attentively. If we go by recent reviews of decisions under Article 102 TFEU and mergers, this means that every item of evidence will be subjected to close review. One drawback of the current case-law is that by providing extremely detailed assessment of every piece there is a risk that the General Court loses sight of the bigger picture.

¹⁷³ DMA, Article 30(1).

¹⁷⁴ DMA, Article 30(2).

¹⁷⁵ DMA, Article 30(3).

¹⁷⁶ Commission Guidelines of 28 June 2006 on the method of setting fines imposed pursuant to Article 23(2a) of Regulation 1/2003, O.J. [2006] C 210/5



2.5 Judicial Review

Decisions will be reviewed by the General Court on issues of fact and law and by the Court of Justice on points of law. Decisions may only be upheld or quashed (in whole or in part). Fines may be modified.¹⁷⁷

In contrast to antitrust law, where the Court is asked to become an economic expert, the form-based approach to obligations and prohibitions means that the Court will be tasked with interpreting provisions that are ambivalent. The Court may need to gain expertise in technology to be able to understand the possible impact of its interpretation of given provisions. On this point, it may well be that the Court adopts a rather deferential approach to the approach taken by the Commission.

2.6 Implementing Acts and Guidelines

The Commission is empowered to clarify aspects of the DMA in two ways: (i) by implementing acts for a discrete set of issues; (ii) by writing guidelines on any aspect of the DMA.¹⁷⁸ In antitrust law, where guidelines prevail, there is now a well-established process by which guidelines are issued for public consultation before they are finalised. This practice should be replicated here. For implementing acts, public consultation is provided expressly in the DMA.¹⁷⁹

Guidelines or implementing acts on procedure are likely to be more helpful in the short term, while explanations on how one might comply with Article 6 obligations may be more effective if they based on Commission experience of handling some cases. Of particular importance, guidelines explaining what is expected in the compliance reports appear necessary. Guidelines might also be useful with respect to Article 7 obligations, which were inserted late in the proceedings and where the legislative intent is not as clear.

¹⁷⁷ DMA, Art 45.

¹⁷⁸ DMA, Articles 46 and 47.

¹⁷⁹ DMA, Art 46(3)



3. RESPONSIVE REGULATION

In sections 1 and 2 I have tried to explain how each section of the DMA can be expected to operate and the problematic issues that may arise. Here I adopt a different approach and suggest how the various procedures set up to secure compliance might be sequenced by the Commission in a manner that ensures they are used effectively.

In earlier work I drew on the theory of responsive regulation by Ayres and Braithwaite to suggest that the DMA should be designed with the assumption that the gatekeepers wish to comply and that the regulator should stimulate compliance with third-party input in the first instance. The regulator however should be responsive to the actions of the gatekeeper and either facilitate compliance if the gatekeeper wishes to comply or have a big stick of increasingly punitive sanctions to secure compliance. This is often portrayed as a pyramid of enforcement as most should occur at the base and there should be little use of the strictest sanctions for example – this pyramid is drawn with reference to inspections of care homes.¹⁸⁰

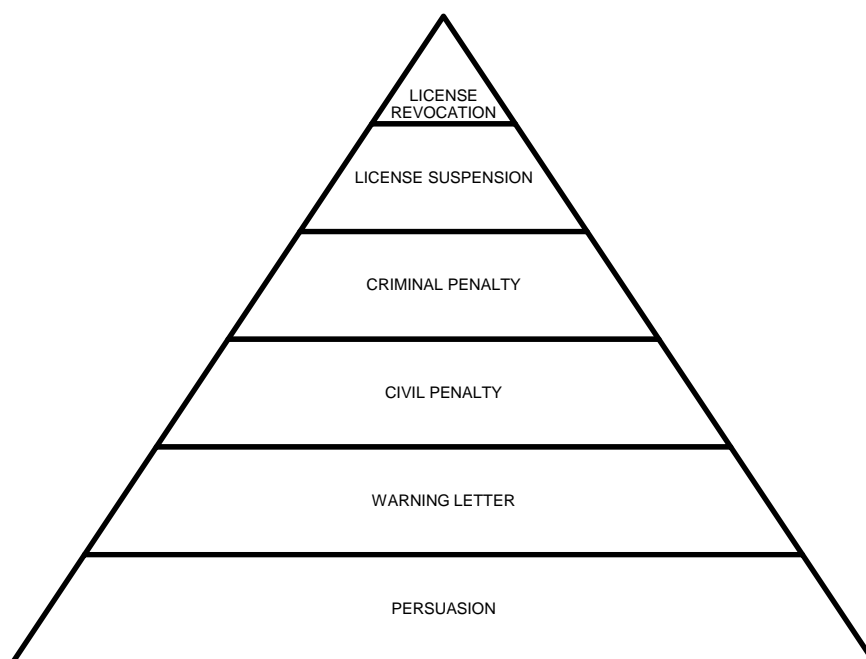


Figure 1: Ayres and Braithwaite's enforcement pyramid.¹⁸¹

At the foot of the pyramid is the most often used remedy: observing that the regulated entity is non-compliant, the regulator nudges compliance by persuading them to do so. If this does not work, then the regulator issues a formal warning, and if this does not work then penalties are escalated until the draconian step of removing the actor from the market is taken. The idea behind this framework is that the regulator and regulated entity are interacting repeatedly so that the regulator can respond to the signals it gets from the regulated entity: if persuasion works, then the regulator does not need to escalate. If it does not, then the regulator can respond to non-compliance. The system is flexible in

¹⁸⁰ I. Ayres and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992)

¹⁸¹ *Ibid.*, p.36



that if the regulator moves up the pyramid and imposes penalties which make the regulated entity more willing to comply, then the regulator can go back to a strategy of persuasion.

The DMA does not follow this approach completely but if we break down the various supervision and enforcement approaches, we have the following stages:

- **Stage 1: Oversight and persuasion**

First, parties decide how to comply and create a mechanism for monitoring compliance, based on Articles 8 and 11. Concomitantly, parties make their compliance transparent so that the regulator national authorities and third parties can see what is being done.

Second, signals from third parties and the Commission can identify gaps and the Commission can send observations to the gatekeeper who can remedy these without further action. To complete this, what is missing in the DMA is a structured process for assessing compliance reports. How can the Commission persuade a gatekeeper to comply? It is expected that there will be informal contacts between the Commission and gatekeepers, but as noted in section 2 above the precise form of the regulatory dialogue is not clear. Indeed, the process of persuasion seems to rely on the gatekeeper approach the Commission with a request for a dialogue.

- **Stage 2: Non-compliance**

The Commission can intervene if it has concerns about compliance and this is gradual: it can issue a specification decision (2A), or it can elect to be more aggressive and issue a non-compliance decision (2B), or even more aggressive and impose fines (2C). Stage 2 is designed to ramp enforcement up the pyramid and deter non-compliance. Note that a non-compliance decision exposes the gatekeeper to follow-on damages actions. In all these steps the role of third parties is vital: it is well-set up for specification decisions and there should be similar types of market tests when a non-compliance decision is issued.

- **Stage 3: Systemic non-compliance**

The top of the enforcement pyramid is systematic non-compliance which allows for a wide range of remedies, including structural ones (stage 3B). However, the party can de-escalate by offering commitments to avoid the most powerful of sanctions (stage 3A). This makes good sense because it maps onto the expectation of a responsive regulator: to de-escalate once the gatekeeper is willing to comply with a less intense means of enforcement.

Reproducing this onto the enforcement pyramid, we see that the model is not reproduced fully but the gist of that approach is present.

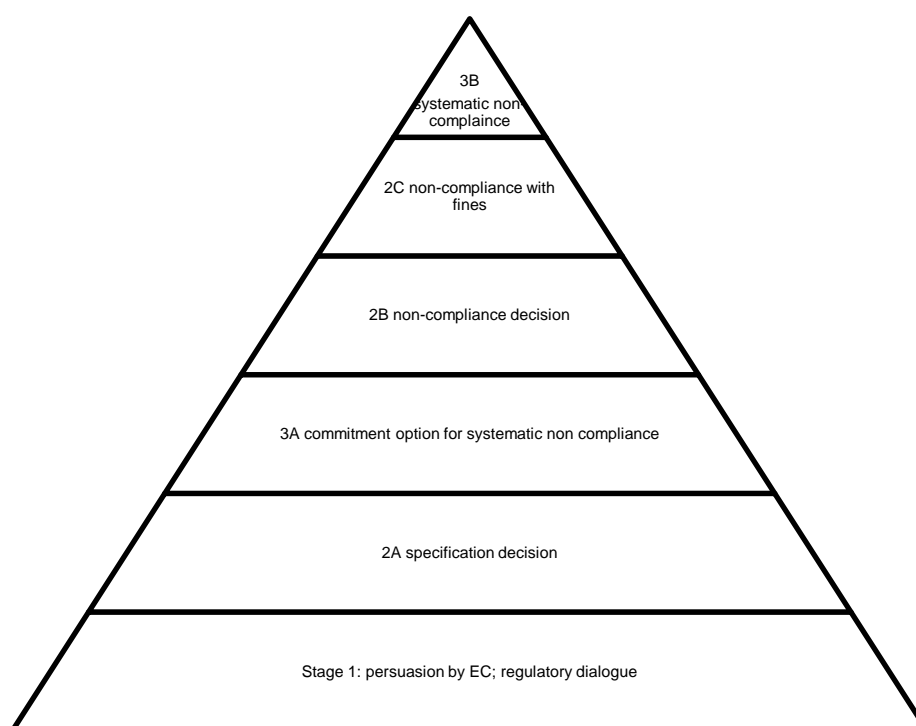


Figure 2: the enforcement pyramid applied to the DMA

The DMA does not replicate the responsive regulation model entirely but in between the Commission proposal and the final version, the legislator has made the system more streamlined such that this approach to regulation is possible. This has advantages for gatekeepers who are able to participate in shaping their compliance, for the Commission in that negotiation is less costly and possibly more productive than litigation, as well as for third parties. Of course, this form of regulation raises some concerns, not least if the procedures at the bottom of the pyramid are not sufficiently transparent (especially as note the regulatory dialogue) and the absence of judicial review may raise concerns that the Commission can persuade firms to over-comply.

For completeness, the DMA does not require the Commission to adopt this enforcement strategy. The Commission is free to move directly to apply punitive measures if it so wishes: the DMA does not have a hierarchy of remedies. However, the recommendation here is that exploring the potential of this enforcement model is worthwhile because it avoids lengthy litigation and allows for a closer engagement with gatekeepers.



4. RIGHTS AND INTERESTS

4.1 Fundamental Rights of Gatekeepers

When it comes to initiating formal procedures, the **DMA has to guarantee the respect of fundamental rights**. These are noted in two recitals:

- Recital 80: In order to ensure effective implementation and compliance with this Regulation, the Commission should have strong investigative and enforcement powers, to allow it to investigate, enforce and monitor the rules laid down in this Regulation, while at the same time ensuring the respect for the fundamental right to be heard and to have access to the file in the context of the enforcement proceedings. ...
- Recital 109: This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular Articles 16, 47 and 50 thereof. Accordingly, the interpretation and application of this Regulation should respect those rights and principles.

Article 16 is the right to conduct a business, Article 47 is the right to a fair trial, and Article 50 is the right not to be punished twice for the same offence. But there are plenty of other rights that are relevant, e.g. the right to good administration found in Article 41. There is no doubt that the Commission seeks to respect the fundamental rights of the parties but as the scope of these rights is often unclear, it is preferable if some are spelled out by way of a procedural regulation, and often their scope is only made clear by the Court of Justice. If we draw from the one applicable in antitrust (Regulation 773/2004),¹⁸² **a few preliminary issues emerge which could be codified** using Article 46 of the DMA which empowers the Commission to issue implementing acts.

- Procedures regulating the power to take statements and oral questions during inspections;
- The right to be heard, set out in Article 34 DMA, which applies to: specification decisions (Article 8), suspension decisions (Article 9), exemptions (Article 10), market investigations (Articles 17, 18), interim measures (Article 24), commitments (Art 25), non-compliance decisions (Art 29) and fines (Art 30 and Article 31(2)). Here procedures for written submissions and oral hearings should be established;
- Access to the Commission's file by the gatekeeper

4.2 Third Parties

By third parties we mean anyone who is not the gatekeeper. The question we look at first is the degree to which the DMA facilitates the participation of third parties, and compare this with antitrust.¹⁸³ We then discuss whether additional third-party rights may be warranted.

¹⁸² Commission Regulation 773/2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty [2004] OJ L123/18.

¹⁸³ Wils (2022) for a comprehensive discussion of EU antitrust.



- **Third-party as informer**

Third parties may inform the Commission of a suspected infringement of the DMA. In antitrust, third parties may ask for anonymity, and a whistleblower tool is set up as well, which also guarantees anonymity. There seems to be nothing to prevent a similar mechanism being established under the DMA and it would be desirable if they were made available. Some businesses who rely on platforms may be unwilling to complain without these guarantees.¹⁸⁴ . A practical issue to consider for informants is that they should advise the Commission if their identity may be inferred from the evidence they submit. If yes, then the Commission has to be cautious about sending this evidence to the gatekeeper and may need to redact it.

As discussed earlier, the Commission has no duty to respond (see section 1.5 above) and the status of complainant who is entitled to a reasoned rejection of its complaint, does not exist in the DMA. This saves resources but on the other hand, the duty to give reasons for rejection makes the Commission more accountable and it can then show that its decision to take up a particular complaint is not based on inappropriate factors.

- **Third-party during the proceedings**

In antitrust law, if a party takes advantage of the procedures to become a complainant, then they are entitled to be closely associated with the proceedings.¹⁸⁵ This means they are entitled to receive a copy of a non-confidential version of the statement of objections and they may be allowed to participate in oral hearings. However, they do not have access to the Commission's file and their rights are generally less extensive than those of the addressee of the statement of objections. No comparable entitlement appears to exist for the DMA.

In antitrust the Commission powers to send requests for information extends to third parties and the same powers exist in the DMA (Arts 21, 22 and 23, discussed above).

- **Third parties and the market test**

During a specification decision, third parties may comment on the measures that it proposes to take (Art 8(6)) as well as during a commitment decision (Art 18(6)).

- **Additional role for third parties?**

Third parties on both sides of the market (business users and end users) can add value to the assessment of the compliance path selected by the gatekeeper. It may well be that the gatekeeper will test various setups to see how users respond. Thus, the views of third parties could be obtained by the gatekeeper and use as evidence of the effectiveness of the remedy. For example, when implementing a choice screen the gatekeeper can demonstrate compliance by providing evidence of various choice screens that were tested and explaining that it has chosen the one which makes switching easiest for users.

¹⁸⁴ Report from the Commission of 5 July 2010, Retail market monitoring report, "Towards more efficient and fairer retail services in the internal market for 2020" COM (2010) 355, p.7. And see A. Renda et al, Legal framework covering business-to-business unfair trading practices in the retail supply chain, Study for the European Commission (2014).

¹⁸⁵ Regulation 1/2003, Art 27(1).



The role of third parties when the Commission is involved might be enhanced. In discussing the suggestions below, one should consider the importance to balance the value of third-party views on the one hand and effective enforcement on the other.

- As mentioned above there should be a stage where the compliance reports are reviewed and minor changes suggested, which do not require any of the formal procedures. Third-party involvement here can be helpful in giving a first impression on the measures adopted and the Commission may receive signals of where there may be risks.
- While third-party notifications do not require the Commission to intervene, guidelines might be issued to indicate the kinds of notifications that the Commission would welcome and perhaps even some criteria by which these notifications are assessed. Third parties must substantiate their complaint and guidance may be offered on what is expected. One additional idea might be that multiple notifications of the same conduct by the same gatekeeper could trigger the Commission into action. Another is that if a notification points to an issue that the parties can resolve bilaterally in court then this indicates that the case is not for the Commission.
- The DMA involves third parties during a specification decision but their input only occurs once, when the Commission has decided on a possible course of action. It may be uneconomical to ask for input before as well but on the other hand there may be advantages to understanding what users need before designing the remedy.
- The provisions for regulatory dialogue in Article 8(3) are under-specified but since the gatekeeper is asked to provide a non-confidential version of the submission, there should be a process by which this can be commented upon by third parties before the Commission communicates its views.¹⁸⁶
- Third-party consultation in case of an infringement decision seems to occur before the decision. However, given that the parties subject to the non-compliance decision have to then design a remedy, one could include a market test following this stage.¹⁸⁷
- If guidelines are to be issued, then consultation with third parties is necessary.

More generally, what third parties will be most able to comment on is the degree to which the remedy succeeds in making the market more contestable and fair. One aspect of the DMA is that we may not know on day one what the appropriate compliance path is – it may be a matter of trial and error. (In antitrust, we have seen this happen in the implementation of Microsoft’s interoperability remedy, Google Shopping and Google Android.) This has two implications: it might be that at the beginning the Commission is relatively lenient when assessing gatekeeper compliance provided the gatekeeper has done its best to comply. However in the longer run, the gatekeeper can be expected to continue to ensure that its measures satisfy the aims of the DMA. The second implication is that in this process of trying to identify the most effective approach, third parties can be involved as those who can inform the Commission and gatekeepers about what may be improved in the current compliance measures. This goes back to the point made in section 1 where it is argued that a combined reading of Articles 11 and 8 suggests that the gatekeeper’s compliance report should serve to demonstrate compliance.

¹⁸⁶ See Art 46(1)(d).

¹⁸⁷ See Art 46(1)(i).



Some concerns may arise (as discussed in section 1) about whether third parties who are business users are sufficiently representative and if they are likely to be biased in their feedback. This can be countered by consulting other sources: privacy and security experts for example can offer valuable feedback on specific technical issues.

Finally, outside of an enforcement paradigm, consultations with third parties about their business models and their relations with gatekeepers can add a source of information. Some have expressed the view that the workshops organised in order to explore how to implement the P2B Regulation were helpful and it appears that similar workshops will be organised to facilitate a better understanding of the DMA.¹⁸⁸ Concomitantly, discussions with gatekeepers can serve the same function. Related to this, it will be helpful to trace the effectiveness of the remedies imposed by the Commission or the compliance measures adopted – the Commission should be learning from the regulatory efforts and this is where third-party input can also be helpful.

¹⁸⁸ https://competition-policy.ec.europa.eu/dma/dma-stakeholders-workshop_en



5. PRIVATE ENFORCEMENT

It is clear that courts and arbitrators may be involved in policing the DMA. Indeed, consumers will be able to launch representative actions in those jurisdictions that provide for this.¹⁸⁹ Before discussing this, it is worth bearing in mind that gatekeepers may design their in-house complaints-management system, in particular in respect of business users. This is already required by the Platform to Business Regulation.¹⁹⁰ The DMA's internal compliance mechanism can be added to this. This can serve to avoid costly litigation and is foreseen in Article 5(6) of the DMA.¹⁹¹

Turning to private enforcement, a leading scholar has indicated that 'As for Articles 5 and 6, there is no doubt that these are sufficiently unconditional and precise and therefore can be invoked before the national courts by individuals that base rights on them.'¹⁹² As he observes the fact that Article 6 obligations may be further specified is irrelevant to assess their direct effect: a specification merely explains how to comply, it does not change the core nature of the obligation. However, specification decisions are relevant in two ways: first, if there is a specification decision and the gatekeeper has acted in compliance with it, the national court should take this into consideration and may not contradict those decisions. Second, if there is no specification decision, the gatekeeper subject to litigation may try and engage the Commission to start proceedings. If this happens, the national court should stay proceedings pending a decision by the Commission, so as not to impose remedies that are incompatible. However, note that there is nothing in the DMA which can constrain a national court in finding an infringement when the Commission considers there has been compliance but has not stated so expressly. The one limitation is the duty that every actor has (including a national court) to co-operate loyally with other institutions applying EU Law found in Article 4(3) TEU. This means that the national court cannot impose remedies that would make the DMA work ineffectively.

To avoid the risk of divergent or aberrant national judgements the DMA contains provisions on co-operation between national courts and the Commission which largely replicate those found in antitrust law. A brief summary and some comments follow based on the experience in antitrust.¹⁹³

- National courts may ask the Commission for information and ask it questions. It is not clear how often this takes place in antitrust.
- Member States shall forward a copy of any judgment applying the DMA. This has not worked in antitrust, with no coherent collection at national level. It is not clear how this can be resolved.
- The Commission may submit written observations to a national court where required to ensure the coherent application of this regulation and may request that the national court transmits information to it. Nearly every time this opinion was submitted in antitrust, the court made a reference for a preliminary ruling to the Court. The reason in my view is rather

¹⁸⁹ DMA, Articles 42 and 52 which amends Directive 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1.

¹⁹⁰ Regulation on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57, Articles 11 and 12.

¹⁹¹ CERRE, DMA Recommendations for the Council and the Parliament, April 2021, p. 72, Draft BEREC Report on the ex ante regulation of digital gatekeepers, BoR (21) 34, 11 March, 2021, Annex II.

¹⁹² A Komninos, The Digital Markets Act and Private Enforcement: Proposals for an Optimal System of Enforcement Eleanor M. Fox *Liber Amicorum, Antitrust Ambassador to the World* (Concurrences, 2021)

¹⁹³ DMA, Article 39.



obvious: courts are much more comfortable receiving an authoritative answer from the Court than a non-binding opinion from the Commission.

- Finally, and most importantly, the national court may not give a judgment that runs counter to a decision adopted or contemplated by the Commission. This means that the national court is expected to stay proceedings pending a decision from the Commission or it may make a request for a preliminary ruling. In antitrust this has not caused any notable problems.

Turning from risk management to remedies, parties using courts can seek damages for lost profits or excess charges and they can ask for injunctions to prevent the gatekeeper from acting in a particular way or mandating the gatekeeper to act in a specific manner. A few remarks here: in antitrust I am not aware of a successful damage claim based on lost profits – even in cartel cases this seems hard to prove and claimants seek restitution of the overcharge. When it comes to injunctions, there may be limits under national law as to how much a judge can do however these limits cannot negate the right which the party is entitled to. Moreover, these remedies might only bind the gatekeeper to act in the way prescribed towards the claimant and not every other user.

- Remedy applies only to benefit the plaintiff: suppose the Commission agrees with a design for Article 6(4): installation and effective use of third-party software applications. Suppose a software provider thinks that the process is not good enough. A court may require that the gatekeeper enable the installation of that third-party software application using a different protocol than that used for all other third-party apps.
- Remedy changes the DMA obligation: a national court finding that there is still self-preferencing contrary to Article 6(5).

Unsurprisingly, there are concerns about fragmentation and a risk that this makes the DMA less effective when there is no Commission decision to constrain national courts. However, as AG Ćapeta has recently remarked, ‘the possible occurrence of divergences is part of the regional integration process, such as is present within the European Union.’¹⁹⁴ She takes the view that this possibility is mitigated by coordination processes. Member States might manage this risk further by requiring that cases which raise the DMA are heard by a specific Court or chamber, as it is of the case for antitrust or economic regulation, which can gain experience. Parties however might not wish to litigate immediately and might favour an approach by which they ‘follow-on’ from a Commission infringement decision. This makes it easier to establish that the gatekeeper had in the past infringed the law.

In my view the most common type of private litigation will be in instances where the business user considers that it is being discriminated against: all other business users have access to the gatekeeper but the gatekeeper treats it differently. If this is uncovered it raises interesting questions about whether compliance is necessarily a one-size fits all or whether the gatekeeper may (or is expected) to deal with users differently to comply with the DMA.

¹⁹⁴ *DB Station & Service AG v ODEG Ostdeutsche Eisenbahn GmbH*, C-721/20, EU:C:2022:288, para 67



6. INSTITUTIONAL DESIGN OF THE DMA

The Commission is the principal actor. As has been made clear the work will be divided between two Directorates-General: DG COMP and DG CNECT, in association with the Legal Service and possibly the JRC European Centre for Algorithmic Transparency.¹⁹⁵ Decisions will be reached by the College of Commissioners with some delegation possibilities. It is clear that the Commission will be under-resourced and a consideration for the future is whether gatekeepers might be asked to pay a supervisory fee, as in the Digital Services Act.¹⁹⁶

6.1 Co-operation with National Authorities

The Commission is expected to co-operate with national authorities. The DMA distinguishes two types of authorities: national competent authorities enforcing the competition rules set out in Art 1(6) who are also expected to be responsible for the DMA (i.e. the national competition authority), and other authorities such as the national consumer protection authority, the data protection agency or the telecom regulator. A very detailed provision is made for co-operation with national competition authorities, while for other national bodies the DMA merely requires that the two actors coordinate their enforcement actions to ensure coherent, effective and complementary enforcement. For example, the Commission could coordinate with the agency in charge of the P2B fairness regulation or with the data protection agency where the gatekeeper is established and examine how far the gatekeeper can comply with the two rules most effectively. In these contexts, the agencies may not exchange confidential information.¹⁹⁷ Parties may waive confidentiality if this helps to ensure a coherent regulatory response. In mergers that are notified in multiple jurisdictions, confidentiality waivers are common to facilitate a quick resolution and coordinated remedies

As mentioned, the provisions for co-operation with national competition authorities are much more detailed and extensive.

First, there are provisions to coordinate enforcement of the DMA and competition law. There is a duty to keep each other informed of enforcement actions and confidential information may be sent to another authority. More specifically: (i) when an NCA intends to launch an investigation on one or more gatekeepers based on national law, the Commission is to be informed and the NCA may also inform other NCAs; (ii) when an NCA intends to impose obligations on gatekeepers based on national law it shall communicate the draft measure to the Commission, even when these are interim measures. Information shared may only be used to coordinate enforcement.¹⁹⁸

But what does coordination in these cases mean? The DMA is silent on this. We may expect that the Commission might provide informal advice to the NCA on the application of national laws. The only

¹⁹⁵ https://algorithmic-transparency.ec.europa.eu/index_en

¹⁹⁶ This in turn draws on the approach followed by ESMA, see e.g. Commission Delegated Regulation 272/2012 with regard to fees charged by the European Securities and Markets Authority to credit rating agencies [2012] OJ L90/6.

¹⁹⁷ Article 339 TFEU, 'The members of the institutions of the Union, the members of committees, and the officials and other servants of the Union shall be required, even after their duties have ceased, not to disclose information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components.' In the antitrust context, see Regulation 1.2003, Article 12 which limits the exchange of confidential information. This was discussed in *Dirección General de Defensa de la Competencia v Asociación Española de Banca Privada and others*, Case C-67/91, EU:C:1992:330.

¹⁹⁸ DMA, Article 38 (1), (2), (3), (5).



mechanism for the Commission to stop an NCA is by starting its own proceedings: once the Commission opens proceedings on the basis of Article 20, the NCAs cannot continue or start an investigation and are expected to report their findings to the Commission.¹⁹⁹ If we compare this to antitrust, there seem to have been some episodes where the Commission has taken over a case started by an NCA, but it is not clear if this was a pre-emptive strike to prevent an NCA from taking a divergent decision.²⁰⁰

The benefit of this procedure is that it tries to avoid the imposition of inconsistent regulatory requirements by NCAs, however we might see some bold NCAs eager to impose additional obligations on gatekeepers by applying national competition law.

There is a second co-operation pathway which relates to the enforcement of the DMA and engages the national competition authority, when this is not acting under its competition law powers, in particular: (i) the Commission may ask that authority to support a market investigation;²⁰¹ (ii) a national competent authority may conduct an investigation into possible non-compliance with Articles 5, 6 and 7 of the DMA.²⁰²

It will be recalled that during the negotiations, some Member States wanted to secure a more significant role for national authorities.²⁰³ Arguably, their marginalization makes sense because national authorities have no powers to impose remedies extraterritorially and this is a matter for national law, so conferring them enforcement powers under the DMA would have risked that each gatekeeper receives different obligations. However, the compromise in the DMA is unhelpful: it is not clear how one may incentivise a national competent authority to commence a non-compliance investigation if it cannot then get any credit for a decision. Given that NCAs are accountable to Parliament based often on the value for money, it would be bizarre to explain that it is acting to facilitate the enforcement of the DMA by the Commission. Nevertheless, in the current proposal for amending the German competition legislation, provisions are made to empower the Bundeskartellamt to carry out its own investigation into infringements of Articles 5, 6 and 7 of the DMA and for co-operation with the Commission.²⁰⁴ The incentive for this step is that the national authority can then contribute to shaping the DMA. The advantage is that this can strengthen the resources available to apply the rules. However, it will be important that if the Commission opts for a responsive approach to regulation that this is not thwarted by NCAs beginning investigations when the Commission sees the option of resolving concerns informally.

¹⁹⁹ DMA, Article 38(7), second sentence.

²⁰⁰ e.g. ebooks was started by the OFT before it moved to the Commission. A laconic press release by the OFT indicated that the case was no longer an enforcement priority because the Commission was well-placed to act (Office of Fair Trading (OFT) closed Competition Act 1998 case, 1 December 2011). The Spanish competition authority stopped its proceedings against Aspen when the Commission decided to investigate concerns about excessive pricing.

²⁰¹ DMA Art 16(5)

²⁰² DMA, Article 38(6) and (7).

²⁰³ Friends of an effective Digital Markets Act, *Strengthening the Digital Markets Act and Its Enforcement* (the friends are France, Germany and the Netherlands). The non-paper is available at: https://www.bmwk.de/Redaktion/DE/Downloads/M-O/non-paper-friends-of-an-effective-digital-markets-act.pdf?__blob=publicationFile&v=4, European Competition Network, Joint paper of the heads of the national competition authorities of the European Union: How national competition agencies can strengthen the DMA (2021).

²⁰⁴ Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz, Entwurf eines Gesetzes zur Verbesserung der Wettbewerbsstrukturen und zur Abschöpfung von Vorteilen aus Wettbewerbsverstößen (15 September 2022).



6.2 EU-level Co-operation

There are two other bodies: an innovative high-level group and a standard comitology committee.

The one with the most potential is the high-level group for the DMA.²⁰⁵ which is composed of representatives from the Body of the European Regulators for Electronic Communications, the European Data Protection Supervisor and European Data Protection Board, the European Competition Network, the Consumer Protection Co-operation Network, and the European Regulatory Group of Audio-visual Media Regulators.

The group serves three functions: (i) to offer advice and expertise on the application or enforcement of the DMA; (ii) in market investigations into new services and obligations it may advise on the need for amending, adding or removing rules in the DMA; (iii) to promote a consistent regulatory framework.

All can be helpful but the third is by far the most urgent task since the obligations in the DMA overlap with a number of EU and national rules. The high-level group is expected to identify and assess ‘trans-regulatory issues’ and may recommend how convergence may be achieved. Annual reports on this matter are expected. This high-level group will grapple issues that may take years to be resolved by the Court and it should work actively to address possible tensions that may arise in the application of a variety of rules.

One issue which it could usefully work on is on how to mainstream data protection in the DMA. In other words, to create a process by which remedies imposed under the DMA are tested for their compliance with the data protection rules. We have seen this issue arise in some abuse of dominance cases where the remedy was the making available of personal data, where co-operation between competition and data protection agencies can ensure coherence and similar workflows can be proposed here.

The digital services comitology committee is made up of representatives of Member States.²⁰⁶ The committee plays two roles: as an advisory committee (DMA, Art 50.2) it provides an opinion which the Commission must take the utmost account of, and as an examination committee (DMA, Art 50.3) its opinion is binding, meaning that a negative vote stops the proposed act.

There is already another body, the EU platform observatory who would also provide help provide a helpful source of information.²⁰⁷ What is missing from this list of institutions are processes to carry out ex post analysis of the DMA’s impact and an independent evaluation can help steer enforcement and identify good practices.




²⁰⁵ DMA, Article 40.

²⁰⁶ Regulation 182/2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission’s exercise of implementing powers [2011] OJ L55/13.

²⁰⁷ <https://platformobservatory.eu/>





Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu
 @CERRE_ThinkTank
 Centre on Regulation in Europe (CERRE)
 CERRE Think Tank