Data-related Aspects of the Digital Market Act Proposal of the EU Commission

Wolfgang Kerber
(University of Marburg)

FA Recht der Daten (GRUR), 1.2.2021

1. Background of the DMA

- large concerns about power of large online platform (esp. GAFA)
- many reports: consensus: we have a huge problem and have to do more!
- Can it be solved within traditional competition law?
  + during 2019 increasing consensus that competition law is not enough
- Furman report (March 2019) was most influential
  + thesis: traditional competition law is not sufficient
  + we need additionally an ex-ante regulation for platforms
  + new "digital market unit" with powers for
    > "codes of conduct" for platforms with a "strategic market status"
    > pro-competitive measures (data mobility, open data / standards)
- Germany: § 19a GWB about firms with "paramount significance for competition across markets" (additional abuse control) (enacted Jan 2021)
- EU: (discussion about "ex-ante regulation" / "new competition tool")
  + Digital Market Act proposal (15 December 2020)
- UK: CMA proposal (8 Dec 2020) how to implement Furman proposal

2. DMA: The problem, objectives, and basic approach

What is the problem? (DMA, p.1)

> Large platforms have emerged benefitting from characteristics of the sector such as strong network effects, often embedded in their own platform ecosystems, and these platforms represent key structuring elements of today's digital economy, intermediating the majority of transactions between end users and business users. Many of these undertakings are also comprehensively tracking and profiling end users.[1] A few large platforms increasingly act as gateways or gatekeepers between business users and end users and enjoy an entrenched and durable position, often as a result of the creation of conglomerate ecosystems around their core platform services, which reinforces existing entry barriers.

Specific problems: lack of contestability and unfair practices

Objectives of the DMA:

- contestability
- fairness: through imbalances of bargaining power between gatekeepers and business users and end users ("unfair business practices" / fair trading)

Legal basis:

- Art. 114 TFEU (internal market)
- DMA is outside of competition law (but Art.101/102 TFEU can still be fully applied)

Basic approach: designating providers of core platform services as gatekeepers which then have to comply with a number of obligations

3. Core platform services and gatekeepers (1)

- Important: DMA limited to digital markets with certain characteristics
- concept of "core platform services" which are relevant for
  + designating gatekeepers
  + obligations of gatekeepers refer to them
- list of core platform services (Art. 2(2) DMA)
  + online intermediation services
  + online search engines
  + online social networking services
  + video sharing platform services
  + number-independent interpersonal electronic communication services
  + operating systems
  + cloud computing services
  + advertising services

  (can be adapted by the Commission)

3. Core platform services and gatekeepers (2)

When are "providers of core platform services" (PCPS) gatekeepers (Art. 3 DMA)?

Three conditions:

(1) significant impact on the internal market
- high EEA turnover (6.5 bn €), threshold number of users (> 45 m end users or > 10,000 business users in EU), high market capitalisation (65 bn €), …

(2) operate one or more important gateways to customers
- very high number of business and end users for CPS

(3) (expected to) enjoy an entrenched and durable position in their operations
- presumption: PCPS has provided a CPS in at least 3 MS to a very high number of business and end users for at least three years

Designation as "gatekeeper" by the Commission (with regular review)

- directly through quantitative criteria or through a market investigation, if quantitative criteria not entirely met or PCPS have substantiated counterarguments
- special rules for PCPS that are foreseen of getting an entrenched and durable position (e.g. for preventing tipping)

4. Obligations of gatekeepers: Overview

Gatekeepers have to comply with a list of directly applicable obligations (ex-ante regulation), overall 18 obligations (7 data-related obligations)

Two types of obligations:

- Art. 5 obligations: (Black-list)

  + list of 7 obligations

- Art. 6 obligations "susceptible of being further specified"

  + list of 11 obligations

  + but here some "regulatory dialogue" possible how to implement

Some institutional aspects:

- PCPS have to make a notification and fulfill the obligations
- the "regulator" is the Commission [but who exactly is regulating?]
- Commission has far-reaching investigating and sanctioning powers, can conduct "market investigations", adapt the list of "core platform services", …
- Art. 16: in case of repeated non-compliance, all (!) behavioral and structural measures are possible [even breaking up as instrument of last resort]

5. Data-related obligations of gatekeepers (1)

More effective data portability: not only personal data, also for business users, also continuous / real-time portability / APIs … (goes far beyond Art. 20 GDPR)

Art. 6(1)h:

(h) 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 ;

Rec. 54:

(54) Gatekeepers benefit from access to vast amounts of data that they collect while providing the core platform services as well as other digital services. To ensure that gatekeepers do not undermine the contestability of core platform services as well as the innovation potential of the dynamic digital sector by restricting the ability of business users to effectively port their data, business users and end users should be granted effective and immediate access to the data they provided or generated in the context of their use of the relevant core platform services of the gatekeeper, in a structured, commonly used and machine-readable format. This should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that business users and end users can port that data in real time effectively, such as for example through high quality application programming interfaces. Facilitating switching or multi-homing should lead, in turn, to an increased choice for business users and end users and an incentive for gatekeepers and business users to innovate.

5. Data-related obligations of gatekeepers (2)

Data generated by business users on platform not allowed to be used by platform to compete with these businesses (dual role of platform) (P2B competition problem)

Art. 6(1)a

(a) 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;

Rec. 43

(43) A gatekeeper may in certain circumstances have a dual role as a provider of core platform services whereby it provides a core platform service to its business users, while also competing with those same business users in the provision of the same or similar services or products to the same end users. In these circumstances, a gatekeeper may take advantage of its dual role to use data, generated from transactions by its business users on the core platform, for the purpose of its own services that offer similar services to that of its business users. This may be the case, for instance, where a gatekeeper provides an online marketplace or app store to business users, and at the same time offer services as an online retailer or provider of application software against those business users. To prevent gatekeepers from unfairly benefitting from their dual role, it should be ensured that they refrain from using any aggregated or non-aggregated data, which may include anonymised and personal data that is not publicly available to offer similar services to those of their business users. This 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.

(also extended to advertising and cloud services (Rec. 44+45)

5. Data-related obligations of gatekeepers (3)

Effective access to data generated by business users on platforms (effective, high-qualitative, continuous / real-time, appropriate technical measures)

Art. 6(1)i

(i) 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; ;

Rec.55

(55) Business users that use large core platform services provided by gatekeepers and end users of such business users provide and generate a vast amount of data, including data inferred from such use. In order to ensure that business users have access to the relevant data thus generated, the gatekeeper should, upon their request, allow unhindered access, free of charge, to such data. Such access should also be given to third parties contracted by the business user, who are acting as processors of this data for the business user. Data provided or generated by the same business users and the same end users of these business users in the context of other services provided by the same gatekeeper may be concerned where this is inextricably linked to the relevant request. To this end, a gatekeeper should not use any contractual or other restrictions to prevent business users from accessing relevant data and should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required under Regulation (EU) 2016/679 and Directive 2002/58/EC. Gatekeepers should also facilitate access to these data in real time by means of appropriate technical measures, such as for example putting in place high quality application programming interfaces.

5. Data-related obligations of gatekeepers (4)

Advertising I: Access to data for independent performance measuring due to the opaqueness/intransparency of effects of ads (verification) (solving an information asymmetry problem in P2B contexts)

Art. 6(1)g: (g) provide advertisers and publishers, upon their request and free of charge, with access to the performance measuring tools of the gatekeeper and the information necessary for advertisers and publishers to carry out their own independent verification of the ad inventory;

Rec. 53: (53) The conditions under which gatekeepers provide online advertising services to business users including both advertisers and publishers are often non-transparent and opaque. This often leads to a lack of information for advertisers and publishers about the effect of a given ad. To further enhance fairness, transparency and contestability of online advertising services designated under this Regulation as well as those that are fully integrated with other core platform services of the same provider, the designated gatekeepers should therefore provide advertisers and publishers, when requested, with free of charge access to the performance measuring tools of the gatekeeper and the information necessary for advertisers, advertising agencies acting on behalf of a company placing advertising, as well as for publishers to carry out their own independent verification of the provision of the relevant online advertising services.

5. Data-related obligations of gatekeepers (5)

Advertising II: Transparency about prices/remunerations in advertising sector (due to opaqueness/intransparency/complexity of these services)

Art. 5g

(g) 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 given ad and for each of the relevant advertising services provided by the gatekeeper.

Rec.42

(42) The conditions under which gatekeepers provide online advertising services to business users including both advertisers and publishers are often non-transparent and opaque. This opacity is partly linked to the practices of a few platforms, but is also due to the sheer complexity of modern day programmatic advertising. The sector is considered to have become more non-transparent after the introduction of new privacy legislation, and is expected to become even more opaque with the announced removal of third-party cookies. This often leads to a lack of information and knowledge for advertisers and publishers about the conditions of the advertising services they purchased and undermines their ability to switch to alternative providers of online advertising services. Furthermore, the costs of online advertising are likely to be higher than they would be in a fairer, more transparent and contestable platform environment. These higher costs are likely to be reflected in the prices that end users pay for many daily products and services relying on the use of online advertising. Transparency obligations should therefore require gatekeepers to provide advertisers and publishers to whom they supply online advertising services, when requested and to the extent possible, with information that allows both sides to understand the price paid for each of the different advertising services provided as part of the relevant advertising value chain.

5. Data-related obligations of gatekeepers (6)

Sharing of search engine data with other search engines for reducing entry barriers and improving contestability (horizontal data-sharing with FRAND conditions)

Art. 6(1)j

(j) 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;

Rec.56:

(56) The value of online search engines to their respective business users and end users increases as the total number of such users increases. Providers of online search engines collect and store aggregated datasets containing information about what users searched for, and how they interacted with, the results that they were served. Providers of online search engine services collect these data from searches undertaken on their own online search engine service and, where applicable, searches undertaken on the platforms of their downstream commercial partners. 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 engine services. Gatekeepers should therefore be obliged to provide access, on fair, reasonable and non-discriminatory terms, to these ranking, query, click and view data in relation to free and paid search generated by consumers on online search engine services to other providers of such services, so that these third-party providers can optimise their services and contest the relevant core platform services. Such access should also be given to third parties contracted by a search engine provider, who are acting as processors of this data for that search engine. When providing access to its search data, a gatekeeper should ensure the protection of the personal data of end users by appropriate means, without substantially degrading the quality or usefulness of the data.

5. Data-related obligations of gatekeepers (7)

Granting a minimum level of choice for end users regarding consent to the combination of personal data (Facebook case of German Bundeskartellamt), also for improving contestability of core platform service

Art. 5(a): (a) 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. ;

Rec. 36: (36) The conduct of combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry. To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised alternative. The possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third party websites, and should be proactively presented to the end user in an explicit, clear and straightforward manner.

6. Assessment: Some very preliminary remarks (1)

Assessing DMA in general: [see, e.g. Caffara/Scott-Morton (2021), de Streel et al (2021), Vezzoso (2021) …]

- very bold and ambitious but also many open questions
- unclear whether main strategy of working with a list of generally prohibited behaviors is the best way of dealing with GAFA in ex-ante regulation
- some critical points:
  - + list based upon past and current cases => backward-looking
  - + more flexibility necessary, because it depends also on business models, whether the prohibited behaviors are a problem or not
  - + no solution for "strategic acquisitions of start-ups" (only new notification duty)

Similar but alternative approaches:

- § 19a GWB: BKartA can prohibit many of these behaviors (abuse control)
- UK / CMA proposal: here an own regulator (DMU) can set up more firm-specific codes of conduct for firms with "strategic market status"
  (i.e. much more flexible approach / no black/grey list of obligations for all)

6. Assessment: Some very preliminary remarks (2)

DMA in the context of EU data policy (1):

- DMA is making partly very far-reaching data-related obligations (about data portability, horizontal data-sharing on search engine markets, access to data on gatekeeper platforms for business users (and limitation of use of these data for gatekeepers), limiting combination of personal data through additional consent)
  + shows the pro-competitive approach of DMA (plus fairness)
- Although DMA does not address directly the problem of data power of gatekeepers, a number of obligations can help to set some limits to the power of GAFA to force users to provide data to them
  + several obligations give business and end users more choice using other distribution channels for their services or using other software, internet providers, apps, ID services, or more choice about combination of personal data
  + these "unbundling measures" do not only help competition / fairness, but through weakening the bundling in the ecosystems, GAFA also has a weaker grip on the data of business and end users (reducing their "data power")
  => But: the problem of collecting data from business and end users (surveillance) could have been much more directly and comprehensively addressed

6. Assessment: Some very preliminary remarks (3)

DMA in the context of EU data policy (2):

- DMA does not contribute much to policy for sharing more data with respect to data-driven innovation / research ("European strategy for data")
  - + horizontal data-sharing /search engines => pure competition remedy
  - + more data portability and data access for business users might lead to a wider reuse of data, but primarily about fairness (P2B, P2C) and competition (also limitations for platform for using those data)
  - + additional consent for combining personal data (Facebook case) is about competition and fairness
  - + "data access" in advertising is about transparency not reuse of data
- no obligations for making data of gatekeepers available
  - + for firms that need access to data for innovation (e.g. facilitating access to "data as an essential facility" or like new provision about data access in § 20 (1) GWB ["relative market power" / "data dependency"]
  - + for (scientific) research (or training algorithms) …