

Digital Markets Act

Headline Messages

- ***The DMA's scope should be refined to ensure consistency and reflect the focus on gatekeepers.*** The DMA risks being over-inclusive in some respects and under-inclusive in others, and leaves open the possibility for overlapping and conflicting EU and national rules. These issues could be addressed with refinements to the draft. In particular:
 - **Article 1(6)** should be amended to preclude national rules from regulating substantially the same practices as the DMA.
 - **Article 2(2)(g)** should be removed to avoid covering a broad range of non-gatekeeper services that fall within the definition of 'cloud'
 - **Article 3(2)(a)** should be removed or replaced with a service-level turnover threshold to avoid unequal treatment between platforms of the same size and importance simply because of the revenues of their owners.
- ***The framework for the application of the substantive rules should be refined to enable a genuine regulatory dialogue and avoid unintended consequences.*** We welcome the DMA's stated aim to enable a regulatory dialogue with gatekeepers. To enable a genuine regulatory dialogue and avoid unintended harmful consequences, however, the rules on the application of the DMA's substantive provisions require refinement. In particular:
 - The Commission should specify the obligations under Article 6 that a given gatekeeper must implement before these obligations become binding for the gatekeeper and exposing it to fines.
 - Gatekeepers should be given the chance to request an exemption from individual obligation beyond the narrow limits set by Article 8, if they can demonstrate legitimate and proportionate considerations that justify such an exemption.
 - Article 10 should permit the Commission to narrow or remove obligations over time -- not only add to them.

- ***There are several proposals we support.*** The EC’s proposal provides a number of sensible suggestions for types of conduct that are typically harmful and can be identified as such. The following provisions are relevant:
 - **Article 5(b)** rightly proscribes the use of most favoured nation clauses.
 - **Article 5(c)** facilitates developers promoting their offers to end users.
 - **Article 5(d)** ensures that business users can raise concerns with public authorities.
 - **Article 6(1)(c)** promotes users’ choice of apps while ensuring scope for protecting the service’s integrity.
 - **Article 6(1)(e)** ensures that user choice will be free from technical incumbrances.
 - **Article 6(k)** requires fair and non-discriminatory conditions on business users’ access to app stores.

- ***Other proposed rules pursue important objectives but require refinement.*** Some of the behavioral rules would benefit from further clarification and refinement to ensure they are practicable, meet the DMA’s objectives and avoid unintended adverse consequences. These rules include: **Articles 5(g) and 6(1)(g)** (disclosure of performance-related information and prices paid/received by advertisers and publishers), **Article 6(1)(a)** (using business users’ data in competition with them), **Article 6(1)(b)** (uninstalling preloaded apps), **Article 6(1)(d)** (equal treatment in ranking), **Article 6(1)(f)** (interoperability), **Article 6(1)(h)** (data portability), **Article 6(1)(i)** (data generated by business users), and **Article 12** (reporting concentrations).

- ***A small number of proposals would be harmful.*** Certain proposals in the DMA would not improve the contestability of digital markets and carry substantial risks to innovation and the welfare of European businesses and consumers. The following provisions are relevant:
 - **Article 5(a)** addresses user consent for combinations of personal data, which area already regulated by the GDPR. Different parallel rules on the permissible extent of data processing is liable to lead to confusion, uncertainty, and contradictory outcomes.
 - **Article 6(1)(j)** addresses third party access to search data, which is likely to harm innovation and expose search engines to manipulation.

- **Certain additional ideas warrant consideration.** It is worth considering other possible solutions and measures, including a role for choice screens and data mobility systems
 - **Choice screens** can be an effective way to address concerns about behavioural biases, including ‘default’ bias. At present, choice screens are shown only on certain platforms, including Google’s Android operating system. They could be applied to other digital platforms too to increase consumers’ awareness of alternatives and facilitate easier switching among services. Choice screens could be considered as a way to ensure compliance with **Articles 6(1)(c) and 6(1)(e)**.
 - **Data mobility systems** can intensify competition and enhance choice in digital markets just as Open Banking has done in the financial sector. Regulators can build on the Data Transfer Project, which has developed much of the necessary technical infrastructure for technology companies, possibly specifying participation in the Project as a measure to comply with **Article 6(1)(h)**.
- **Rules should have a clear connection to the DMA’s metrics for success.** The DMA claims that its rules will significantly increase GDP, employment, sales, and consumer surplus. Any rules that ultimately become part of the GDP should have a clear connection to achieving these goals.

* * *

A. Scope

Article 2: Definitions

Article 2(2) Core platform services

“Core platform service’ means any of the following: (a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; (h) advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g);

Comments

The DMA proposal makes clear that it is concerned with platforms that connect businesses with consumers, and which can regulate that connection: see Article 3(1)(b) and recitals 6 and 12.

Recital 13, however, creates ambiguity because it suggests that “end users” within the meaning of the DMA can also be “business users”.

Consistent with the DMA’s stated objective and scope, it would therefore be useful to clarify that mere inputs and B2B services do not qualify as “core platform services” under the DMA. This is consistent with the DMA’s objective of addressing concerns relating to services that “directly intermediate between business users and end users” (Recital 12, emphasis added).

Absent clarification, there is a risk of confusion as to whether mere inputs or B2B services would be caught, despite not having the characteristics of a gatekeeper that regulates businesses’ access to end users. Examples could include data storage solutions for businesses or business analytics tools.

Article 2(2)(h): advertising services

Advertising services are treated as core gatekeeper services only if they are “provided by a provider of any of the core platform services listed in points (a) to (g).”

Comments

We understand -- and support -- the DMA's aims of ensuring transparency in online advertising. Recital 42 refers to sector-wide concerns and the "*sheer complexity of modern day programmatic advertising.*"

However, the current language of Article 2(2)(h) brings advertising services within scope only if they are offered by a provider of other core platform services.

This undermines the DMA's objective of ensuring transparency because it leaves many important advertising services out of scope that would meet the DMA's quantitative thresholds. It would also lead to unjustified unequal treatment since the question of whether a particular advertising service is a 'gatekeeper' is unrelated to what other services are provided by the same undertaking.

Articles 2(2)(g) and 2(11): cloud computing services

Cloud computing means a digital service as defined in point 19 of Article 4 of Directive (EU) 2016/1148 of the European Parliament and of the Council".

Comments

The definition of cloud computing services in the NIS Directive is, by design, broad because the Directive aims to address issues of cybersecurity -- it does not limit itself to services that regulate businesses' access to users.

The NIS Directive definition therefore covers all digital services that "*allow access to a scalable and elastic pool of shareable computing resources*". The Commission's accompanying Communication states that this definition includes "*software as a service*".

The DMA's cross-reference to the NIS Directive therefore would bring a broad range of services under its scope that have none of the characteristics of gatekeeper platforms. And it would create unequal treatment between online services and their on-premises equivalents. It would, for example, apply to online email, calendaring, productivity, and database services, while on-premises competitors of such services would not be covered.

Article 3(2)(a): group level turnover / market capitalisation thresholds

This provision formulates a quantitative threshold at the level of the “*undertaking to which*” the core platform service belongs of “*an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, or [...] average market capitalisation or the equivalent fair market value of [...] at least EUR 65 billion in the last financial year, [...]*”.

Comments

A turnover-based threshold for a given service may be a reasonable proxy for the significance of that service. Formulating a turnover or market capitalization threshold at the group level, however, is liable to lead to unjustified unequal treatment.

The same kind of service with the same number of users may or may not be covered by the DMA depending on whether the undertaking that owns the service reaches the specified revenue or value threshold, even if that undertaking’s revenues are unrelated to the service in question.

As such, the DMA risks being both underinclusive by not covering services that are in fact important (*i.e.*, services with a large number of users, but belonging to undertaking low turnover would not meet the group-wide turnover threshold). At the same time it risks being overinclusive by covering services without market significance (*i.e.*, services that generate little revenue, but that belong to an undertaking with significant revenues from unrelated sources would be covered).

The fact that the threshold operates as a presumption does not resolve this concern, since the general criteria are broadly defined and meeting the thresholds has considerable legal consequences.

B. Application of the rules

Article 1(6) - overlapping national measures

“This Regulation is without prejudice to the application of Articles 101 and 102 TFEU. It is also without prejudice to the application of: national rules prohibiting anticompetitive agreements, decisions by associations of undertakings, concerted practices and abuses of dominant positions; national competition rules prohibiting other forms of unilateral conduct insofar as they are applied to undertakings other than gatekeepers or amount to imposing additional obligations on gatekeepers”

Comments

Article 1(5) stipulates that *“Member States shall not impose on gatekeepers further obligations by way of laws, regulations or administrative action for the purpose of ensuring contestable and fair markets.”* Similarly, Recital 9 acknowledges that national competition rules *“should not affect the obligations imposed on gatekeepers under this Regulation and their uniform and effective application in the internal market.”*

At the same time, however, Art. 1(6) reserves the possibility for Member States to apply their competition rules. Retaining the possibility for national competition laws to regulate substantively the same practices as the DMA is liable to frustrate the DMA’s goal of achieving a harmonised set of rules on the contestability of digital markets. For example, the latest amendment to the German Act against Restrictions of Competition -- like the DMA -- addresses practices concerning self-preferencing, data usage and interoperability.

The need for consistency across the DMA and national competition laws is recognised in the Legislative Financial Statement accompanying the DMA, which refers to *“an emerging fragmentation of the regulatory landscape”*; Member States addressing *“platform related problems at national level”* (including through competition measures); and *“national rules in response to the problems associated to the conduct of gatekeepers in the digital sector”* including as regards *“MFN clauses”* (a competition issue) (paragraphs 1.5.2-1.5.3).

Therefore, permitting more extensive national measures alongside the DMA will exacerbate -- not resolve -- the problem of fragmented rules across Member States.

Article 3(8) - direct applicability of Article 6 obligations

“The gatekeeper shall comply with the obligations laid down in Articles 5 and 6 within six months after a core platform service has been included in the list pursuant to paragraph 7 of this Article.”

Article 25 - direct exposure to non-compliance decisions for Article 6 obligations without specification

“The Commission shall adopt a non-compliance decision in accordance with the advisory procedure referred to in Article 32(4) where it finds that a gatekeeper does not comply with one or more of the following:

(a) any of the obligations laid down in Articles 5 or 6;

(b) measures specified in a decision adopted pursuant to Article 7(2);”

Article 26 - direct exposure to fines for Article 6 obligations without specification

“In the decision pursuant to Article 25, the Commission may impose on a gatekeeper fines not exceeding 10% of its total turnover in the preceding financial year where it finds that the gatekeeper, intentionally or negligently, fails to comply with:

(a) any of the obligations pursuant to Articles 5 and 6;

(b) the measures specified by the Commission pursuant to a decision under Article 7(2);”

Comments

Article 3(8) suggests that the obligations set out in Article 6 are directly applicable and subject to fines for non-compliance under Article 26 without further specification.

This is in tension with Recitals 33 and 58 which envisage a “*regulatory dialogue with gatekeepers*” and further specification for obligations that “*require specific implementing measures in order to ensure their effectiveness and proportionality*”. In line with these recitals, the obligations listed under Article 6 are identified as being susceptible to further specification.

The direct applicability under Article 3(8), however, means that a gatekeeper will have to comply with Article 6 - and is exposed to high fines and non-compliance decisions - even before the envisaged regulatory dialogue can take place that would specify what a particular gatekeeper is meant to do in concrete terms to comply in an effective and proportionate manner. Moreover, the threat of fines and non-compliance decisions is inconsistent with the envisaged possibility to seek guidance under Article 7(7).

This approach is liable to lead to legal uncertainty, stifle technical development, and undermine the envisaged concept of a

regulatory dialogue.

To enable a genuine regulatory dialogue and safeguard legal certainty, a better approach is to provide for specification of the obligations under Article 6 prior to their applicability.

This approach is reflected in the recent amendment to the German competition law and the UK proposals for 'pro-competitive interventions.

Article 8 - possibility to justify practices

The draft DMA, unlike the amendment to the German competition act and the UK proposal for digital codes of conduct, does not provide for a general possibility for gatekeepers to justify their conduct. Instead, Articles 8 and 9 include only narrow and highly restrictive exceptions to the obligations under Articles 5 and 6.

Comments

Given the wide scope of the DMA, the onerous nature of its obligations, and the complex technologies involved, there is a serious risk that a rigid application -- without a possibility to justify exceptions -- will have disproportionate and counter-productive consequences. Rather than promote openness and innovation, a rigid application may stifle innovation, diminish competition, and harm businesses and end users.

By contrast, providing for a possibility to justify exceptions would future-proof the DMA and give it the requisite flexibility to achieve its objectives while avoiding unintended harmful consequences. This approach would also be consistent with the approach adopted under the amendment of the German competition act and the UK proposals for digital codes of conduct.

Article 10 - updating lists of obligations

"The Commission is empowered to adopt delegated acts in accordance with Article 34 to update the obligations laid down in Articles 5 and 6 where, based on a market investigation pursuant to Article 17, it has identified the need for new obligations addressing practices that limit the contestability of core platform services or are unfair"

Comments

Article 10 grants the Commission the possibility to add new obligations to Articles 5 and 6, following a market investigation. Recital 78 suggests that this possibility serves the need to ensure the regulation is future-proof. For the same reason, the Commission should have the possibility to sunset or narrow obligations listed in Articles 5 and 6 if -- in light of technical, commercial, or other developments -- it considers that those obligations are no longer warranted.

Moreover, certain DMA provisions address policy objectives that are covered in other regulations, which creates a risk of misalignment (and possibly conflicting rules). For example, the GDPR pursues -- and seeks to strike a balance between -- the objectives of (i) enhancing user protection over the data, and (ii) promoting the free flow of data within the internal market. That balance risks being materially altered by provisions of the DMA that deal with data combinations, access and portability. Accordingly, there is a need for a mechanism to ensure regulatory alignment as between the DMA and other legislative measures -- Articles 10 and 17 can provide a solution in this regard.

Article 2 - Definition of services

The DMA does not explain under what circumstances functionality offered by a gatekeeper constitutes a distinct service as opposed to an element of the core platform service provided by the gatekeeper.

Comments

Several of the DMA's provisions govern the relationship between a gatekeeper's core platform service and other separate or 'ancillary' services that the gatekeeper provides. The DMA, however, provides no guidance as to how a separate service is to be distinguished from the core platform service. Existing case law on tying provides a basis for identifying when a separate 'service' (as opposed to a mere product feature) exists.

Article 38(2) -- Evaluation mechanism

"The evaluations shall establish whether additional rules, including regarding the list of core platform services laid down in point 2 of Article 2, the obligations laid down in Articles 5 and 6 and their enforcement, may be required to ensure that digital markets across the Union are contestable and fair. Following the evaluations, the Commission shall take appropriate measures, which may include legislative proposals"

Comments

Consistent with our comments in respect of Article 10, any review mechanism ought to include the possibility to remove or narrow obligations -- not only to add them.

Any evaluation mechanism should -- as far as possible -- use objective, quantifiable measures to evaluate whether the current list of obligations are proportionate and warrant retention in the DMA. The Legislative Financial Statement sets out expected enefits of the DMA that can be measured and ought, therefore, to be addressed in the envisaged evaluation process. These include: (i) a 1.5% annual increase in GDP, (ii) 1-1.4 million new jobs, (iii) increased sales via smaller platforms, and (iv) a 13 billion euro consumer surplus.

C. Specific provisions

<p>Article 5(a) - Combination of personal data</p> <p><i>“refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679.”</i></p>
<p>Comments</p> <p>We support rigorous protection of personal data. The proper legal instrument for that protection is the GDPR, which already provides for a high level of protection.</p> <p>Introducing rules on the protection of personal data in the DMA is liable to give rise to tension with the GDPR and create legal uncertainty. For example, the GDPR allows combining data across services on grounds other than user consent, such as legitimate interests or a contract.</p> <p>This is for good reasons: requiring individual consent for every instance of cross service use is liable to be cumbersome, unwieldy, and disruptive for users and services, and may hinder or delay innovative developments and vertical integration that benefit users and businesses.</p> <p>The obligation in Article 5(a), moreover, contradicts existing case law on data combination: in its <i>Facebook</i> decision, the Bundeskartellamt expressly found that Facebook’s combination of data from different internal services was legitimate and beneficial, and only challenged the combination of data derived from third-party services.</p> <p>At the same time, concerns related to proper protection and use of personal data apply universally, regardless of the nature and importance of a particular service. There is therefore no good reason to diverge on the level of protection of personal data depending on the type of service.</p>
<p>Article 5(g) - disclosure of prices for advertising services</p> <p><i>“provide advertisers and publishers to which it supplies advertising services, upon their request, with information concerning the price paid by the advertiser and publisher, as well as the amount or remuneration paid to the publisher, for the publishing of a</i></p>

given ad and for each of the relevant advertising services provided by the gatekeeper.”

Comments

We support transparency on the terms of advertising services and make clear to our advertiser and publisher customers the prices they pay. We have also published our aggregated take-rates so that publishers and advertisers understand what share of spend we retain.

Article 5g, however, could be read to require gatekeepers not only to be transparent about the prices that a given counterparty (advertiser or publisher) pays, but also to disclose the prices that *other* counterparties pay on a granular basis. For example, a publisher would see not only the fees it pays to the gatekeeper for publisher-facing services it uses (as is the case today), it would also see the fees paid by every advertiser to the gatekeeper for advertiser-facing services. Conversely, an advertiser would be able to see the fees every publisher pays for publisher-facing services.

There are significant problems with this approach:

First, it is not necessary to allow a counterparty to make decisions on what advertising service to use. For example, a publisher will want to select the publisher-facing ad service that generates the most publisher revenue. The publisher does not need to know the prices that advertisers pay for the services they purchase to make this selection. If Product A generates EUR2 revenue and Product B generates EUR1 of ad revenue for the publisher per ad - it is irrelevant to the publisher's choice that the advertiser behind the bid on Product A paid 20 cents for advertiser services while the advertiser behind the bid on Product B paid 10 cents.

Second, business partners can suffer commercial harm, including reduced competition, from mandating disclosure of the fees they pay. For example, advertisers could suffer higher costs and reduced competition from the fees they pay being disclosed to publishers. Many publishers compete to sell inventory *direct* to advertisers (i.e. outside of the intermediation services of the gatekeeper) in addition to using intermediation services. Telling publishers the fees paid by advertisers for intermediation services will give publishers commercially sensitive information on the cost of the advertisers' "outside option" when negotiating direct deals and therefore risks reduced competition.

Accordingly, the recent amendment to German competition legislation does not require similarly far reaching disclosures but focuses on disclosure of sufficient information to assess the value of the service (§19a ARC, paragraphs 2(6)).

These considerations warrant treating Article 5(g) as an Article 6 measure to be specified by the European Commission, based on the German provision. This can most efficiently be achieved by consolidating Articles 5(g) and 6(1)(g) into a single provision.

As regards Article 6(1)(g) specifically, we have two principal comments. First, the requirement to provide data for free contrasts with Article 6(1)(j), which permits charges based on FRAND rates. Second, the clause ought not to require the disclosure of data that might damage the integrity of the system, consistent with Article 6(1)(c).

Article 6(1)(a) -- Using businesses' data to compete with them

“refrain from using, in competition with business users, any data not publicly available, which is generated through activities by those business users, including by the end users of these business users, of its core platform services or provided by those business users of its core platform services or by the end users of these business users”

Comments

We support the principle that gatekeepers should not use data they gather from business users to distort competition in favour of gatekeepers' own rival businesses.

The language of Recital 43, makes clear that the concern is with data “gained from transactions” with a business user and the use of these data by the gatekeeper for “*similar services*”. We consider that, for clarity and legal certainty, this language should be reflected in Article 6(1)(a) itself.

In addition, we note the principle in recital 45 that obligations concerning cloud computing “*should not affect the right of gatekeepers to use aggregated data for providing ancillary data analytics services.*” The same principle ought to apply to other product areas too -- there is no reason for limiting it to Cloud.

Article 6(1)(b) -- Uninstalling preloaded apps

“allow end users to un-install any pre-installed software applications on its core platform service without prejudice to the possibility for a gatekeeper to restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third-parties”

Comments

Recital 46 explains that this provision aims to prevent a gatekeeper from “*favour[ing] its own services or products on its core*

platform service, to the detriment of the same or similar services that end users could obtain through third parties.” Any rule on users’ ability to uninstall apps should, therefore, require the same conditions to be applied to all preloaded apps whether they belong to gatekeepers or third parties.

Moreover, while Article 6(1)(b) offers an exception for apps that are essential to the operating system or the device, it omits services on which other preloaded or downloaded apps may rely. It also overlooks the possibility to allow users to disable apps, which amounts to the same outcome as uninstalling from a user’s perspective, but avoids much of the technical complexity that comes from fully removing an app from a device.

The better approach, in our view, is to apply the wording of Recital 47, which envisages the possibility for gatekeepers to *“implement proportionate technical or contractual measures”* to safeguard integrity.

Article 6(1)(d) - Ranking

“refrain from treating more favourably in ranking services and products offered by the gatekeeper itself or by any third party belonging to the same undertaking compared to similar services or products of third party and apply fair and non-discriminatory conditions to such ranking”

Recital 49

“the gatekeeper should not engage in any form of differentiated or preferential treatment in ranking on the core platform service, whether through legal, commercial or technical means, in favour of products or services it offers itself or through a business user which it controls. To ensure that this obligation is effective, it should also be ensured that the conditions that apply to such ranking are also generally fair. Ranking should in this context cover all forms of relative prominence, including display, rating, linking or voice results.”

Comments

We support principles that ensure ranking is free from artificial manipulation and provides users with relevant results.

Ranking is a complex task especially for services that offer results across a wide spectrum of different types of queries and information. A crucial element to provide useful and relevant results is for a service to have the ability to use different formats and different algorithms for different results.

The High Court of England and Wales found, for example, in *Streetmap* that Google showing a map in response to queries for locations was beneficial for users and had no demonstrable adverse impact. In *Shopping*, the European Commission recognized that it was beneficial for Google to show specialized results with different formats and algorithms.

Yet the language in Recital 49 could be read to suggest that Article 6(1)(d) is meant to outlaw any differentiated treatment of results. Such a position recently forced Google to remove Shopping Units in Turkey with detrimental consequences for countless Turkish merchants, which lost traffic and now pay higher prices for promoting their offers, and harm to users for whom it is now more difficult to find relevant product offers. It also runs counter to the explanation on “fairness” in Recital 57 which identifies as unfair only unjustified differentiation and disproportionate advantages. While Recital 57 discusses fairness principles in the context of app stores, there is no good basis for formulating different fairness principles across different obligations under Article 6(1). In particular, as Recital 57 makes clear a categorical and absolute prohibition of differentiation - as suggested by Recital 49 - is incompatible with a properly understood fairness standard.

The ambiguity created by Recital 49 is compounded by the fact that Article 6(1)(d) uses three different overlapping terms (no disfavoring, fair, non-discriminatory) to denote the requisite ranking standard, which is liable to create confusion and uncertainty.

It is critical to clarify that Article 6(1)(d) does not preclude gatekeepers engaging in justifiable differentiation (e.g., ranking different types of results with different formats and algorithms, or showing paid results). Otherwise, search services would be forced to undo years of innovation and their ability to show useful and relevant results would be undermined.

Article 6(1)(f) - Interoperability

“allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services”

Comments

We are active proponents for open and interoperable systems. We developed Android, for example, to be an open and fully interoperable operating system and we work on numerous industry initiatives to promote interoperability.

As developers of interoperable systems, we know, however, that enabling interoperability can pose difficult questions and tradeoffs in terms of functionality, quality assurance, user safety, and intellectual property, for example. Critically, enabling interoperability presents different challenges for an operating system (which by design is meant to interoperate with third-party

products) and application level services.

In line with these considerations, Recital 52 suggests that Article 6(1)(f) is limited to providers of operating systems. However, this limitation is not clearly articulated in the wording of Article 6(1)(f) which in conjunction with the introductory language to Article 6(1) could be read as applying in an undifferentiated manner to all core platform services.

An overly broad and rigid interoperability requirement is liable to prevent or delay technical development and innovation. We therefore recommend clarifying that the obligation under Article 6(1)(f) applies only to operating systems and recognizes the need for a reasonable balance in the provision of interoperability (including, per Recital 41, an exemption for conduct that leads to an “*improvement of end user offering*”).

Article 6(1)(h) -- Data portability

“provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access”

Comments

We have long-supported consumers’ control over their data, and realised some time ago that data portability made users value our services more. Since 2007, our projects to enhance data portability include the Data Liberation Front, Google Takeout, and the Data Transfer Project.

However, it is not clear what “*continuous and real time*” access means in this context, or whether it is possible as a technical matter for any given product. The reference to “*effective*” data portability provides the Commission with flexibility to determine whether a particular data portability tool is sufficient in a given situation, whether data is provided sufficiently quickly, or whether further measures are required.

Article 6(1)(i) -- Data generated by business users

“provide business users, or third parties authorised by a business user, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products or services provided

by those business users; for personal data, provide access and use only where directly connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end user opts in to such sharing with a consent in the sense of the Regulation (EU) 2016/679”

Comments

We have a number of concerns with Article 6(1)(i).

First, the definition of what constitutes business users’ data appears exceptionally broad. For example, Recital 54 refers to “*data inferred from*” business users’ activity. Inferred data would typically include proprietary commercial or technical insights that require engineering work to produce and may be used to improve Google’s services. A requirement to disclose business secrets of this kind would undermine innovation.

Second, as noted in respect of Article 6(i)(h), it is not clear what “*continuous and real time*” (or “*high quality*”) access means in this context, or whether it is possible as a technical matter for any given product.

Third, the requirement to provide data for free contrasts with Article 6(1)(j), which permits charges based on FRAND rates.

Article 6(1)(j) - access to search data

“provide to any third party providers of online search engines, upon their 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 online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data”

Comments

Recital 56 contemplates the disclosure of “*aggregated datasets containing information about what users searched for, and how they interacted with, the results that they were served*”. Article 6(1)(j), however, seems to go further by requiring disclosure of ranking, query, click, and view data, subject only to anonymization.

We question the premise of this far reaching and intrusive disclosure and sharing requirement. There is no empirical evidence that access to data is a material limiting factor in search engine competition. Nor is there a good basis for singling out search

data for regulatory disclosure and sharing obligations, as opposed to other data sets.

The disclosure obligation foreseen in Article 6(1)(j) conflicts with fundamental legal principles, including the protection of intellectual property, proportionality, and equal treatment. We therefore suggest that this provision should be removed. In fact, the disclosure and sharing obligation imposed under Article 6(1)(j) contravenes established case law on the duty to share assets with rivals.

Moreover, anonymization alone does not necessarily protect against privacy violations (see a [study in Nature by Yves Alexandre de Montjoye](#), one of the author's of the Commission's report into 'Competition Policy for the Digital Era'). And disclosure of search data may have other serious, harmful consequences including exposing a search service to ranking manipulation and copying of its results and search algorithms.

Should a disclosure obligation for search data, nonetheless be maintained, it must give due consideration to legitimate interests standing against such disclosure.

Article 12 -- Reporting concentrations

"A gatekeeper shall inform the Commission of any intended concentration within the meaning of Article 3 of Regulation (EC) No 139/2004 involving another provider of core platform services or of any other services provided in the digital sector irrespective of whether it is notifiable to a Union competition authority under Regulation (EC) No 139/2004 or to a competent national competition authority under national merger rules"

Comments

We recognise the Commission's interest in being made aware of transactions involving core platform services. However, the requirement to report transactions that do not involve core platform services is unrelated to the objectives of the DMA -- keeping markets contestable -- and undermines the DMA's logic of applying obligations only to in-scope core platform services.