cerre Centre on Regulation in Europe

DMA HORIZONTAL AND VERTICAL INTEROPERABILITY OBLIGATIONS

ISSUE PAPER

November 2022

Marc Bourreau

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, ARCOM, Booking.com, Comreg, DuckDuckGo, Google, Mediaset, Meta, Microsoft, Ofcom, Qualcomm, Spotify, TikTok, Vodafone. 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.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

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, to the specification of market rules and to 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

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.

1. 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.

2. HORIZONTAL INTEROPERABILITY

2.1. The Obligation and its Objective

2.1.1. 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)**,[1] 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.[2]

However, the DMA transforms this possibility introduced by the EECC for national regulatory authorities "to impose" interoperability under some conditions,[3] 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").

[1] 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.

[2] 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).

[3] 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.

2.1.2. 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.

2.2. Interpretation and Implementation Issues

2.2.1. 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.[4] 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

[4] 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).

messengers from different suppliers. Therefore, there exists some competition between messaging platforms via multihoming.[5] However, interoperability may substitute for multihoming since it allows users to access all networks at lower costs,[6] possibly with a quality loss.[7] 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.[8] 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.[9] 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.

2.2.2. 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

[5] 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.

[6] 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.

[7] 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.

[8] See also Bourreau, Krämer and Buiten (2022).

[9] See, "Europe's Digital Markets Act Takes a Hammer to Big Tech," Wired, March 2022, https://www.wired.com/story/digital-markets-act-messaging/.

contestability. Therefore, our reading is that messaging users of gatekeepers within the EU must be able to talk to any user in the world. In any case, the geographical scope of the provision has to be clarified.

2.2.3. 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.[10] 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".[11] 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.

[10] 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.

[11] The European Commission can extend this list.

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 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.

2.2.4. 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**.[12] 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,

[12] 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

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:

> *"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.

2.2.5. 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.

3. VERTICAL INTEROPERABILITY

3.1. The Obligation and its Objective

3.1.1. 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).

3.1.2. 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.[13] 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)

3.1.3. 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:

[13] 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.

3.2. Interpretation and Implementation Issues

3.2.1. 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**.

3.2.2. 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.[14] 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.

3.2.3. 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

[14] 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.

and foreclose its competitors in the complementary product and service markets. Such sabotage tactics may be difficult and time-consuming to monitor.

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.

3.2.4. 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.

3.2.5. 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.[15] Finally, it may encourage gatekeepers to adopt non-price 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.

[15] See Bourreau and Krämer (2022) for a more in-depth discussion.

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_ALT_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.

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

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