THE DIGITAL MARKETS ACT (DMA): A PROCOMPETITIVE RECALIBRATION OF DATA RELATIONS?

Philipp Bazenov†

Abstract

Since its publication in December 2020, the European Commission's regulatory proposal for a Digital Markets Act (DMA) continues to be the subject of sustained political and academic interest, particularly in the United States and Europe. Part of the "European strategy for data," the DMA is designed to address "the most salient incidences of unfair practices and weak contestability" in the digital economy, responding to concerns about the data-derived dominance of U.S. technology companies operating in Europe. This paper aims to provide the first comprehensive legal analysis of the DMA's recalibration of data relations in the European Union. Through an analysis of the data-specific obligations imposed on gatekeepers under the DMA and their interaction with existing laws and jurisprudence, this paper finds that the proposed access rights and limitations on the collection, combination and use of data give rise to significant ambiguities and could make "Big Tech" the winners of an act originally designed to tackle their dominance. This paper also finds that the DMA may recalibrate data relations in favor of Chinese tech companies wishing to strengthen their position in the EU against their U.S. competitors. Nevertheless, this paper will show that the adoption of the DMA will be a positive first step in the direction of recalibrating data relations in a way that—once teased out by future enforcement and case law—could allow for a more active contestation of digital markets, and a freer flow of data.

TABLE OF CONTENTS

† New York University School of Law; LL.M. in Competition, Innovation and Information Law. University College London; LL.B. in Law. Email: philipp.bazenov@law.nyu.edu. An earlier draft of this paper was awarded the Betty Bock Prize in Competition Policy at the NYU School of Law. I am grateful to Thomas Streinz for his helpful comments, suggestions, and his continued support. I am also grateful to Eleanor M. Fox and Harry First for their helpful comments on antitrust and digital platforms. I further thank Nora Kocher, Erin Husi, and the member editors of The Journal of Law, Technology & Policy whose suggestions have helped improve this work. Any errors or omissions are my own.

I. INTRODUCTION

For years, competition enforcers on both sides of the Atlantic have been trying to reduce concentration in digital markets and to tackle data-fueled anticompetitive and unfair conduct.[1] With the spotlight of public attention now placed on the data-derived dominance of Big Tech, policymakers have also started to act.

In June 2021, the U.S. House Judiciary Committee approved a bipartisan package of six bills aimed directly at strengthening antitrust enforcement against

1. Mikolaj Barczentewicz, *Privacy and Security Risks of Interoperability and Sideloading Mandates*, TRUTH ON THE MKT., (Feb. 3, 2022), https://truthonthemarket.com ("There has been a wave of legislative proposals on both sides of the Atlantic that purport to improve consumer choice and the competitiveness of digital markets.").

"Big Tech."[2] During the same month, Professor Lina Khan, a vocal critic of Big Tech's anticompetitive business models,[3] was sworn in as FTC Commissioner, following her nomination by President Biden. Furthermore, on July 9, 2021, President Biden issued an *Executive Order on Promoting Competition in the American Economy*, in which he declared that it was "the policy of [his] Administration to enforce the antitrust laws to meet the challenges posed by … the rise of the dominant Internet platforms, especially as they stem from … the aggregation of data, … the surveillance of users, and the presence of network effects."[4] Among other things, the Order encourages the FTC "to exercise [its] statutory rulemaking authority" in the areas of "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy" and "unfair competition in major Internet marketplaces."[5]

In Europe, there has been growing pressure on the European Commission to regulate digital markets. In particular, the Commission has been called upon to address the dominance of *gatekeepers* who provide digital intermediation and platform services and can abuse their power vis-à-vis business users and consumers as regards data collected and derived from their use of such platforms.[6] To address these issues, in February 2020, the European Commission presented a "Digital Strategy" and a "European Strategy for Data" which is meant to rely on a legal framework of "data protection, fundamental rights, safety and cybersecurity" as well as strong competition on the EU Single Market to make the EU "a leading role model for a society empowered by data" to the benefit of "every European," "businesses," and "the planet."[7]

One of the European Commission's latest regulatory proposals forming part of the Digital Strategy is the Digital Markets Act (DMA) published on December 15th, 2020.[8] Some high-quality reports and academic opinions about the significance of the DMA for the wider theoretical and conceptual frameworks in EU competition law (for example, within the context of the debate around the creation of a "New Competition Tool" (NCT)) as well as the distinction between competition law and regulation have since been published.[9]

2. Ending Platform Monopolies Act, H.R. 3825, 117th Cong. (2021); Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Cong. (2021); Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, H.R. 3849, 117th Cong. (2021); Merger Filing Fee Modernization Act of 2021, H.R. 3843, 117th Cong. (2021); American Choice and Innovation Online Act, H.R. 3816, 117th Cong. (2021); State Antitrust Enforcement Venue Act of 2021, H.R. 3460, 117th Cong. (2021).

3. Cecilia Kang, *Biden Nominates Lina Khan, a Vocal Critic of Big Tech, to the F.T.C.*, N.Y. TIMES (Mar. 22, 2021), https://www.nytimes.com/2021/03/22/business/lina-khan-ftc.html.

4. Exec. Order No. 14036, 86 Fed. Reg. 36987 (July 9, 2021).

5. *Id.* at §§ 5(h)(i-iv).

6. Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM (2020) 842 final (Dec. 15, 2020) [hereinafter DMA].

7. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*, at 1, COM (2020) 66 final (Feb. 19, 2020); *see also Shaping Europe's Digital Future*, EUR. COMM'N, https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy (explaining the European digital strategy) (last updated Sept. 15, 2021).

8. DMA *supra* note 6, at 1.

9. *See, e.g.*, *infra* notes 23, 49, 127, 131, and 137.

However, this paper differs from existing contributions. Through an analysis of the data-specific access and sharing obligations in the DMA and a subsequent comparison with existing regulations on the collection, processing and sharing of data in the EU, as well as recent legislative and jurisprudential developments in the area of competition law, this paper considers whether the DMA creates ambiguous, overlapping, or duplicative obligations and, if so, whether this may undermine legal certainty and diminish the DMA's practical effects in improving the contestability of digital markets. In doing so, this paper "follows the data" to understand which parties have access to what types of data under what conditions, how the DMA will change the status quo, and what effects this may have on competition in digital markets, including for U.S. technological companies. In particular, this paper focuses on the six (out of eighteen) *gatekeeper* obligations in the DMA that are specific to data. It will find that these obligations fall into one of two broad categories: obligations to *grant access* to data and obligations to *limit* the collection, combination, and use of data.

This paper will show that the obligations in the DMA may fail to "revolutionize" the data-dependent platform economy and that it is conceivable that *gatekeepers*, rather than business users and consumers, will be the largest beneficiaries of the obligations imposed on other gatekeepers under the DMA. Nevertheless, it will find that the adoption of the DMA will be a move in the right direction of recalibrating data relations in a way that—once teased out by future enforcement and caselaw—could allow for a more active contestation of digital markets, and a freer flow of data across the EU.

This paper proceeds in four parts. Part II analyzes the DMA's key provisions, objectives, and obligations imposed on *gatekeepers*. Part III "follows the data" to understand how the DMA will recalibrate[10] data relations in the EU and beyond against the background of existing regulations, Commission competences, and Member State competition law. Part IV identifies and analyzes the risk of gatekeepers rather than their SME competitors, business users, and consumers becoming the true beneficiaries of the DMA. It also considers what this may mean for the competition between U.S. and Chinese "Big Tech" companies in European digital markets. Part V concludes the findings.

10. For the purposes of this paper, "(re)calibration" means the precise (re)adjustment for a particular function. *Calibrate*, Merriam-Webster.com Dictionary, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/calibrate (last visited Apr. 15, 2022). In the case of the DMA, the function to be served by the readjustment of data relations through regulation is the transformation of digital markets in the EU to meet the objectives defined by the European Commission, including but not limited to increasing the contestability of digital markets and reducing data-based unfair practices. DMA *supra* note 6, at 2–3. In light of this paper's approach of "following the data," the concept of "recalibration" is particularly useful in assessing the solutions the DMA aims to present to the problems of data-fueled anticompetitive and unfair conduct. This is because the data relations that will be recalibrated by the DMA (e.g., between gatekeepers and business users, between different gatekeepers, and between gatekeepers and consumers) already exist. Thus, rather than merely creating new data relations where there were none, the DMA primarily aims to change how the benefits of the existing data relations in digital markets are distributed "to allow end users and business users alike to reap the full benefits of the platform economy." *See* DMA *supra* note 6, at 2–3.

II. KEY PROVISIONS AND MECHANISMS OF THE DMA

A. Objectives and Context

On December 15th, 2020, the European Commission published a "Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector," also known as the *Digital Markets Act* (DMA).[11] The stated general objective of the DMA is "to allow platforms to unlock their full potential by addressing at EU level the most salient incidences of unfair practices and weak contestability so as to allow end users and business users alike to reap the full benefits of the platform economy and […] digital economy […] in a contestable and fair environment."[12] The Commission has pointed to a number of challenges which the DMA is meant to address.[13] However, it is submitted that all of these challenges fall into at least one of the following three categories: First, competition and contestability of digital markets; second, and relatedly, the creation of a non-fragmented European Single Digital Market; third, data and consumer protection.

First, the DMA is meant to address issues of competition and the contestability in digital markets which are not sufficiently addressed by EU competition law in its current scope.[14] For instance, recent proposals by academics and the Commission to create a New Competition Tool (NCT) in the EU, which would stand "between competition law and economic regulation"[15] and would address market failures which fall outside the scope of existing EU competition law for lack of anticompetitive conduct or due to specific market characteristics, reflects these concerns.[16] This is especially the case in digital markets, which are categorized by strong network effects that, together with data-related market characteristics, allow large platform operators to build "platform ecosystems" to which they can control the access.[17] This turns large digital platform operators into *gatekeepers* of their respective "platform ecosystems" which intermediate a multitude of "transactions between end users and business users," making the latter dependent on *gatekeepers* and their services.[18] As a result, *gatekeepers* are able to entrench their dominance in existing markets, but also to leverage their existing dominance to gain strong market positions in adjoining markets. Gatekeepers' status in relation to their *platform ecosystems* also gives them a superior bargaining position in

11. Consolidated Version of the Treaty on the Functioning of the European Union art. 26, 114, Oct. 26, 2012, 2012 O.J. (C 326/59).

12. DMA, supra note 6, at 2–3.

13. *Id.*

14. *See id.* at 2 ("The identified . . . problems are currently not (or not effectively) addressed by existing EU legislation.").

15. Heike Schweitzer, *The New Competition Tool: Its Institutional Set Up and Procedural Design*, EUR. COMM'N (2020), https://ec.europa.eu/competition/consultations/2020_new_comp_tool/kd0420574enn.pdf.

16. Massimo Motta & Martin Peitz, *Intervention Triggers and Underlying Theories of Harm*, at 5 (2020), https://op.europa.eu/en/publication-detail/-/publication/0165f92c-14dd-11eb-b57e-01aa75ed71a1/language-en.

17. Kimmo Karhu & Paavo Ritala, *Slicing the Cake Without Baking it: Opportunistic Platform Entry Strategies in Digital Markets*, 54 LONG RANGE PLANNING, 1, 2 (Oct. 2021) (explaining that organizations must be able to control the platform to have success).

18. DMA, *supra* note 6, at 1.

establishing and maintaining contractual relations with other businesses and—through their terms of service—with consumers.[19] In this regard, the DMA is meant to prevent gatekeepers' anticompetitive or unfair conduct in relation to businesses and consumers by imposing obligations on *gatekeepers* to, on the one hand, refrain from the imposition of certain types of contractual clauses and, on the other hand, provide competing businesses with access to data needed for effective competition.[20] In some respects, the DMA also limits the unfair and anticompetitive uses which *gatekeepers* can make of any data they collect as a result of the intermediation between businesses and consumers offered on their platforms.[21]

Secondly, the DMA aims to prevent a fragmentation of the EU Single Market in relation to the laws governing the processing and transfer of personal and non-personal data. This aim is arguably necessitated by recent regulation and enforcement actions in a number of EU Member States—most notably Germany—aimed at establishing fair and contestable digital markets, as well as consumer and data protection against the background of the challenges posed by large digital platforms.[22] The risk of such national law measures is that they can lead to a complex patchwork of laws and regulations inhibiting the processing and transfer of data across the Single Market, thereby undermining legal certainty and contestability, and potentially inhibiting economic growth.[23]

Thirdly, the DMA picks up the aim of protecting consumers and their privacy in relation to data collected by *gatekeepers* as a result of consumers' use of their products.[24] It should be noted, however, that the DMA is *not* primarily a data protection statute. In fact, the DMA's economic goals in relation to the coherency and contestability of digital markets and its underlying conceptualization of data as an *economic resource* may be seen to be *in tension* with data protection, which has a *fundamental rights* dimension in the EU and its Member States.[25] As will be explained in this paper, some of the DMA's data sharing requirements may even seem entirely antithetical to data protection.[26] The aim of data protection in the DMA should therefore primarily be seen as a *constraint* on data sharing and access to data where the latter would conflict with

19. *See* Jorge Padilla et al., *Self-preferencing by Gatekeeper Platforms: Implications for Digital Regulation*, VOX E.U. (Oct. 22, 2020), https://voxeu.org/article/self-preferencing-gatekeeper-platforms-implications-digital-regulation ("[F]irms with large bases of loyal customers that can determine how and whether third parties can access these customers.").

20. *See* DMA, *supra* note 6, at 24 ("To prevent gatekeepers from unfairly benefiting . . . it should be ensured that they refrain from using any aggregated or non-aggregated data . . . not publicly available.").

21. *Id.*

22. Dr. Jürgen Beninca et al., *Germany Adopts New Competition Rules for Tech Platforms*, JONES DAY (Jan. 2021), https://www.jonesday.com/en/insights/2021/01/germany-adopts-new-competition-rules.

23. *See* Oscar Borgogno & Giuseppe Colangelo, *Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs*, 35 COMPUT. L. & SEC. REV. 1 (2019) (explaining the link between data sharing, the free flow of data and economic growth); *see also* Michal S. Gal & Daniel L. Rubinfeld, *Data Standardization*, 94 N.Y.U. L. REV. 94, 737–770 (2019).

24. *See* DMA, *supra* note 6, at 29 ("The data protection and privacy interests of end users are relevant.").

25. *See* discussion *infra*, Sections III.B–C. (citing Streinz, *infra* note 270).

26. *See* discussion *infra*, Sections III.B-C.

consumers' rights to data protection,[27] for example under the General Data Protection Regulation (GDPR) or the Directive on Privacy and Electronic Communications or would give rise to an abuse of dominance through the imposition of unfair contractual conditions on the collection and processing (including through a combination across different services) of personal data.[28]

In considering the effects of the DMA on the status quo of data relations in the EU, it should therefore be kept in mind that some of the obligations imposed by the DMA on *gatekeepers* only serve *one* of the three objectives, while others serve two or all three overlapping objectives.

It should also be pointed out that the DMA is not meant to single-handedly address *all* of the challenges arising in digital markets, but rather forms part of a wider framework of EU regulatory initiatives creating a "Digital Strategy for Data," which, for example, also includes the Digital Services Act (DSA)[29] and the Data Governance Act (DGA).[30] While this paper's analysis and arguments will focus specifically on the DMA, it is helpful to keep in mind that both the DSA and the DMA proposals originate from the "Digital Services Act package" and align with the objectives articulated by the European Commission in its February 2020 communication *Shaping Europe's digital future* and the 2015 *Digital Single Market Strategy for Europe* (DSM).[31] For instance, the DSM called for a "fit for purpose regulatory environment for platforms and intermediaries" against the background of fragmented digital markets characterized by the presence of powerful platforms and diverging national practices on the removal of illegal content transmitted, stored, or hosted by Internet intermediary service providers.[32] Five years later, the Commission's *Shaping Europe's digital future* communication announced more specifically that there would be two work strands to reform the current legal framework.[33] The first strand of the reform would build upon core aspects of the E-Commerce Directive[34] to harmonize "the responsibilities of online platforms and information service providers and reinforce the oversight over platforms'

27. Meredith Broadbent, *The Digital Services Act, the Digital Markets Act, and the New Competition Tool*, CTR. FOR STRATEGIC INT'L STUD., (Nov. 10, 2020), https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool (explaining that if the commission mandates data sharing, it risks creating conflicts with the GDPR).

28. *See* discussion of the German Facebook case, and the DMA's prohibition on the combination of user data in the absence of opt-in consent *infra* Section II.D.2.

29. *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive*, 2000/31/EC, COM (2020) 825 final (Dec. 15, 2020) [hereinafter DSA].

30. *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020).

31. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Shaping Europe's Digital Future'*, COM (2020) 67 final (Feb. 19, 2020); *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A Digital Single Market Strategy for Europe'*, COM (2015) 192 final (May 6, 2015) [hereinafter DSM].

32. *See* DSM, *supra* note 31, at 11 (discussing a fit for purpose regulatory environment for platforms and intermediaries).

33. *See* Motta & Peitz, *supra* note 16, at 49.

34. Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178).

content policies in the EU."[35] The second strand would be aimed at achieving contestability and fairness in digital markets "characterized by large platforms with significant network effects acting as gate-keepers" through the introduction of novel *ex ante* rules for gatekeepers.[36] In December 2020, the two work strands of the *Digital Services Act package* resulted in two separate regulation proposals—the first strand resulting in the proposed DSA, and the second strand in the proposed DMA.[37]

Before discussing the effects of the DMA on data relations, it is useful to gain an overview of the DMA's key provisions and mechanisms.

B. Definitions and Scope of Application

The DMA defines "data" as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording."[38] Based on the definition of "personal data" in Article 4(1) GDPR, the DMA distinguishes between two categories of data: "personal data" and "non-personal data," defining the latter as "data other than personal data."[39] The DMA's scope of application is limited to "core platform services provided or offered by *gatekeepers* to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service."[40] As such, the DMA—unlike other data regulations in the EU—is an *asymmetric* regulation, in the sense that "different firms in the same industry are subjected to different levels of regulatory restraint."[41]

35. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's Digital Future, at 10–12 COM (2020) 67 final (Feb. 19, 2020); European Commission Press release IP/20/962, Commission Launches Consultation to Seek Views on Digital Services Act Package (June 2, 2020).

36. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's Digital Future, at 7–10 COM (2020) 67 final (Feb. 19, 2020).

37. *Id.*; European Commission, Inception Impact Assessment, (June 4, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com%3AAres%282020%292877647. For an overview of the DSA's relation to the DMA and the E-Commerce Directive, *see* Andrej Savin, *The EU Digital Services Act: Towards a More Responsible Internet*, 1 (Copenhagen Business School, CBS LAW Research Paper No. 21-04, 2021).

38. DMA, *supra* note 6, at 36.

39. *Id.*; *see also* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1, 33 [hereinafter GDPR] ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.").

40. DMA, *supra* note 6, at 36 (emphasis added).

41. Thomas P. Lyon & Haizou Huang, *Asymmetric Regulation and Incentives for Innovation*, 4 INDUST. CORP. CHANGE 769 (1995).

1. Designation as "Gatekeeper"

To come within the scope of the DMA, a company must be designated as a "gatekeeper" by the European Commission.[42] Article 2(1) of the DMA defines "gatekeeper" as "a provider of core platform services designated pursuant to Article 3."[43] Thus, to be designated as a *gatekeeper*, a company must both, provide a core platform service *and* meet the requirements in Article 3.[44]

The DMA recognizes eight different *core platform services* the providers of which are capable of being designated as gatekeepers: Online intermediation services,[45] online search engines,[46] online social networking services,[47] video-sharing platform services, number-independent interpersonal communication services,[48] operating systems,[49] cloud computing services,[50] and advertising services offered by the providers of any such services.[51]

As for the second limb of the designation—meeting "the requirements in Article 3"—the DMA states that a provider of a *core platform service* must meet three requirements:[52] Firstly, it must have "a significant impact on the internal market," secondly, it must "operate a core platform service which serves as an important gateway for business users to reach end users," and thirdly, it must "enjoy an entrenched and durable position in its operations or it [must be] foreseeable that it will enjoy such a position in the near future."[53] The DMA lists a number of circumstances which will give rise to rebuttable *presumptions* of satisfaction of these three requirements.[54]

For instance, the "significant impact on the internal market" requirement will be presumed to be met where the provider in question has had an annual turnover in the European Economic Area ("EEA") of EUR 6.5 billion or more in the last three financial years, or where it provides a core platform service in at least three Member States and its average market capitalization or equivalent fair market value in the last financial year amounts to EUR 65 billion or more.[55] Similarly, the operation of "a core platform service which serves as an important gateway for business users to reach end users" requirement will be presumed to be met where a provider provides a core platform service to more than 45 million monthly active end users and more than 10,000 yearly active business users in

42. *See* DMA, *supra* note 6, at 36 (explaining what the European Commission regards as a gatekeeper).
43. *Id.* at 34.
44. *Id.* at 34, 36.
45. *Id.* at 34.
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.* at 35.
50. *Id.*
51. *Id.*
52. *Id.* at 36.
53. *Id.* Note the significant difference between the designation thresholds for "gatekeepers" under the DMA and "very large online platforms" under the DSA. The latter merely requires an online platform to have an average of 45 million or more active monthly recipients of its service in the EU (with the number being adjusted by the Commission through delegated acts in the future to correspond to 10% of the EU's population, so as to reflect population change). *See* DSA, *supra* note 31, at 59.
54. DMA, *supra* note 6, at 36.
55. *Id.*

the EU.[56] Where this presumption is met for the last three financial years, there will, at the same time, also be a presumption as to the third requirement of an "entrenched and durable position."[57]

Of note, a provider that meets all three presumption thresholds is placed under an obligation to inform and provide relevant information to the European Commission within three months after it meets such thresholds, facilitating the Commission's *gatekeeper* designation process.[58] However, it is important to keep in mind that the three presumptions are *rebuttable* in the sense that providers of core platform services can avoid a designation as a *gatekeeper* if they present—together with their notification—"sufficiently substantiated arguments" demonstrating that they do not satisfy the three requirements of Article 3, taking into account the list of six market analysis "elements" set out in Article 3(6).[59] These six elements are: the size (turnover, market capitalization, operations and position) of a provider,[60] the number of business users dependent on its core platform services to reach end users and the number of end users,[61] barriers to entry from network effects and data driven advantages (i.e., in relation to a provider's access to and control of data or analytics capabilities),[62] scale and scope effects which benefit a provider (including as regards data),[63] lock-in effects in relation to business and end users, and "other structural market characteristics."[64] The six elements are also important where a provider does *not* satisfy the thresholds giving rise to presumptions of meeting the three requirements of Article 3(1) DMA, but the Commission *nevertheless* wishes to designate it as a gatekeeper on the basis of a *market analysis*. In such cases, the Commission must "take into account" the six elements of Article 3(6) in conducting its market analysis before it can designate a provider as a *gatekeeper*.[65]

Where a provider has been designated as a *gatekeeper*, its status must be reviewed by the European Commission at least biennially by verifying, among other things, whether the *gatekeeper* in question continues to meet the three requirements in Article 3(1)DMA.[66] If the facts which served as a basis for the designation of the provider in question as a *gatekeeper* have ceased to apply, the Commission must account for such change in a corresponding decision, and, if appropriate, lift the *gatekeeper* designation.[67] It should also be noted that the Commission is granted extensive investigative and enforcement powers under

56. *Id.* at 37.
57. *Id.*
58. *Id.* Note that a provider's failure to notify the Commission does not bar the latter from designating such provider a *gatekeeper*. In this sense, the notification requirement in art. 3(3) DMA should primarily be seen as *facilitating* the designation process, rather than serving as a prerequisite to designation.
59. *Id.* at 37–38.
60. *Id.* at 37.
61. *Id.*
62. *Id.* at 38.
63. *Id.*
64. *Id.*
65. *See id.* at 45 (setting out the procedure for gatekeeper designation through market investigation).
66. *Id.* at 38.
67. *Id.*

the DMA, including in relation to data held by private companies.[68] For instance, for the purpose of monitoring, implementing and enforcing the DMA, the Commission may "request access to data bases and algorithms" of private companies and "request explanations" about them by way of a "simple request or […] decision."[69]

2. Obligations of "Gatekeepers"

The European Commission's designation of a provider as a "gatekeeper" triggers eighteen different obligations in relation to each of the gatekeeper's core platform services.[70] By imposing obligations on *gatekeepers* once they are designated as such, the DMA takes an *ex ante* approach to the regulation of their conduct in digital markets.[71] Of these eighteen obligations in the DMA, eleven are "susceptible of being further specified."[72] All of the obligations in the DMA address at least one of the three categories of objectives of the DMA.[73] However, the majority of obligations relate to issues of competition and the contestability of digital markets, in particular, through the creation of data access rights for businesses for the purpose of analysis for the sale or advertising to end consumers, as well as through specific limitations on the collection, processing, sharing, and use of data collected in relation to businesses and end consumers by the *gatekeepers*.

For the purposes of this paper, it should be noted that not all of the DMA's obligations imposed on *gatekeepers* make explicit reference to the collection,

68. *See* DMA, *supra* note 6, at 47 (recognizing the need to regulate large platforms that act as intermediaries between the transactions of end users and business users while listing some of the investigative and enforcement powers of the Commission).

69. DMA, *supra* note 6, at 47.

70. *See* Case 322/81, NV Nederlandsche Banden Industrie Michelin v Comm'n, 1983 EU:C 313 (discussing to some extent, this mechanism is reminiscent of the notion of "special responsibility of dominant undertakings" in EU competition law under Art. 102 TFEU and CJEU caselaw, whereby dominant companies have "a special responsibility not to allow [their] conduct to impair genuine undistorted competition on the [internal] market."); *see also* Case C-209/10, Post Danmark A/S v Konkurrencerådet, 2012 EU:C 172; Case T-228/97, Irish Sugar v Commission, 1999 EU:T 246; Case C-457/10 P, AstraZeneca v Comm'n, 2012 EU:C 770.

71. It is submitted that the distinction between ex ante regulation and ex post competition law is frequently overstated in the policy debates surrounding the regulation of "Big Tech." For instance, as Pierre Larouche and Alexandre de Streel have pointed out, "[m]uch of EU competition law is really *ex ante*, from merger control to the use of guidelines, notices, block exemptions, etc., up to and including many Article 102 TFEU cases, which are decided before the impugned conduct has fully produced its actual effects . . . . [I]t is not so much the timing of the analysis and the remedy—as the *ex ante* versus *ex post* distinction suggests—that really disqualifies competition law enforcement in the eyes of the Commission; rather, the duration of competition law procedures is what makes it seem as if competition law is always running behind market developments." Pierre Larouche & Alexandre de Streel, *The European Digital Markets Act: A Revolution Grounded on Traditions*, J. EUR. COMPETITION L. & PRACTICE, 7–8 (2021), https://ssrn.com/abstract=3911361; Heike Schweitzer, *The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What Is Fair: A Discussion of the Digital Markets Act Proposal*, *forthcoming in* Zeitschrift für Europäisches Privatrecht 2021, Issue 3, n.111 ("both, competition rules and the rules foreseen in the DMA are ex ante rules. The difference lies in the degree of specification ex ante.").

72. DMA, *supra* note 6, at 40–41.

73. *Id.* at 39–41; *supra* Part II.A (stating that refraining from more favorably treating services provided by the gatekeeper or third-party affiliates protects competition, protecting consumer privacy is served by the obligation to refrain from combining personal data with personal data from third party sites, and the obligations as a whole provide a uniform set of protections for the entire EU system).

processing, combination, sharing, or access to data.[74] For example, *gatekeepers* are placed under the obligations to refrain from self-preferencing[75] and from imposing technical restrictions on end users' ability "to switch between […] different software applications and services to be accessed using the operating system of the gatekeeper."[76] Equally, *gatekeepers* must allow end-users to uninstall "pre-installed software applications on its core platform service" that are not essential to the functioning of the OS or device or cannot be offered independently by third parties.[77]

This paper will focus on the six *gatekeeper* obligations in the DMA that are specific to *data*. It is submitted that these six obligations fall into one of two broad categories: Firstly, obligations to *grant access* to data (including for the purposes of data sharing and portability), and, secondly, obligations to *limit* the collection, combination, and use of data. As the below six subsections will show, the obligations imposed by the DMA contain ambiguities in relation to key terms or requirements which risk undermining legal certainty for *gatekeepers* and other market actors, thereby potentially limiting the DMA's efforts to improve the contestability of digital markets and to fuel innovation by providing more data inputs to non-gatekeepers.

Some may assume that gatekeepers—when in doubt—will err on the side of caution and resolve the ambiguities described in this paper in favor of *overcompliance*.[78] However, this view neglects *gatekeepers*' business models and the economic reality to which gatekeepers as *for-profit* commercial entities are subject.[79] For instance, while the fines imposed under the DMA may seem significant, their damage to gatekeepers may be overshadowed by the competitive advantages and profits these companies can derive from their exclusive access to certain sets of data.[80] It may therefore be naïve to think that gatekeepers will resort to overcompliance just so as to avoid closer scrutiny of their practices by the Commission under the DMA.[81] It is arguably more likely that gatekeepers will try to use ambiguous terms in the DMA as loopholes to avoid sharing data with their competitors and business users.[82]

---

74. *See, e.g.*, DMA, *supra* note 6, at 39–40 (obligating gatekeepers to avoid discouraging business users from raising issues with public authorities and self-preferencing).

75. *Id.* art. 6(1)(d) ("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 . . . .").

76. *Id.* art. 6(1)(e).

77. *Id.* art. 6(1)(b).

78. *See, e.g.*, House of Lords Select Committee on Communications and Digital, *Uncorrected Oral Evidence: Freedom of Expression Online* (Mar. 9, 2021) – Evidence Session No. 16, Questions 125–132, 12 https://committees.parliament.uk/oralevidence/1869/pdf/ (discussing an assumption of overcompliance by platform operators if statutory liability is imposed on them for third party action).

79. *See id.* (assuming overcompliance by platform operators if statutory liability is imposed on them for third party action).

80. DMA, *supra* note 6, at 50–51; *see also* Andrei Hagiu & Julian Wright, *When Data Creates Competitive Advantage*, HARV. BUS. REV. (Jan.-Feb. 2020), https://hbr.org/2020/01/when-data-creates-competitive-advantage (discussing competitive advantages to companies with data access).

81. *See* Borgogno & Colangelo, *supra* note 23, at 13 (recognizing the strong commercial incentives to share as few data as possible with third parties and the strong risk that gatekeepers could design systems subtly designed to prevent full interoperability with competitors' interfaces).

82. *Id.*

It should also be noted that the DMA contains a limitation on the imposition of measures in relation to *gatekeepers* in *Member State law* that have "the purpose of ensuring contestable and fair markets" and exceed the obligations set by the DMA.[83] Thus, under the DMA, Member States will be precluded from "impos[ing] on gatekeepers further obligations by way of laws, regulations or administrative action for the purpose of ensuring contestable and fair markets."[84] The DMA also provides that "[n]ational authorities shall not take decisions which would run counter to a decision adopted by the Commission under [the DMA]."[85] Whether or not these provisions are likely to limit the fragmentation of the regulatory landscape across EU Member States will be discussed in Part III.D. of this paper.[86] Of note, Article 1(6) DMA provides a broad and explicit carve-out for EU *and* national (Member State) *competition law*. For example, the DMA is without prejudice to Articles 101 and 102 of the Treaty on the Functioning of the European Union ("TFEU") and their national equivalents "prohibiting anticompetitive agreements, decisions by associations of undertakings, concerted practices and abuses of dominant positions."[87] The DMA is also without prejudice to "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" to those imposed by the DMA.[88] With that in mind, the below subsections will discuss the DMA's six data-related obligations imposed on *gatekeepers* and the ambiguities they may give rise to.

3. Data Access, Sharing and Portability Obligations

a. Facilitate Data Portability by End Users

Per Article 6(1)(h) DMA, *gatekeepers* must "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 […the GDPR], including by the provision of continuous and real-time access."[89] In the words of the DMA, this is to facilitate "switching or multi-homing" which, in turn, could "lead […] to an increased choice for […] users and an incentive for gatekeepers and business users to innovate."[90]

The reference to the GDPR is instructive. The right to data portability is explicitly recognized in Article 20 GDPR, which gives data subjects "the right to receive the personal data concerning [them…], which [they…have] provided to a controller, in a structured, commonly used and machine-readable format and […] to transmit those data to another controller without hindrance,"[91] where the

83. DMA, *supra* note 6, at 34.
84. *Id.*
85. *Id.*
86. *See infra* Part II.
87. DMA, *supra* note 6, at 34.
88. *Id.*
89. *Id.* at 40.
90. *Id.* at 27.
91. *See also* GDPR, *supra* note 39, recital 68 (addressing the right to data portability).

processing of such data was based on the data subject's consent[92] or was necessary for performance under a contract to which the data subject is a party.[93] Thus, the DMA does not *create* the right to data portability in EU law. Rather, the DMA makes two key additions to the right of data portability in EU law.[94] It widens this right to cover the data of business users and closes a gap which the GDPR left open, namely, *how* access to data for the purposes of portability should be provided.[95]

With regards to the widening of the right to data portability, the DMA now provides for a portability of data generated through the activities of both end users and *business* users, whereas the right to data portability in the GDPR was limited to personal data of private persons, by virtue of the scope of "data subjects" in the GDPR.[96] Furthermore, the *right to data portability* in the GDPR was limited to data which the data subjects "provided to a controller," whereas the DMA gives a right to portability of data "generated through the activity of […] user[s]."[97] This becomes apparent in recital 54 DMA, which lists both data which users "provided *or* generated in the context of their use of" the gatekeeper's service, requiring that users be given "effective and immediate access" to *both* types of data.[98] This distinction is important because the "generated" data definition arguably encompasses data which was not provided by users to the platform (i.e., their data "input"), but also includes data which the *gatekeeper* was able to generate by way of *inference or contextualization* of such user inputs.[99] This broadens the concept of data portability beyond the mere facilitation of users' ability to smoothly port a copy of "their" data, which they would potentially be capable of replicating an infinite number of times by providing the same inputs to a *gatekeeper's* competitors, to now also include the portability of data which users *cannot* themselves replicate and provide to other companies, since such data has been generated using the input data provided by the users as a basis, but differing from it.[100]

This recognition is important because even some specialized competition courts in Europe, such as the Cartel Senate of the Düsseldorf Higher Regional Court hearing an appeal against the German Cartel Office's *Facebook*

92. *Id.* arts. 6(1)(a); 9(2)(a).

93. *Id.* art. 6(1)(b).

94. *See* Borgogno & Colangelo, *supra* note 23, at 6 (pointing out albeit in relation to data *portability* under Art.20(1) GDPR rather than pure access that the GDPR merely requires the data to be transmitted in a "structured, commonly used and machine readable" format, but does *not* "mandate the adoption of interoperable standards." For example, they observe that the simple "encouragement" in Recital 68 GDPR to adopt interoperable standard is not binding. Overall, the authors observe that this lack of standardization "is likely to raise serious concerns on effectiveness and legal certainty," potentially rendering the portability rights at issue ineffective in practice).

95. *Id.*

96. *Compare* GDPR, *supra* note 39, at 39–47 ("Rights of the data subject"), *with* DMA, *supra* note 6, at 40 (obligating gatekeepers to "provide effective portability of data generated through the activity of a business user or end user.").

97. GDPR, *supra* note 39, at 13; DMA, *supra* note 6, at 40.

98. DMA, *supra* note 6, at 27 (emphasis added).

99. *Id.* at 27 ("data [users] provided or generated in the context of their use of the relevant core platform services of the gatekeeper . . . .").

100. *Id.*

decision,[101] have refused to accept enforcers' data-related theories of harm on the basis that consumers could provide their data for an unlimited number of times to any third-party social network operator, including to a gatekeeper's competitors[102]—neglecting the fact that gatekeepers can derive competitive advantages from *inferred* data which consumers *cannot* replicate.[103] The portability of data—including inferred data—through real-time access under the DMA arguably addresses this issue, which may recalibrate data relations in favor of both end users and business users of gatekeepers' services.[104] This may give business users access to data relevant to competition, without which they cannot effectively contest digital markets in which gatekeepers are present.[105]

However, this recalibration of data relations in favor of business users has its limits. For instance, with regards to the DMA's clarifications on *how* data portability is to be facilitated, the key addition made by Article 6(1)(h) DMA to the status quo (i.e., end users' ("data subjects'") right to data portability under the GDPR) is that the exercise of data portability is to be facilitated through "the provision of continuous and real-time access" to data generated through users' activity.[106] In particular, recital 54 posits that the data is to be provided by the gatekeeper "in a structured, commonly used and machine-readable format" and that, to ensure that users can port their data "in real time effectively," for example "high quality application programming interfaces" (APIs) could be used.[107] Of note, the portability obligation of the DMA also covers "any other data at different levels of aggregation that may be necessary to effectively enable such portability."[108] By contrast, the GDPR merely requires controllers to transmit data provided by the users "directly from one controller to another, *where technically feasible*," leaving open when exactly this would be the case.[109] Against this background, the DMA's instructions on the required portability mechanisms are arguably a step forward, allowing more effective exercises of data portability rights by users.[110]

However, the DMA does not provide for a *standardization* of the data format or the mechanisms to be used by gatekeepers for the mandatory sharing

101. Bundeskartellamt [Federal Cartel Office] Feb. 6, 2019, B6-22/16 – translation at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

102. Oberlandesgericht Düsseldorf [Higher Regional Court of Düsseldorf], Aug. 26, 2019, VI-Kart 1/19 (V) translation at https://www.d-kart.de/wp-content/uploads/2019/08/OLG-D%C3%BCsseldorf-Facebook-2019-English.pdf.

103. For example, through the contextualization of such data (i.e., setting it in relation with data provided by other users or generated from a user's interaction with the gatekeeper's service), and through a gatekeeper's superior inference capabilities (e.g., higher-quality, "trained" algorithms).

104. *See* DMA, *supra* note 6, at 27 (imposing obligations on gatekeepers to provide additional data access to end users while reducing the gatekeepers' exclusive control over that data).

105. *Id.* (providing end users free access to the performance measuring tools of the gatekeeper would enhance fairness, transparency, and contestability of online advertising services).

106. *Id.* at 40.

107. *Id.* at 27.

108. *Id.*

109. GDPR, *supra* note 39, at 13 (emphasis added).

110. DMA, *supra* note 6, at 40.

of data under the DMA.[111] Obviously, there may be good reasons for this. After all, a fixed standardization carries the risk of locking in a standard that may become outdated over time and of raising compliance costs.[112] However, this risk could arguably be addressed by the inclusion of a provision that would allow the Commission or a separate designated body to regularly revise the standardized formats and mechanisms to reflect the state of the art at a particular point in time.[113]

In any case, two things are worth pointing out about what the current lack of standardization means for the DMA. Firstly, gatekeepers may "try to comply in autonomous and non-standardized ways" with their data obligations under the DMA, "thereby ultimately precluding a sound free flow of data within the Internal Market."[114] For instance, if gatekeepers share the data through APIs which are "designed […] to prevent full interoperability with competitors' interfaces," the procompetitive effects of the DMA's data sharing provisions for business users may actually be very limited in practice.[115] This is a likely development, since gatekeepers have "strong commercial incentives to share as few data as possible with third parties"[116] to preserve their data-derived dominance in the relevant markets. Secondly, even if the APIs were designed by gatekeepers in good faith to effectively comply with the DMA's data sharing requirements, the data provided through them may be of limited utility to the business users receiving the data, if their format (which, in turn, may affect their scope) is left undefined.[117] Among other things, this is due to three types of reasons, summarized by *Gal and Rubinfeld* as "metadata uncertainties," "obstacles to data transformation," and "missing data."[118] For instance, due to diverging or suboptimal formats, the shared data may lack the context needed to derive utility and value from it, or the costs of a combination of the accessed data into "coherent datasets" may be so high as to preclude its use by smaller business users in the first place.[119] As pointed out by *Gal and Rubinfeld*, APIs do not solve the problems relating to the "data transformation" and "missing data" elements.[120] Overall, the lack of standardization provisions under the DMA's data sharing provisions may therefore limit the practical procompetitive

111. Even the use of APIs is merely listed as an "example" rather than a strict obligation under the DMA, and only appears in recital 56, rather than Art. 6(1)(h) DMA itself.

112. *See* Gal & Rubinfeld, *supra* note 23, at 753 (pointing out the "risk of lock-in to an inefficient standard" and the possibility of high compliance costs).

113. *Id.*

114. Borgogno & Colangelo, *supra* note 23, at 13.

115. *Id.*

116. *Id.*

117. *See* Jef Ausloos et al., *Getting Data Subject Rights Right*, 10 JIPTEC 283, 283–309 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544173 (discussing the idea that modern "data systems collect such a large number of data points, that only a format that allows the data subject to analyze the data themselves will allow them to have sufficient oversight over the data processing being undertaken" and stating the chosen format may exclude some of the metadata which the gatekeeper has access to, but that may be "lost," or cut out, during the conversion into the format of provision to business users under Art. 6(1)(h) DMA).

118. *See* Gal & Rubinfeld, *supra* note 23 at 737–70 and 747–49 (summarizing reasons for APIs' limited utility).

119. *Id.* at 748–49 (acknowledging the rising costs associated with combining data into coherent datasets that has also affected large companies like Amazon).

120. *Id.* at 750.

benefits that could otherwise stem from a sharing of data relevant to competition, as required under the DMA.[121]

b. Provide Access to Engagement Data to Business Users

Article 6(1)(i) DMA requires gatekeepers to:

> [P]rovide 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 […GDPR].[122]

This obligation is particularly interesting in that it gives business users the right to access data which were generated not only in the context of their own interaction with a gatekeeper's platform, but also to the data generated by *end users* who engage with business users' offering on such platform.[123] It is submitted that one possible explanation of the DMA's creation of business users' right to access data generated by end users' interaction with a platform is that this would be reasonable in light of the *contractual relations* between business users and end users underlying the use of the platform.[124] However, if this was the case, it would be unclear why recital 55 requires that gatekeepers ought to "enable business users to obtain consent of their end users for […] data access and retrieval, where such consent is required under […the GDPR and the Directive on Privacy and Electronic Communications]" and why *gatekeepers* are barred from providing access to personal data of end users to private users,

121. The same is true for limits on data portability exercisable by data subjects under the GDPR, in the sense that a lack of standardization of the data that can be ported to a platform's competing providers leads to high switching costs for users, who will lose out on functionality, since the new operator will not be able to make full use of the data, with some relevant data even missing. Gal & Rubinfeld, *supra* note 23, at 752.

122. DMA, *supra* note 6, at 40.

123. *Id.*

124. Alexandre de Steel, *Digital Markets Act: Making Economic Regulation of Platforms Fit for the Digital Age*, CTR. ON REGUL. EUR. 12–14 (Nov. 2020).

unless end users "opt[…] in to such sharing."[125] In other words, the combination of these two DMA provisions assumes that gatekeepers will sometimes lawfully hold personal data about end users which they can only share with business users if the relevant end users *consent* to such sharing, leaving out the possibility of lawfully sharing personal data on bases other than consent, such as if business users asserted that they needed access to such personal data for the performance of their wider obligations under a contract.[126]

Interestingly, while recital 55 provides that gatekeepers "should enable business users to obtain consent of their end users for […] data access and retrieval, *where such consent is required* under […the GDPR and the E-Privacy Directive]," [127] Article 6(1)(i) does *not* appear to allow for data transfers unless users *opt in* "to such sharing with a *consent* in the sense of the […GDPR]," [128] leaving out the other options for a lawful processing of the data, such as business users' need to access the data for the performance of their contractual obligations, which may appear implied by the recital's words "where such consent is required." [129] This ambiguity could undermine the legal certainty of the obligation in Article 6(1)(a) and may lead to gatekeepers continuing to refuse access to the types of user data covered by this provision on the basis of a lack of consent, or the inability to obtain the latter.[130] Such refusals would be especially unsurprising considering the widespread practice of platforms and other actors in the digital economy citing third parties' rights to privacy or the protection of personal data under the GDPR to refuse data access that is actually legitimate (for example, covered by the research exemption of the GDPR).[131] Additionally, the standardization-related observations made in relation to the requirement of Article 6(1)(h) DMA apply,[132] potentially limiting the practical utility of the engagement data accessed by business users under Article 6(1)(a).

c. Provide Search Data to Competing Search Engines

Article 6(1)(j) of the DMA requires that *gatekeepers* who offer online search services:

> [P]rovide […] 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

125. DMA, *supra* note 6, at 27.
126. *See generally* Alexandre De Steel, *supra* note 124, at 1–12 (discussing gatekeeper functions).
127. DMA, *supra* note 6, at 27.
128. *Id.* at 40.
129. *Id*. at 27.
130. *See* Jef Ausloos & Michael Veale, *Researching With Data Rights*, TECH. & REGUL. 136, 145 (2020) (discussing the issues with data access based on affirmative consent).
131. GDPR, *supra* note 39, at 84–85.
132. DMA, *supra* note 6, at 40.

> anonymisation for the query, click and view data that constitutes personal data.[133]

The requirement in Article 6(1)(j) arguably goes further than any other obligation in the DMA with regards to data-fueled competition in digital markets.[134] In essence, Article 6(1)(j) forces gatekeeper search engine providers to share their "ranking, query, click and view data"—crucial data generated by end users' interaction with a search engine which is key to the development of high-quality search engines—with their *competitors*.[135] As an *ex ante* measure, it is imposed without the need to show any abusive conduct on the part of a *gatekeeper* search engine provider, relying solely only on its designation as a "gatekeeper."[136] An interesting parallel to the triggering of this obligation by a designation as *gatekeeper* is the *special responsibility of dominant undertakings* "not to allow [their] behaviour to impair genuine undistorted competition on the internal market" triggered by companies' status as "dominant undertakings" pursuant to Article 102 of the Treaty on the Functioning of the European Union (TFEU) as interpreted by the Court of Justice of the European Union (CJEU) under EU competition law.[137] However, the obligation imposed on dominant undertakings by virtue of their *special responsibility* differs from the highly specific *ex ante* obligations in the DMA to grant other companies access to data, among other things, due to the conduct element required to trigger liability.[138] Such conduct may be difficult to prove under the current competition law framework. For instance, there is a very high threshold to show that data collected and processed by a gatekeeper constitutes an "essential facility," access to which is indispensable for competition,[139] so that denying competitors such access would constitute an abuse of dominance under Article 102 TFEU.[140] Article 6(1)(j) may help to significantly lower this threshold.

Importantly, the data access requirement of Article 6(1)(j) is subject to an *anonymization of personal data* by the gatekeeper.[141] While a plain reading of the anonymization requirement may suggest that it is intended to merely ensure compliance with the protection of personal data under the GDPR and, therefore,

---

133. *Id.* at 41.

134. *Id.* (requiring a gatekeeper to provide data access upon reasonable request).

135. *Id.*

136. *Id.*

137. Case C-209/10 *Post Danmark A/S v Konkurrencerådet*, EU:C:2012:172, ¶ 23; *see also* Case 322/81 *Nederlandsche Banden Industrie Michelin v Commission*, EU:C:1983:313, ¶ 57 (discussing dominant undertakings); Case T-228/97 *Irish Sugar v Commission*, EU:T:1999:246, ¶ 112 (discussing dominant position); Case C-457/10 P *AstraZeneca v Commission*, EU:C:2012:770, ¶ 134 (regarding dominant positioning).

138. *See* Schweitzer, *supra* note 15 ("both competition rules and the rules foreseen in the DMA are ex ante rules", the latter have a higher "degree of specification ex ante").

139. Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftverlag GmbH & Co. KG and others* ECLI:EU:C:1998:569 ¶24, 41. *See also* Joined Cases C-241/91 P and C-242/91 P *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission* ECLI:EU:C:1995:98 ¶ 48–57 (discussing essential functions).

140. *Id.*; Borgogno & Colangelo, *supra* note 23, at 11–12.

141. *See* DMA, *supra* note 6, at 41 ("subject to anonymization for the query, click and view data that constitutes personal data"); *The eData Guide to GDPR: Anonymization and Pseudonymization Under the GDPR*, JDSUPRA (Dec. 9, 2019), https://www.jdsupra.com/legalnews/the-edata-guide-to-gdpr-anonymization-95239/.

would allow for a redaction of all personal data before access is given to competitors, recital 56 indicates that the requirement is more complex than this. Recital 56 requires gatekeepers to "ensure the protection of the personal data of end users by appropriate means, without *substantially degrading the quality or usefulness of the data*."[142]

It is submitted that the term "[without] substantially degrading the quality or usefulness of the data" is highly ambiguous and confuses more than it helps to understand the requirement in Article 6(1)(j). For instance, it is unclear and left unexplained just *how much* of a degradation in quality or usefulness would constitute *substantial* degradation for the purposes of Article 6(1)(j).[143] In fact, it is unclear in the first place how the "usefulness" of data relating to a person can be left "substantially undegraded" by an *anonymization* of said data, depending on the use that competing search engines as recipients of said data would make of it. This is because the standard against which the degradation is to be assessed is left unexplained, and a plain reading of the requirement would arguably suggest that degradation of the data is to be assessed against the quality and utility of the still-personal data held by the gatekeeper. Against this standard, any anonymization could be said to *substantially degrade* its quality. Arguably, the practical result of this ambiguity will be that gatekeepers will seek to strike a balance between the two extremes so as to keep their conduct outside the scope of obvious violations that would make it worthwhile for the Commission or the competent national data protection authorities to closely scrutinize a set of data (not) provided by a particular gatekeeper. One may only hope that enforcers' expectations will be teased out more clearly by future investigations and CJEU case law, should this balance be difficult for gatekeepers to strike or should the Commission and the national data protection authorities come to demand conflicting or incompatible standards of non-degradation of data and anonymization of data, respectively. It should be pointed out, however, that the problem of striking a balance between sufficient anonymization to protect personal data and not degrading the data to an extent that will make it lose its value and practical utility for the recipients of such data under a mandatory sharing provision has been known for some time, and several solutions have been suggested for this problem. For instance, Graef and Prufer[144] acknowledged this problem (albeit in the context of the right to data portability under the GDPR) but noted that synthetic data,[145] data vaccination,[146] or data

142. DMA, *supra* note 6, at 27–28 (emphasis added).

143. *See id.* (lacking any specificity as to what would constitute substantial degradation).

144. Inge Graef & Jens Prufer, *Governance of Data Sharing: A Law & Economics Proposal*, TILEC Discussion Paper No. 2021-001 (January 2021), https://ssrn.com/abstract=3774912.

145. *Id.* at 14 n.37 ("[A]n artificial (synthetic) data set is created that has the same aggregate characteristics as the original to-be-shared data set. However, as the shared data set is artificial, no real individuals can be re-identified. It seems that, with synthetic data, the value that can be derived from cross-section analyses of the original data set can be maintained. However, the time-series value, which stems from knowing what user X liked in the past when serving her in the present, cannot be transferred to receiving firms in this way.").

146. *Id.* (presenting data vaccination as an "alternative solution," whereby "content and personal identifiers are split and saved in different databases, which are only brought together again when an application is run.").

pooling[147] may provide "(imperfect) solution[s]" to it.[148] These solutions—however limited—have not been picked up by the DMA at all, leaving an ambiguity as to the appropriate standard of balancing anonymization with non-degradation of the utility of data instead.[149] Of course, it is possible that the Commission will issue guidelines following the passing of the DMA which will make suggestions as to the appropriate mechanism for the sharing of data. This may also be teased out by future CJEU case law, should disputes on the appropriate standard of anonymization or non-degradation in a particular case arise in the future.[150] The reference to a degradation of the "usefulness" of anonymized data in the DMA is also interesting because the "usefulness" of data necessarily depends on the *use* that will be made of it.[151] Thus, it is unclear whether gatekeepers would need to assess the "use" by a *business user* requesting access to such data before granting them access, or whether business users are required to provide the context for such assessment themselves (i.e., informing about the potential uses of such data).[152] The DMA leaves this question unaddressed, placing the burden of predicting such uses and of striking an appropriate balance between anonymization and preserving usefulness and quality on gatekeepers.[153] It is submitted that the ambiguity of this requirement may undermine legal certainty, since gatekeepers may lack a clear understanding of what is required from them to ensure compliance with the Article 6(1)(j), while at the same time ensuring compliance with the GDPR.[154] This risks limiting the practical utility of the access requirement in Article 6(1)(j) as an *ex ante* measure in facilitating the contestability of EU-wide online search markets.[155] Furthermore, as will be discussed in Part IV of this paper, the broad phrasing of the obligation in Article 6(1)(j) ("any third party providers") means that other *gatekeepers* that do not currently offer a search service could rely on it to obtain search data from another gatekeeper, so as to expand their dominance in adjacent markets into the online search market.[156] This may make gatekeepers, rather than small online search providers the biggest beneficiaries of the obligation in Article 6(1)(j).[157]

147. *Id.* at 15 ("Data pooling is an alternative to the direct sharing of data. Here, the data is pooled by a central actor (e.g., the competent authority) 'behind a curtain' . . . offer[ing] firms with a right to 'receiving' the shared data to send their ML-algorithms to the pool and let them be trained there.").

148. *Id.*

149. *See generally* DMA, *supra* note 6.

150. *See generally At A Glance: De-Identification, Anonymization, and Pseudonymization*, BRYAN CAVE LEIGHTON PAISNER LLP (Feb. 28, 2016), https://www.bclplaw.com/en-US/insights/at-a-glance-de-identification-anonymization-and-pseudonymization.html (discussing the unclear standards on anonymization); Sebastiao Barros Vale, *Upcoming Data Protection Rulings In the EU: An Overview of CJEU Pending Cases*, FUTURE OF PRIVACY FORUM (Sep. 15, 2021), https://fpf.org/blog/upcoming-data-protection-rulings-in-the-eu-an-overview-of-cjeu-pending-cases (discussing upcoming cases).

151. DMA, *supra* note 6, at 27–28.

152. *Id.*

153. *Id.*

154. *Id.* (showcasing that the DMA does not set forth how to properly balance compliance).

155. *Id.* at 41.

156. *See infra* Part IV.

157. *See infra* Part IV (providing a more detailed discussion of why gatekeepers may, at the same time, be the biggest beneficiaries and losers of the data access and sharing obligations in the DMA).

4. Limitations on Data Processing

a. Refrain from Using Non-Public Data in Competition with Business Users

Article 6(1)(a) DMA requires *gatekeepers* to:

> [R]efrain from using, in competition with business users, any data not publicly available,[158] 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.[159]

The idea behind the obligation in Article 6(1)(a) DMA is simple. It is meant to prevent gatekeepers from taking "advantage of [their] dual role to use data, generated from transactions by [their] business users on the core platform, for the purpose of [their] own services that offer similar services to that of [their] business users."[160]

However, the obligation in Article 6(1)(a) is striking in that it places a limitation on the *uses* that a gatekeeper can make of data that it already lawfully *possesses*.[161] For instance, Article 6(1)(a) does not use the word "processing" when expressing its prohibition, but rather relies on the term "*using*, in competition with business users."[162] This distinction between "processing [data]" and "using [data] in competition" is important because—against the background of Article 6(1)(a)—it allows gatekeepers to collect, process, and transfer[163] data which is *capable* of being used in competition with business users but does not allow gatekeepers to *actually use* such data in competition with business users.

This raises the question of what exactly is meant by the ambiguous term "in competition with business users" and just how broad an interpretation of "in competition" will be adopted by enforcers, since this will determine the scope of the prohibition in Article 6(1)(a) DMA.[164] For example, a narrow reading of "in competition with business users" would arguably include reliance on such data for *actual* competition in markets where business users already compete

158. DMA, *supra* note 6, at 40 ("Data that is not publicly available" includes "any aggregated and non-aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers on the core platform service of the gatekeeper.").

159. *Id.*

160. *Id.* at 24.

161. *Id.* at 40.

162. *Id.*

163. *See generally* GDPR, supra note 39 (addressing the "processing" of data but not "use").

164. DMA, *supra* note 6, at 40.

with the gatekeeper in question.[165] Whereas a broad reading of "in competition with business users" could, for example, also include *potential* competitors in adjoining markets, and, maybe, even the development of data-reliant products for a future commercialization on such markets.[166] In the absence of a clarification on how broad the scope of the prohibition in Article 6(1)(a) will be, gatekeepers may therefore be deprived of the legal certainty they need to comply with this requirement.[167]

Another interesting feature of Article 6(1)(a) is that it only prohibits the use of "data not publicly available," which is defined in Article 6(2) as including "any aggregated and non-aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers on the core platform service of the gatekeeper."[168] The fact that the limitation of Article 6(1)(a) includes data that a gatekeeper *infers* from the engagement of users with its platform is important because it may lead to two very different outcomes.[169] On the one hand, it could disincentivize gatekeepers' processing of user data for the purpose of gaining a competitive advantage over business users who a gatekeeper may wish to start to compete with.[170] In this outcome, the problematic implications would probably be limited to the risk of disincentivizing the development of innovative algorithms required for the evaluation of such data, as well as a waste of economic utility and value of such data.[171] Furthermore, a loss of economic efficiency may result from lower levels of information available on the users of a platform and the transactions they engage in.[172]

However, there is another, less apparent, outcome that the prohibition in Article 6(1)(a) could have.[173] Gatekeepers may decide to *make public* the data they wish to rely on in competition with (some of) its business users, so as to fall outside the scope of Article 6(1)(a) and continue to rely on such data in the course of their trade.[174] At first sight, such an outcome may appear attractive from a competition point of view.[175] After all, it would give competing business users access to large parts of the same data the *gatekeepers* use to contest the market in question.[176] However, it is submitted that this perspective is misleading. There is nothing in the DMA requiring gatekeepers to share their superior *analytical capabilities* (nor the context of the data) with their

165. *Id.*
166. *Id.*
167. *Id.*
168. *Id.* at 41.
169. *Id.* at 40–41.
170. Michal S. Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, J. COMPETITION L. & ECON. (forthcoming 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444.
171. *Id.* at 3 ("limitations on data sharing could thus prevent the emergence of better data-based products or services, and could reduce firm's ability to develop and fine-tune new algorithms".).
172. *Id.* ("legal limitations on data collection, processing, and use could *prevent firms from obtaining the data necessary for their operations*.").
173. DMA, *supra* note 6, at 40.
174. *Id.* ("a gatekeeper shall: refrain from using, in competition with business users, any data not publicly available . . . .") This may open the door to make data public for the purpose of using it "in competition."
175. Gal & Aviv, *supra* note 170, 175–77 (discussing potential effects on competition).
176. DMA, *supra* note 6, at 40.

competitors, which means that they can make much better and effective *use* of any set of data they make public.[177] Furthermore, Article 6(1)(a) DMA leaves open the *format* in which the data is to be made publicly available since it does not posit that data will only be considered publicly available if it is presented in a way that allows other entities to make any meaningful use of it.[178] Additionally, it is thinkable that, instead of relying on the data to *compete* with business users, gatekeepers will—subject to the required approvals under the EU Merger Regulation (EUMR)—rely on such data to make informed decisions about *acquiring* some of its most innovative business users.[179] This would not offer any benefits to consumers, but rather deprive them of the already limited choice they would otherwise have, while further strengthening the gatekeepers' positions in the market.[180]

Overall, it is unclear whether the limitation in Article 6(1)(a) will actually fulfil its goal of preventing gatekeepers from taking "advantage of [their] dual role to use data, generated from transactions by [their] business users on the core platform, for the purpose of [their] own services that offer similar services to that of [their] business users."[181] It appears that the effectiveness of Article 6(1)(a) may be greatly enhanced through the provision of guidance on the interpretation of the term "in competition with business users"[182] and on the introduction of (updateable) standard requirements for data and the means of their provision. Otherwise, it cannot be excluded that gatekeepers will make such data public in a format limiting their usefulness, or by inefficient means, while avoiding the DMA's prohibition on using such data "in competition with business users."[183]

b. Refrain from Combining Personal Data from Different Services

Article 5(a) of the DMA requires gatekeepers to:

> [R]efrain from combining personal data sourced from […] 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 [the GDPR].[184]

177. *See generally id.* (making no provision to share analytical skills, only data).

178. *See infra* Part II.B.iii.a (stating the importance of data standardization for effective procompetitive data sharing regimes).

179. DMA, *supra* note 6, at 40 (lacking prohibitions on using the subject data for any purpose other than competition).

180. Graef & Prufer, *supra* note 144.

181. DMA, *supra* note 6, at 24.

182. *Id.* at 40.

183. Borgogno & Colangelo, *supra* note 23, at 6.

184. DMA, *supra* note 6, at 39.

The obligation in Article 5(a) builds on existing jurisprudence from the Member States—in particular, Germany—but does so with a twist.[185] For instance, the combination of personal data obtained by platform operators from different sources without giving users a genuine *choice* as to the level of personalization and data-combination they desire was found to be an abuse of dominance under German competition law in the *Facebook* decision of the German Federal Court of Justice ("FCJ").[186] However, as will be discussed in Section III.D.2 of this paper, the *Facebook* decision left open the question as to *how exactly* this personalization choice can be provided.[187] For instance, the FCJ did not elaborate on whether this choice could be given through an *opt-out* during or following a user's registration for the platform service in question, or whether a stricter standard was to apply.[188] In recital 36, the DMA resolves this question in favor of *opt-ins*, which means that users will need to give active and positive consent before they are provided with a more personalized version of a gatekeeper's service that is based on a combination of their data from different sources.[189] In the words of recital 36, *gatekeepers*:

> [S]hould enable their end users to freely choose to *opt-in* to such [combination] business practices by offering a less personalized alternative . . . [this] 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.[190]

It should be pointed out, however, that the requirement of a *proactive, explicit, clear, and straightforward presentation* of a less personalized alternative to a gatekeeper's service is ambiguous.[191] For instance, it could be understood as requiring the simultaneous provision of at least two (or more) personalization-level options during a user's registration for a platform, with the default being set on the *least personalized* option (higher level of data protection), and users "opting in" to data combination and higher personalization by actively selecting a *more personalized* setting (lower level of data

185. *Id.* at 36–38.

186. For an overview and discussion of the German *Facebook* case and its significance for the DMA and its practical effects, *see* Part III.D.2.

187. *See id*.

188. *Id*.

189. DMA, *supra* note 6, at 22.

190. *Id*.

191. Rupprecht Podszun, *Should Gatekeepers Be Allowed to Combine Data? – Ideas for Art. 5(a) of the Draft Digital Markets Act* (June 4, 2021), https://ssrn.com/abstract=3860030.

protection).[192] However, under a more gatekeeper-friendly, broad reading, the requirement could also be interpreted as the provision of a visible notice that a less personalized version of the platform service is available (but with *no* box being pre-selected, and the more personalized box, for example, being the first on the list).[193] Upon an even broader reading of "opt-in," the terms of service visible to users upon registration could contain a visible, highlighted section requiring separate confirmation that users have "read and understood" the section, and providing that users' future registration in any *other* service provided by the same gatekeeper will constitute an "opt-in" to the combination of her data with her future data on the new service, unless the user changes her privacy settings in the primary service of her registration.[194] Gatekeepers could argue that the DMA does not regulate how *exactly* the opt-in is to be provided, so long as it is "proactively presented" (which this highlighted section would be) in an explicit, clear, and straightforward manner (the text of such section could be plain and contain an easily understandable explanation of how to change the settings).[195] However, this ambiguity will probably be easy to fix, for example through the publication of guidelines on the interpretation of this requirement.[196]

Overall, if a *narrow* reading of "opt-in" will be accepted, the requirement in Article 5(a) may become an important tool for the limitation of the data-driven advantages of gatekeepers who would otherwise be able to entrench their dominance and to leverage it on other markets, limiting the contestability of such markets.[197] However, it remains to be seen whether the imposition of the obligation in Article 5(a) is enough to avoid a fragmentation of the single digital market by addressing the concerns expressed by the German Bundeskartellamt (Federal Cartel Office (FCO)) and FCJ, who can continue to rely on the national competition law carveout in the DMA and Regulation 1/2003 in applying stricter concepts of protection against gatekeepers than those provided for by the DMA and EU competition law.[198]

5. Compliance Obligations of Gatekeepers

In addition to the five *specific* data-related obligations imposed on gatekeepers discussed above, the DMA sets out a number of obligations on *gatekeepers* aimed at ensuring compliance with the DMA, as well as obligations regulating gatekeepers' interaction with the Commission.[199]

192. *Id*. at 4.
193. DMA, *supra* note 6, at 39.
194. *Id.*
195. Podszun, *supra* note 191, at 5.
196. *Id*. at 1.
197. *Id*. at 2–3.
198. *See* Bernd Meyring, *Germany's Gatekeeper Rules: The Start of Divergence for Gatekeepers?*, LINKLATERS (Jan. 19, 2021), https://techinsights.linklaters.com/post/102gox7/germanys-gatekeeper-rules-the-start-of-divergence-for-gatekeepers (recognizing the potential for legislative fragmentation because of the overlap between Germany's rules and the DMA).
199. DMA, *supra* note 6, at 41.

a. Data-Related Obligations in Relation to the Commission

Per Article 19(1) of the DMA, the Commission may "request access to data bases and algorithms" and "request explanations" about them by way of a "simple request or […] decision."[200] Recital 69 makes clear that the Commission's right to request access extends to "any relevant […] data, database, algorithm and information necessary to open and conduct investigations and to monitor the compliance with the obligations laid down in […the DMA], irrespective of who possesses the documents, data or information in question, and regardless of their form or format, their storage medium, or the place where they are stored."[201]

Furthermore, *gatekeepers*' planned or actual implementation of measures which the European Commission finds to be ineffective in ensuring compliance with the DMA allow the Commission to *specify* the measures needed to ensure compliance, in a decision adopted within six months from the opening of proceedings.[202] Such measures need to be *proportionate* to the specifics of the gatekeeper and its service, and must follow a communication of preliminary findings to the relevant *gatekeeper* no later than three months from the opening of the proceedings.[203] It remains to be seen how actively the Commission will be in using this provision. However, it is submitted that—if used appropriately—this section could help to resolve many of the ambiguities pointed out in relation to the five specific sections set out above, which could otherwise be interpreted too broadly by the gatekeepers.[204]

Another obligation relating to the processing of data that relates to the Commission is contained in Article 13 DMA.[205] The latter requires that that "[w]ithin six months after its designation […], a gatekeeper shall submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services […],"[206] and that such description ought to be updated annually.[207] Per recital 61, the report should at least include "a description of the basis upon which profiling is performed, including whether personal data and data derived from user activity is relied on, the processing applied, the purpose for which the profile is prepared and eventually used, the impact of such profiling on the gatekeeper's services, and the steps taken to enable end users to be aware of the relevant use of such profiling, as well as to seek their consent."[208] The impact that Article 13 may have on the recalibration of data relations between gatekeepers, the Commission and the public will be discussed in Section III.B. of this paper.

200. *Id.* at 47.
201. *Id.* at 31.
202. *Id.* at 41.
203. *Id.*
204. *Id*.
205. *Id*. at 44.
206. *Id*.
207. *Id*.
208. *Id*. at 29.

b. Other Data-Related Obligations

In line with Article 7(1) of the DMA, any measures taken by *gatekeepers* for the purpose of ensuring compliance with its obligations under the DMA must "be effective in achieving the objective of the relevant obligation[s]"[209] and must comply with the GDPR, the Directive on Privacy and Electronic Communications and any legislation covering "cyber security, consumer protection and product safety."[210] Thus, the obligations in the DMA are not meant to *override* any standards of protection provided to consumers, but rather to provide for more competitive markets while ensuring that existing data and consumer protection standards are *complied with*.[211] Whether and to what extent the DMA is successful in achieving this dual goal is an important question. Some of the data access and sharing obligations involving personal data will make simultaneous[212] compliance with both the sharing and data protection obligations under EU law very difficult.[213]

Furthermore, the DMA addresses consent:

> Where consent for collecting and processing of personal data is required to ensure compliance with this [the DMA…], a gatekeeper […is required by the DMA] to take the necessary steps to either enable business users to directly obtain the required consent to their processing, where required under [the GDPR] and Directive 2002/58/EC, or to comply with Union data protection and privacy rules and principles in other ways including by providing business users with duly anonymized data where appropriate.[214]

The DMA further requires that gatekeepers refrain from making "the obtaining of this consent by the business user more burdensome than for its own services."[215]

In discussing the obligations imposed on gatekeepers by the DMA, it is worth pointing out that the DMA provides for a narrow possibility of *exemptions* from the obligations imposed on *gatekeepers*.[216] Exemptions must be based on an *overriding public interest*, that is, on grounds of public morality, public

209. *Id*. at 41.
210. *Id*.
211. *Id*.
212. See the discussions on the overlaps and tensions between data protection and data sharing obligations in Part II of this paper.
213. See discussion in Part II of this paper on the interaction between the DMA and data protection laws, such as the GDPR.
214. DMA, *supra* note 6, at 43.
215. *Id*.
216. *Id*.

health, or public security.[217] In such cases, the Commission may exempt a *gatekeeper* from the specific obligation in question by way of adopting an *exemption decision* no later than 3 months after a *gatekeeper's* submission of a reasoned request for that purpose.[218] In deciding whether to grant an exemption, the Commission must "ensure a fair balance" between the three public interests and the objectives of the DMA, and "take into account" the "effects on the gatekeeper […] and on third parties."[219]

6. *Consequences of Gatekeepers' Non-Compliance with their Obligations Under the DMA*

A gatekeeper's non-compliance with its obligations under the DMA must be determined by the Commission through the adoption of a "non-compliance decision" pursuant to Article 25(1) DMA.[220] Following a communication of preliminary findings to the gatekeeper—including an explanation of the measures to be taken—the Commission can issue a cease-and-desist order and require the non-compliant gatekeeper to provide it with a "description of the measures [taken] to ensure compliance with the decision."[221]

A gatekeeper covered by a non-compliance decision issued pursuant to Article 25(1) DMA may be required to pay a fine, subject to a limitation period of three years.[222] The amount of the fine will depend on the severity of the non-compliance and the gatekeeper's total annual turnover in the preceding financial year. Generally, acts of non-compliance with the DMA are divided into two categories—conduct leading to the imposition of fines of up to 10%, and conduct leading to the imposition of fines of up to 1% of the total annual turnover.[223] In either of the two categories, the stated percentage is a ceiling, not a floor, so that the amount of the fine may be adjusted downwards depending on the "gravity, duration, recurrence [of the non-compliant conduct], and […where applicable], delay caused to the proceedings."[224] For instance, intentional or negligent violations of the core obligations, such as the ones contained in Articles 5 and 6, or of commitments may lead to the imposition of a fine of up to 10% of a gatekeeper's total annual turnover.[225] Whereas fines of up to 1% of the total annual turnover may be imposed for violations such as failures to provide required (complete and correct) information or notices to the Commission.[226] Fines of up to 1% may also be imposed for failures "to provide access to data-bases and algorithms pursuant to Art. 19 [DMA]."[227]

217. *Id.* at 42–43.
218. *Id.*
219. *Id.*
220. *Id.* at 49.
221. *Id.*
222. *Id.* at 51.
223. *Id.* at 50.
224. *Id.*
225. *Id.*
226. This includes the provision of information pursuant to DMA Articles 3(2), 12, 13, 19, 20 and 21.
227. DMA, *supra* note 6, at 50.

The Commission may also impose periodic penalty payments of up to 5% of the average daily turnover from the date of the decision, so as to compel gatekeepers to meet their obligations under Articles 16(1) (decisions imposing behavioral and structural remedies), 19 (requests for information), 21 (on-site inspections by the Commission), 22(1) (interim measures in urgent cases with a "risk of serious and irreparable damage for […] users"), 23(1) (commitments binding on the gatekeeper), and 25(1) DMA (non-compliance decisions).[228]

III. FOLLOW THE DATA: HOW THE DMA RECALIBRATES DATA RELATIONS IN THE EU

The explanatory memorandum to the DMA states that the DMA is "coherent with the proposal for a Digital Services Act […,] the Commission's digital strategy […and] the targeted […] ex ante regulation of specific sectors…."[229] It also states that the DMA "builds on the existing *P2B Regulation*, without conflicting with it" and "complements existing […] competition rules," as well as "the data protection laws" including in the GDPR.[230] However, as noted by Graef et al. in a different context, "where data sharing regimes overlap, their interaction will inevitably lead to questions about how to interpret and implement their respective requirements,"[231] potentially resulting in "spill-overs."[232] This section aims to identify the differences and overlaps between the DMA and existing laws, regulations, and jurisprudence in relation to data in the EU so as to understand whether and how the DMA recalibrates data relations in the EU. It will do so through smaller case studies looking, among other things, at who has access to what types of data under what conditions and how the DMA will change this.

A. Recalibration Against the Background of the P2B Regulation

The P2B Regulation[233] was passed in June 2019 with the aim of promoting "fairness and transparency for business users of online intermediation services."[234] Unlike the DMA, the P2B Regulation is a *symmetric* regulation in the sense that it imposes obligations on *all* online intermediation services "in scope."[235] This distinction stems from the fact that the P2B Regulation is meant to provide for a *basic* level of "transparency and fairness rules applicable to *all*

228. *Id.* at 51.

229. *Id.* at 3–4.

230. *Id.* at 3.

231. INGE GRAEF ET AL., SPILL-OVERS IN DATA GOVERNANCE: THE RELATIONSHIP BETWEEN THE GDPR'S RIGHT TO DATA PORTABILITY AND EU SECTOR-SPECIFIC DATA ACCESS REGIMES 17 (2019), https://ssrn.com/abstract=3369509.

232. *Id.* at 3.

233. Regulation 2019/1150, of the European Parliament and of the Council of 20 June 2019 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services, 2019 O.J. (L 186) 1 (EU) [hereinafter P2B Regulation].

234. *Id.*

235. ALEXANDRE DE STREEL, CTR. ON REGUL. EUR., DIGITAL MARKETS ACT: MAKING ECONOMIC REGULATION OF PLATFORMS FIT FOR THE DIGITAL AGE 10 n.14 (2020) https://cerre.eu/wp-content/uploads/2020/11/CERRE_DIGITAL-MARKETS-ACT_November20.pdf.

online platforms regardless of their size or position,"[236] whereas the DMA seeks to impose *very strict* obligations on a *small* number of core platform services providers (those designated as *gatekeepers*).[237]

In addition to the difference in scope between the two regulations, they differ by the *types* of obligations they impose.[238] For instance, most of the P2B Regulation's obligations relate to *transparency*, that is, they impose duties on online intermediation services to transparently *disclose* whether and how they are engaging in a number of potentially unfair or anticompetitive practices.[239] By contrast, the DMA largely provides for obligations that relate directly to said practices, and require providers classified as gatekeepers to refrain from *engaging* in such practices, rather than just requiring their disclosure.[240] The following example illustrates this difference:

> Providers of online intermediation services shall include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services."[241]

By contrast, the DMA positively requires gatekeepers to *provide* business users with access to such data, subject to appropriate levels of anonymization or end user consent.[242]

In this respect, the most obvious question that will arise in practice is whether a company is to be designated as a *gatekeeper*, thus triggering the stricter obligations of the DMA, or the weaker disclosure obligations of the P2B Regulation.[243] This question is not answered by reference to the overlap between the P2B Regulation and the DMA, but rather by reference to the scope-defining provisions of the DMA itself.[244] Nevertheless, the intertwined scope of the P2B Regulation and DMA mean that companies which *have* been designated as

236. DMA, *supra* note 6, at 3 (emphasis added).

237. *Id.* ("Consistency with existing policy provisions in the policy area" (emphasis added)).

238. *Digital Markets Act: The European Commission Unveils Plans to Regulate Digital 'Gatekeepers'*, CROWELL (Jan. 5, 2021), https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Digital-Markets-Act-The-European-Commission-Unveils-Plans-to-Regulate-Digital-Gatekeepers.

239. P2B Regulation, *supra* note 233, at 68.

240. DMA, *supra* note 6, at 33–34.

241. P2B Regulation, *supra* note 233, at 73.

242. *See* discussion of obligations in Sections II.B.3–6 of this paper.

243. *See* Konstantina Bania, *The Digital Markets Act and Regulation of P2B Relations: Mission Impossible?*, LONDON SCH. ECON.: BLOG (Dec. 14, 2020), https://blogs.lse.ac.uk/medialse/2020/12/14/the-digital-markets-act-and-regulation-of-p2b-relations-mission-impossible (discussing the overlapping authorities of the DMA and P2B).

244. DMA, *supra* note 6, at 36.

gatekeepers will, at the same time, be subject to the obligations set out in the P2B Regulation *and* the DMA, giving rise to an overlap of obligations.[245] While the drafters of the DMA state that the latter "builds on the *P2B Regulation* without conflicting with it," it remains to be seen in practice whether the potentially overlapping obligations in the P2B Regulation and the DMA are sufficiently aligned or separate so as to avoid the risk of undermining legal certainty.[246]

It should be noted, however, that most of the overlaps between the P2B Regulation and the DMA have been intentional.[247] For instance, the drafters of the DMA expect the Commission "in its enforcement of […] obligations" under the DMA to "benefit […] from the transparency that online intermediation services and online search engines have to provide under the P2B Regulation on practices that could be illegal under the [DMA] list of obligations if engaged in by gatekeepers."[248] However, while the P2B Regulation and DMA are regulating in a near-identical policy area, their key enforcement mechanisms differ significantly.[249] For instance, the transparency obligations and provisions on dispute resolution (e.g., through mediation) contained in the P2B Regulation are meant to provide more *effective recourse for business users* vis-à-vis providers of online intermediation services,[250] which they would otherwise be unable to obtain due to their dependency on such providers (fear to jeopardize relations with them), lack of information (addressed by the transparency requirements in the P2B Regulation through both, disclosures and obligations relating to some specific contractual terms)[251] or lack of resources to seek redress through the courts.[252] Thus, the P2B Regulation is focused on actively enabling business users, who are the beneficiaries of the fairness and transparency obligations imposed on online intermediation service providers by the P2B Regulation, and who can exercise constraints on the power of such providers by exercising their rights, including in relation to data disclosure.[253] Additionally, the P2B Regulation tasks *Member States* with the enforcement of said

245. *See* Teresa Rodríguez de las Heras Ballell, *The Scope of the DMA*, VERFASSUNGSBLOG (Aug. 30, 2021), https://verfassungsblog.de/power-dsa-dma-02 (examining potential overlaps in DMA and P2B jurisdiction).

246. *Identification and Assessment of Existing and Draft EU Legislation in the Digital Field*, at 42, AIDA SPECIAL COMM. (Jan. 2022), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf.

247. *See* DMA, *supra* note 6, at 3 (Information on "[c]onsistency with existing policy provisions in the policy area").

248. *Id*.

249. *Compare id.* at 9 (stating a decentralized enforcement mechanism is not optimal) *with* P2B Regulation, *supra* note 233, at 66 (discussing the benefits of allowing entities to seek legal recourse under Member States national law).

250. P2B Regulation, *supra* note 233, at 58, 66.

251. *Id.* at 73 (prohibiting retroactive changes to T&Cs, and requiring that online intermediation service providers' T&Cs include "information on the conditions under which business users can terminate the contractual relationship with the provider of online intermediation services; and include […] a description of the technical and contractual access, or absence thereof, to the information provided or generated by the business user, which they maintain after the expiry of the contract between the provider of online intermediation services and the business user.").

252. *See, e.g.*, *id.* at 65, 74–75 (addressing mediation, dispute resolution, and complaint handling).

253. DMA, *supra* note 6, at 61.

Regulation.[254] Member States can use existing "enforcement systems" for that purpose, so long as the enforcement is "adequate and effective."[255] By contrast, the DMA relies on *centralized* enforcement by the European Commission.[256] Member State authorities and business users are *not* at the center of the enforcement strategy envisaged by the DMA.[257]

These differences may have a practical impact on data relations between business users and gatekeepers in the EU, once (or if) the DMA comes into force.[258] This is because the P2B Regulation's reliance on business users to exercise their rights vis-à-vis online intermediation service providers and Member State authorities' enforcement of the P2B Regulation brings two significant deficits which may undermine the Regulation's practical utility, and which the DMA could potentially solve. Firstly, the reliance on business users carries the risk of *underenforcement* and limited utility of the rights provided to business users under the P2B Regulation, since business users may be reluctant to complain against the behavior of an online intermediation service provider on whom they are *dependent*, with little to no alternatives, out of fear of retaliation or termination of business relations with them.[259] The mediation and complaint measures provided in the P2B Regulation are unlikely to mitigate this fear in any significant way, especially since such retaliation may follow before any complaint or claim is processed, meaning that business users would have to sacrifice a *certain* business relationship in the short term to launch a lengthy complaint with an *uncertain* outcome in the long term.[260] Secondly, the fact that the P2B Regulation leaves enforcement to the Member States with nearly full flexibility on institutional organization increases the likelihood of a *patchwork* of enforcement standards, causing a de-facto fragmentation of the Digital Single Market based on the mechanisms and prioritization of the enforcement of data-related rights under the P2B Regulation.[261] This may diminish the ability of business users in Member States which do not engage in active enforcement in this sphere to make use of their data and information-related rights under the P2B Regulation.[262]

The DMA seems capable of solving both of these problems in relation to business user-gatekeeper relations through its provision of centralized

254. P2B Regulation, *supra* note 233, at 67.

255. *Id*.

256. Press Release, European Parliament, Digital Markets Act: Ending Unfair Practices of Big Online Platforms (Nov. 23, 2021, 10:48 AM), https://www.europarl.europa.eu/news/en/press-room/20211118IPR17636/digital-markets-act-ending-unfair-practices-of-big-online-platforms.

257. *Id*.

258. Konstantina Bania, *The P2B Regulation Is Not Consigned to Oblivion: ACM Launches Market Study, Reminding Us That Transparency in the Platform Economy Is Important*, PLATFORM L. BLOG (Nov. 3, 2021), https://theplatformlaw.blog/2021/11/03/the-p2b-regulation-is-not-consigned-to-oblivion-acm-launches-market-study-reminding-us-that-transparency-in-the-platform-economy-is-important (discussing differences in enforcement between DMA and P2B).

259. *See* ALEXANDRE DE STREEL ET AL., DIGITAL MARKETS ACT: MAKING ECONOMIC REGULATION OF PLATFORMS FIT FOR THE DIGITAL AGE 18, 25, 90 (2020) https://cerre.eu/wp-content/uploads/2020/11/CERRE_DMA_Making-economic-regulation-of-platforms-fit-for-the-digital-age_Full-report_December2020.pdf (discussing smaller platforms' fear of retaliation from large platforms).

260. *Id*. at 90.

261. *Id*. at 76.

262. *Id*.

monitoring and enforcement powers to the Commission.[263] However, this solution raises new questions stemming from the overlap between enforcement under the P2B Regulation by Member States and enforcement under the DMA by the Commission.[264] The DMA does not *replace* the P2B Regulation and its obligations, but rather, is meant to build on it.[265] However, it is conceivable that Member States which will engage in active enforcement under the P2B Regulation will, on some occasions, impose standards of obligations on gatekeepers which are duplicative of the obligations imposed by the Commission.[266] While a duplication of obligations is not necessarily problematic, high levels of coordination between the competent Member State authorities (where they exist) and the Commission must be ensured and clear common goals must be defined to avoid uncertainty and confusion as regards the competencies of the enforcing authorities in any given situation.[267] How well this will work in practice remains to be seen.[268] Overall, however, when considered against the background of the P2B Regulation, the DMA recalibrates data relations between gatekeepers and business users through centralized enforcement, the imposition of data sharing obligations on gatekeepers, the creation of extensive data access rights by business users (including in relation to data inferred from the engagement with their product by end users) and extensive remedies for non-compliance, which are significantly more likely to tilt data relations in favor of business users.[269] It remains to be seen whether this recalibration of data relations in favor of business users, will, at the same time, lead to a recalibration of data relations with *end users*, in particular as regards their non-personal or anonymized data, as a result of the DMA's conceptualization of data as a *resource*.[270]

B. Recalibration vis-à-vis the European Commission and the Public

The DMA tilts data relations between gatekeepers and the Commission in favor of the latter, most notably with regards to the Commission's access to data

263. *See id.* at 79–80 (discussing the benefits of centralized enforcement mechanisms).

264. DEP'T. ENTER., TRADE & EMP., CCPC SUBMISSION TO CONSULTATION ON THE DIGITAL MARKETS ACT PROPOSAL 7 (2021) [hereinafter CCPC Submission] https://enterprise.gov.ie/en/Consultations/Consultations-files/CCPC-DSA-Submission.pdf (Ireland's body in charge of P2B compliance calling for clarification regarding questions arising from the DMA's enactment).

265. *See* DMA, *supra* note 6, at 3 ("[the DMA] builds on the existing P2B Regulation, without conflicting with it").

266. *See* ALEXANDRE DE STREEL ET AL., ENFORCEMENT AND INSTITUTIONAL ARRANGEMENTS 16 (2021), https://cerre.eu/wp-content/uploads/2021/05/CERRE_FOURTH-ISSUE-PAPER_DMA_European-Parliament-Council-recommendations_May-2021.pdf (discussing the difficulty entities find settling disputes with major platforms).

267. CCPC Submission, *supra* note 264, at 7 (explaining the desire for a Member State to have communication to navigate overlaps in enforcement).

268. *Id.*

269. *See* Aline Blankertz & Julian Jaursch, *What the European DSA and DMA Mean for Online Platforms*, BROOKINGS (Jan. 14, 2021), https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms (offering examples of how the DMA may offer better terms for business users).

270. *See* Thomas Streinz, *The Evolution of European Data Law in* THE EVOLUTION OF EU LAW 902, 902 (Paul Craig & Gráinne de Búrca eds., 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971 (discussing the origins of the framework of seeing data as a resource).

processed and stored by the gatekeepers.[271] This is likely to facilitate enforcement both, under the DMA and EU competition law, thereby contributing to more competitive digital markets.[272]

A good example of this recalibration is the obligation on gatekeepers under Article 13 DMA to annually submit an "independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services" to the Commission.[273] In addition to eliminating the lack of information as to the profiling practices of gatekeepers on the part of the Commission allowing for better monitoring and enforcement, this obligation is also relevant to the recalibration of data relations between gatekeepers and their actual and potential *competitors*.[274] This is because—to the extent that the Article 13 obligation will help to enhance transparency of gatekeepers' profiling practices—it may contribute to the ability of actual or potential competitors in the relevant market "to differentiate themselves better through the use of superior privacy guaranteeing facilities" and to put "external pressure on gatekeepers to prevent making deep consumer profiling the industry standard."[275]

While the aim and key mechanism of Article 13 of the DMA are clear, one may question the drafters' assumption that the obligation of submitting audited descriptions to the Commission will have any meaningful impact on gatekeepers' data collection and processing practices aimed at consumer profiling. After all, the drafters seem to assume that a reduction of profiling practices will stem from "external pressure on gatekeepers" exercised by actual or potential competitors' product differentiation on the basis of "superior privacy guaranteeing facilities."[276] This assumption neglects two key considerations. First, it is unclear whether and how the Commission's knowledge of a gatekeeper's profiling practices can be transposed into the differentiation practices of the gatekeepers' actual and potential competitors required to exercise meaningful "external pressure" on gatekeepers. For instance, it is unclear whether the Commission will pass such information on to competitors or whether it can even lawfully do so, in the first place, in the absence of express statutory authorization in the DMA or otherwise.[277] Second, it is unclear whether the drafters of the DMA are right to presume that end users will actually respond to a product or service differentiation on the basis of

271. *See* Blankertz & Jaursch, *supra* note 269 (discussing the Commission's regulatory power over gatekeepers as a result of the DMA).

272. Assuming that competition enforcement actually leads to more competitive markets; note that it is unclear whether the Commission will share the data provided to it by gatekeepers with national competition authorities. No such requirement appears to be contained in the DMA.

273. DMA, *supra* note 6, at 44.

274. *Digital Markets Act Impact Assessment Support Study Annexes*, at 197, COM (Dec. 2020) 630, https://op.europa.eu/en/publication-detail/-/publication/2a69fd2a-3e8a-11eb-b27b-01aa75ed71a1.

275. DMA, *supra* note 6, at 29.

276. *Id.*

277. For example, reporting obligations could be introduced (or the Commission could be allowed to publish the information provided by the gatekeepers) which could open the gatekeeper's profiling practices to public scrutiny. In the absence of personal data (or its anonymization, should this be possible) and any protectable business secrets contained in such reports, no additional legal basis would arguably be needed for this information to be made public.

"superior privacy guaranteeing facilities" by switching providers or, at least, multi-homing (i.e., what the "privacy-elasticity of demand" is).[278] After all, the switching costs for consumers will remain significant, in light of the strong network effects in digital platform markets, even when taking into account the right to data portability.[279] Furthermore, there is strong evidence to suggest that a "privacy paradox" exists, whereby many consumers claim to place great importance on matters of privacy but do not act accordingly in practice, often trading their privacy and personal data for minimal short-term benefits.[280] For instance, consumers are regularly willing to trade their privacy and data for relatively small benefits.[281] Considering the strong network effects associated with services provided by gatekeepers, end users may consider lower levels of data protection a "price worth paying" or may simply not care about the level of data protection in this practical context. However, these potential deficits in relation to end users do not diminish the fact that Article 13 certainly recalibrates data relations between gatekeepers and the *Commission*, in favor of the latter.[282] Of course, if the privacy-elasticity of demand turns out to be higher in practice than assumed in this section, Article 13 may also recalibrate data relations vis-à-vis the public in their capacity as users,[283] forcing gatekeepers to pay closer attention to the privacy preferences of consumers to compete successfully. However, for the reasons set out above, this is unlikely to happen on a meaningful scale in practice.[284]

The recalibration of data relations between gatekeepers and the Commission also becomes apparent in Article 19(1) DMA, granting the Commission extensive rights to "request access to data bases and algorithms" and "request explanations" about them by way of a "simple request or […] decision."[285] Thus, Article 19(1) DMA may give the Commission access to data, which is vital for successful enforcement, helping to eliminate some of the information asymmetries between tech companies and enforcers. The fact that such access is to be granted to the Commission "irrespective of who possesses the documents, data or information in question, and regardless of their form or

278. *See* OXERA, MARKET POWER IN DIGITAL PLATFORMS (2018), https://www.oxera.com/wp-content/uploads/2018/10/Market-power-in-digital-platforms.pdf (describing the idea that consumers elasticity for data privacy will inhibit platforms' ability to exploit their data).

279. STÉPHANE CIRIANI & MARC LEBOURGES, THE MARKET DOMINANCE OF US DIGITAL PLATFORMS: ANTITRUST IMPLICATIONS FOR THE EUROPEAN UNION 2 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977933.

280. *See, e.g.*, Alessandro Acquisti & Jens Grosslags, *Privacy and Rationality in Individual Decision Making*, 3(1) IEEE SEC. & PRIV. 26–33 (2019), https://ssrn.com/abstract=3305365 (finding that, even with sufficient information, consumers are likely to "trade off long-term privacy for short-term benefits", despite "growing privacy concerns"); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880–1903 (2013), https://ssrn.com/abstract=2171018; *see also* BARRY BROWN, STUDYING THE INTERNET EXPERIENCE, HP PUBL'G SYS. & SOLS. LAB'Y (2001), https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf (in which "privacy paradox" was likely used for the first time in this context).

281. *See* Acquisti & Grosslags, *supra* note 280, at 26 (finding that, even with sufficient information, consumers are likely to "trade off long-term privacy for short-term benefits," despite "growing privacy concerns").

282. DMA, *supra* note 6, at 44.

283. *Id.*

284. *Id.*

285. *Id.* at 47.

format, their storage medium, or the place where they are stored"[286] in recital 69 may spill over into a recalibration of data relations with other actors "possessing" data, access to which the Commission may request.[287] However, it remains to be seen how often and how effectively the Commission is going to make use of its Article 19(1) right and whether this will have a significant impact on the monitoring and enforcement activities of the Commission. If so, the effects of this provision may go beyond enforcement under the DMA, spilling over into ordinary competition enforcement under Articles 101 and 102 TFEU in reliance on the data obtained by the Commission under the DMA.[288]

C. Recalibration Against the Background of the GDPR

As a horizontal and symmetrical omnibus regulation on personal data, the GDPR has a much broader scope of application than the asymmetric DMA which only applies to *gatekeepers*.[289] The GDPR also differs from the DMA in its core objectives and conceptualization of "data."[290] The GDPR appears to focus on the protection of the *fundamental right* to the protection of *personal* data recognized in the TFEU and the Charter of Fundamental Rights (CFR).[291] By contrast, the core aims of the DMA center around a framing of data as a resource with economic value.[292] The Act seeks to contribute to the creation of a Digital Single Market in which data can move freely by eliminating divergences between Member State laws constituting "obstacles to the freedom to provide and receive services" and "cross-border business,"[293] as well as establishing common levels of protection of business users and end-users against unfair behavior on the part of gatekeepers, so as to "ensure contestable and fair digital markets" across the EU.[294] This dichotomy of internal market and free movement of data objectives on the one hand, and the fundamental rights framing of data protection on the other hand, is striking.[295] However, it is not

286. *Id.* at 31.

287. Note that the reliance on "possession" of data underscores the lack of a data ownership regime in EU law—a factor that may lead to complex arguments about data as a resource that can or cannot be divested of like physical assets.

288. *Compare* Consolidated Version of the Treaty on the Functioning of the European Union arts. 101–102, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU] (outlining the rules of competition within the EU internal market) *with* DMA, *supra* note 6, at 47 (outlining the process of governmental enforcement requesting information pertaining to investigations under the DMA).

289. GDPR, *supra* note 39; 2016 O.J. (L 119) 1, 4 ("Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union.").

290. *Compare id.* at 33 (defining "personal data" for the purposes of GDPR) *with* DMA, *supra* note 6, at 1 (outlining the importance and size of the digital economy as a need to fight unfair practices).

291. *See* TFEU, *supra* note 288, at 55 ("Everyone has the right to the protection of personal data concerning them."); Charter of Fundamental Rights of the European Union 1, 10, Dec. 18, 2000, 2000 (C 364) ("Everyone has the right to the protection of personal data concerning him or her.").

292. *See* DMA, *supra* note 6, at 1 (outlining the importance and size of the digital economy as a need to fight unfair practices).

293. *Id.* at 16.

294. *Id.*

295. *Compare* GDPR, *supra* note 39, at 33 (defining "personal data" for the purposes of GDPR) *with* DMA, *supra* note 6, at 1 (outlining the importance and size of the digital economy as a need to fight unfair practices).

new to EU data law.[296] In fact, it formed a core tension of EU data law since its early years, and is reflected in Article 16 of the TFEU which provides that "everyone has the right to the protection of personal data concerning them," but at the same time posits that the Parliament and Council must lay down rules on "the free movement of such data."[297] This balance need not always be framed as a tension. In the GDPR, personal data protection is conceptualized as a *prerequisite* for the free movement of such data, in the absence of which diverging levels of data protection across different Member States would "hamper[…] the free movement of personal data within the internal market."[298] Equally, the Data Protection Directive (DPD)—the predecessor of the GDPR—requires a "balancing of the control of […] personal information and the free movement of data in the internal market."[299] Nevertheless, scenarios are thinkable where a "fundamental rights" conceptualization of personal data will be at tension with a conceptualization of "data as a resource" which ought to move freely across the EU Common Market and which may serve as a key input for effective competition, innovation and economic growth across different sectors of the economy.[300]

Against this background, it is submitted that the DMA recalibrates data relations in the EU by placing greater emphasis on market objectives, most prominently for reasons related to competition and contestability.[301] For instance, while the DMA requires that gatekeepers comply with their obligations under the DMA in conformity with the GDPR, the DMA contains a number of provisions reflecting a "data as a resource" framing which may cause ambiguity in data protection that could be resolved in favor of a lowering of data protection standards for the sake of enhancing competition.[302] For instance, the anonymization requirement forming part of the data sharing obligations placed on gatekeepers providing search engine services (discussed in Section II.B.3.c of this paper) creates an ambiguous standard of anonymization by requiring that the data be anonymized *enough* to comply with data protection laws, but not *too anonymized*, so as not to diminish the utility of such data to competitors who get an access rights to such data under the DMA.[303] It is submitted that this is indicative of a conceptualization of data protection as a *trade-off* to competition which, on the facts, will lead to practical problems in gatekeepers' balancing of

296. *See* Streinz, *supra* note 270 (providing a history of EU data law and its evolution from right to data as a resource).

297. *See* Streinz, *supra* note 270, at 31 (discussing the history of EU disclosure law that may inhibit the free movement of goods and services); TFEU, *supra* note 288, at 55 (referring to the right to data protection and the free movement of that data).

298. GDPR, *supra* note 39, at 3.

299. PRIVACY AND COMPETITIVENESS IN THE AGE OF BIG DATA: THE INTERPLAY BETWEEN DATA PROTECTION, COMPETITION LAW AND CONSUMER PROTECTION IN THE DIGITAL ECONOMY 12 (2014), https://edps.europa.eu/sites/default/files/publication/14-03-26_competition_law_big_data_en.pdf (last visited Feb. 27, 2022).

300. *See* Gal & Rubinfeld, *supra* note 23, at 754 ("The importance of widening the use of data cannot be overstated. Data serve as a foundation input in the information-based economy.").

301. *See* DMA, *supra* note 6, at 1 (outlining the importance and size of the digital economy as a need to fight unfair practices).

302. *See generally id.* at 5; Streinz, *supra* note 270 (discussing the framing of data as a resource).

303. *See* DMA, *supra* note 6, at 41 (detailing the anonymization requirement).

these competing requirements.[304] For instance, to comply with both the DMA and the GDPR (or at least not violate either of the two regulations too openly), gatekeepers will need to ensure that they do not diminish data protection standards below what is required by the GDPR, but at the same time not anonymize data to an extent that will deprive it of almost all practical utility for competitors who will not be able to use such data to strengthen their competitive position.[305] This may lead to a limitation of the DMA's positive impact in enhancing the compatibility of digital markets through the imposition of mandatory data sharing obligations. In this context, an interesting insight is offered by Gal and Aviv who found that the non-sectoral, omnibus protection of personal data under the GDPR detrimentally affects competition and comes at an enormous *cost* to the economy.[306] For instance, they found that "the GDPR raises the transaction costs of sharing data between different data controllers."[307] Against this background, it is worth noting that, while accepting a "data as a resource" framing, the DMA imposes "opt-in" as opposed to "opt-out" obligations for the combination of data under Article 5(a), thereby limiting the economic value that can be derived from personal data on what appears to be a competition basis, but at the same time, imposing a consent standard which *exceeds* the standard for lawful processing set by Article 6 GDPR.[308]

Overall, while the DMA does not intentionally override the data protection standards of the GDPR, its move towards a "data-as-a-resource" framing and its ambiguous anonymization requirements may have unforeseen spillover effects.[309] It is therefore submitted that, rather than trying to pretend that a tradeoff between competition and data protection does not exist and that data access rights favorable to competition can always be fully reconciled with rights to data protection, EU policymakers should acknowledge and embrace the competing interests of data protection and competition and balance them in future regulations of digital markets.[310] Not striking this difficult balance means that, in practice, it will be struck by private actors such as gatekeepers, who are biased in the sense that data collection and processing are key to their business models, or to enforcers, including the European Commission, and the Courts (including the CJEU) whose contribution to the development of legal principles

304. *Bridging the DMA and the GDPR – Comments by the Centre for Information Policy Leadership on the Date Protection Implications of the Draft Digital Markets Act*, HUNTON ANDREWS KURTH LLP: CTR. FOR INFO. POL'Y LEADERSHIP, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_data_protection_implications_of_the_draft_digital_markets_act__6_dec_2021_.pdf (last visited Feb. 7, 2022).

305. *See generally* Gabriel Nicholas & Michael Weinberg, *Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors?*, NYU CTR. INNOVATION L. & POL'Y., (Nov. 2019), https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition (presenting an overview and analysis of the reasons for why exported user data may be of limited utility to actual and potential competitors).

306. Michal Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, J. COMPETITION L. & ECON. 33, (Mar. 2020), https://ssrn.com/abstract=3548444.

307. *Id.* at 36.

308. *See* DMA, *supra* note 6, at 40–41 (detailing the opt-in requirement); GDPR, *supra* note 39, at 36–37 (discussing consent and other bases for the lawful processing of personal data).

309. *See generally* DMA, *supra* note 6 (providing the "data-as-a-resource" framing and anonymization requirements).

310. *See generally id.* (exemplifying the current approach).

under competition and data-related regulations will lack the democratic legitimacy of a balance approved by the Parliament and Council.[311] In light of the ambiguous data sharing and anonymization provisions of the DMA, it remains to be seen which standard of anonymization will actually be applied (e.g., developed over time to ensure state of the art anonymization) by gatekeepers and how the Commission will react to it.[312]

D. Recalibration Against the Background of Recent Developments in German Competition Law

The FCO has repeatedly pointed out the significant challenges posed by data in digital markets and "the special features of multi-sided platforms and networks" to legislators and competition enforcers.[313] For instance, the FCO has highlighted the difficulties of assessing "data as a factor to establish market power" and the development of suitable theories of harm associated with the collection, possession and processing of data.[314] This view was coupled with calls by the German competition enforcers and policymakers to "modernize current competition law by adapting existing analytical tools . . . to the need to introduce pro-competitive regulatory frameworks."[315] The practical result of these considerations have been two recent developments in German competition law: The passing of the 10th Amendment of the German Act Against Restraints of Competition (GWB) in January 2021 and the FCO's decision in the *Facebook* case, both of which will be discussed below.[316]

1. Tenth Amendment of the German Act Against Restraints of Competition (GWB)

The 10th amendment to the GWB came into force on January 18th, 2021.[317] The primary aim of the new German law was to implement Directive (EU) 2019/1[318] on the empowerment of "competition authorities of the Member

311. *See generally* DIETER GRIMM, THE CONSTITUTION OF EUROPEAN DEMOCRACY (Justin Collings ed., 2017) (presenting a detailed overview of the democratic deficits of the development of important or fundamental legal principles by the Commission and CJEU rather than the European Parliament or Council).

312. *See generally* DMA, *supra* note 6 (providing the described provisions).

313. *Market Power of Platforms and Networks* 1 (Bundeskartellamt, Working Paper B6-113/15, 2016).

314. BUNDESKARTELLAMT & AUTORITÉ DE LA CONCURRENCE, COMPETITION LAW AND DATA 3–4, (2016), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

315. OECD Directorate for Financial and Enterprise Affairs Competition Committee, *Abuse of Dominance in Digital Markets – Contribution from Germany* (Dec. 8, 2020), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2020/OECD_2020_ABUSE_OF_DOMINANCE_IN_DIGITAL_MARKETS.pdf?__blob=publicationFile&v=2.

316. *Id.* at 6–16.

317. Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen [GWB-Digitalisierungsgesetz] [GWB Digitalization Act], Jan. 18, 2021, Bundesgesetzblatt [BGBL I], at 1, 2. http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s0002.pdf (containing the10th amendment to the GWB in German).

318. Directive 2019/1 of the European Parliament and of the Council of 11 December 2018 to Empower the Competition Authorities of the Member States to Be More Effective Enforcers and to Ensure the Proper Functioning of the Internal Market, 2019 O.J. (L 11) 3–33.

States." However, the Bundestag also took the opportunity to equip the GWB with tools suited to address anticompetitive conduct relating to data, taking into account the specific characteristics of digital markets.[319] While it would exceed the scope of this paper to evaluate and discuss all of the new amendments to the GWB, two key modified provisions are worth pointing out for the purposes of considering the DMA's recalibration of data relations against the background of competition law in Germany—§§ 18 and 19a of the GWB.[320]

The newly introduced §19a(2) GWB relates to "undertakings with paramount significance for competition across markets" and allows the FCO to directly *prohibit* the creation or increasing of barriers to entry or the hindering of other undertakings or demanding terms of service which would allow for such a use, by "undertakings with paramount significance" which *use data* collected on the dominated market, including in combination with competition-relevant data from sources other than the dominant market.[321] In the FCO's understanding, the type of conduct which the FCO can now prohibit under §19a of the GWB "as a *preventive measure*" includes "the self-preferencing of a group's own services or impeding third companies from entering the market by processing data relevant for competition."[322]

The other key provision of the GWB—§18—was amended to include new statutory factors for the determination of market dominance for the purposes of German competition law.[323] For instance, the old §18(3) GWB market dominance factors such as, market share, financial strength, barriers to entry, and access to supply or sales markets, are now complemented by an undertaking's "*access to data relevant to competition*."[324] This addition is interesting because, under the previous version of the GWB, "access to data relevant to competition" was only a relevant market dominance factor in *multi-sided markets*,[325] but not in other types of markets. With the new §18(3)(iii) GWB, this factor will now apply universally.[326] Another addition to §18 can be found in the newly inserted §18(3b) GWB.[327] This section provides that "[w]hen evaluating the market dominance of an undertaking that is active as an intermediary in multi-sided markets, the importance of the intermediary services

319. Act Against Restraints of Competition [GWB], June 26, 2013, BGBL I at 1750, 3245, as amended by Gesetz [G], July 9, 2021, BGBL I at 2506, art. 4 (Ger.), https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf.

320. *Id.* at 2–5.

321. *Id.* at 4.

322. Press Release, Bundeskartellamt, Amendment of the German Act against Restraints of Competition (Jan. 19, 2021) (emphasis added) https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html.

323. Act Against Restraints of Competition [GWB], June 26, 2013, BGBL I at 1750, 3245, as amended by Gasetz [G], July 9, 2021, BGBL I at 2506, art. 4 (Ger.), https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf.

324. *Id.* at 2–3.

325. *See id.* at 3 (listing "access to data relevant for competition" as a relevant market dominance factor in multi-sided markets).

326. *Id.*

327. *Id.*

it provides for the access to procurement and sales markets must also be taken into account."[328]

While many more additions to the GWB have been made in the 10th revision,[329] a number of interesting insights on the future interaction between the DMA and German competition law can be gained from the amended §§ 18 and 19 GWB.[330] Firstly, the fact that the new amendments were passed in German Parliament with the votes of parliamentarians from three very different political fractions—the conservative CDU/CSU, the social-democrat SPD, and the Green Party—shows that there is strong support across the political spectrum in Germany for more regulatory intervention and action in digital markets.[331] Against this background, while the FCO has more autonomy than competition authorities in many other Member States and is, in many respects, not subject to significant political pressure, it may still feel empowered and confirmed in its course of more active competition enforcement in digital markets in the near future.[332] Secondly, and more importantly to this paper, §§ 18 and 19a GWB equip the FCO with tools that will allow it to engage in investigations and enforcement that may overlap with the future competences of the European Commission under the DMA.[333] The political support, combined with the tools for more active enforcement, arguably make it possible that a fragmentation of obligations on gatekeepers will occur on the digital single market, whereby the FCO could impose a standard on "undertakings with paramount significance for competition across markets" under the German domestic §19a GWB that differs from or even conflicts with the standard applied by the Commission under the DMA.[334]

While this must have been intended or at least foreseen by the drafters of the DMA (given the DMA's explicit national competition carveout), a fragmentation of obligations on gatekeepers may undermine the creation of a Digital Single Market across which data can be collected and used on the same terms, complicating and potentially increasing the cost of compliance for gatekeepers.[335] The overlap may give rise to difficult institutional tensions between the Commission and the FCO should there ever be a conflict of obligations imposed on gatekeepers as a result of two separate investigations concerning the same conduct (under the DMA and under national competition

328. Author's translation. *See also id.* ("In assessing the market position of an undertaking acting as an intermediary on multi-sided markets, account shall be taken in particular of the importance of the intermediary services provided by the undertaking for accessing supply and sales markets.").

329. The full amendments, as published in the Federal Gazette, are 31 pages long.

330. Act Against Restraints of Competition [GWB], June 26, 2013, BGBL I at 1750, 3245, as amended by Gasetz [G], July 9, 2021, BGBL I at 2506, art. 4 (Ger.), https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf.

331. Wettbewerbsrecht Novelliert und Kinderkrankengeld-Regelung Ausgedehnt [Competition Law Amended and Children's Sickness Benefit Regulation Extended], DEUTSCHER BUNDESTAG (Jan. 14, 2021), https://www.bundestag.de/dokumente/textarchiv/2021/kw02-de-digitalisierungsgesetz-gwb-814250 (Ger.).

332. *See id.* (providing background).

333. Act Against Restraints of Competition [GWB], June 26, 2013, BGBL I at 1750, 3245, as amended by Gasetz [G], July 9, 2021, BGBL I at 2506, art. 4 (Ger.), https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf.

334. *See id.* at 4–5 (providing § 19a GWB).

335. *See generally* DMA, *supra* note 6, at 40–41 (providing the text of the DMA).

law, respectively). Should the risk of such conflict materialize in practice, this may raise the question of whether a solution similar to the DMA's limitation on stricter regulation of gatekeepers in the Member States would be possible and appropriate.[336]

2. The Facebook Decision[337]

On February 6, 2019, the FCO published a decision[338] in which it prohibited Facebook "from making the use of the Facebook social network by private users residing in Germany, who also use its . . . services WhatsApp, Oculus, Masquerade and Instagram, conditional on the collection of user and device-related data by Facebook and combining that information with *facebook.com* user accounts without the users' consent". It also prohibited the imposition of "terms making the private use of Facebook.com conditional on Facebook being able to combine information saved on the 'Facebook account' . . . with information collected on websites visited or third-party mobile apps used via programming interfaces ('Facebook Business Tools') and use this data [without the users' consent]."[339] The FCO based its decision on §19(1) GWB which prohibits "the abuse of a dominant position by one or several undertakings."[340] It held that Facebook was dominant in the market for "private social networks with private users" and that its terms of service violated the GDPR, so that their imposition was *exploitative* and unfair, and constituted an illegal abuse of dominance under §19(1) GWB.[341]

To conceptualize the alleged violation of the GDPR as an abuse of dominance under §19(1) GWB, the FCO relied on the notion that, according to German domestic case law, "principles from [non-competition law] provisions of the legal system that regulate the appropriateness of conditions agreed upon in unbalanced negotiations can be used as concepts for appropriateness in the

336. *See* DMA, *supra* note 6, at 34. Such solution would resolve the overlap in favor of a more centralized enforcement by the Commission and would give rise to challenging questions under Regulation 1/2003 allowing for a higher level of protection under national competition law in some circumstances (as discussed earlier in this paper). Of course, this tension could, in principle, be resolved in favor of national competition authorities instead. However, this would run counter to the idea underlying the high degree of centralization of enforcement by the Commission under the DMA in the first place, arguably aimed at preventing a fragmentation of the Digital Single Market (at least as a *desideratum*).

337. With minor modifications, the summary of the Facebook case provided in this part of the present paper is taken from an earlier paper I havethe author has written on the Facebook case in Fall 2020 as part of the *Antitrust: International and Comparative Seminar* at the NYU School of Law. However, the analysis of the interaction with the DMA and the recalibration of data relations that follows from it is entirely new to this paper.

338. Bundeskartellamt, Feb. 6, 2019, B6-22/16 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

339. Bundeskartellamt, Case Summary of Decision B6-22/16 of 6 February 2019 "Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing" 1 https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4.

340. The German national equivalent of Art. 102 TFEU. Act Against Restraints of Competition [GWB], June 26, 2013, BGBL I at 1750, 3245, as amended by GasetzGesetz [G], July 9, 2021, BGBL I at 2506, art. 4 (Ger.), https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf.

341. Bundeskartellamt, Feb. 6, 2019, B6-22/16 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

assessment of abusive practices under Section 19(1) GWB."[342] The FCO relied on this case law to state that "the principles of data protection law underlying the GDPR are . . . a suitable standard for measuring the appropriateness of the data processing terms of a dominant supplier . . . [and] must be taken into account . . . as a higher-ranking constitutional law that specifies constitutionally guaranteed rights."[343]

The FCO cited the FCJ's decision in *VBL-Gegenwert*[344] for the proposition that "an abusive practice can . . . be found based on . . . §19(1) GWB, e.g. where general business terms are used that are inadmissible under the legal principles of . . . the German Civil Code, and . . . represent a manifestation of market power."[345] It also cited the decision in *Pechstein*[346] for the proposition that "to safeguard constitutionally protected rights, [§19 GWB] must be applied in cases where one contractual party is so powerful that is would be practically able to dictate contractual terms, thus eliminating the other party's contractual autonomy [in order to] uphold the protection of constitutional rights."[347] As the relevant constitutionally protected right in this case, the FCO cited the "right to self-determination in business affairs (contractual freedom)" which it considered to be under attack where a "party is able to unilaterally determine the terms of . . . contract"[348] and where such contractual terms are "unfair" and "a sufficient degree of market power is involved" in their imposition.[349]

The FCO assumed that the doctrine from *VBL-Gegenwert* and *Pechstein*, which was developed "to take into account the appropriateness concepts of Sections [307-309] of the German Civil Code (BGB)[350] within the framework of § 19(1) GWB," can, by analogy, also be applied "to all other principles of legal provisions," so long as "a sufficient degree of market power is involved and to the extent that the principles concern the appropriateness of conditions agreed upon in unbalanced negotiations."[351] In the FCO's view, this applied to "constitutional principles that protect the right to informational self-

342. *Id.* at ¶ 526.

343. *Id.*

344. Bundesgerichtshof [BGH] [Federal Court of Justice], Nov. 6, 2013, 58/11, VBL-Gegenwert I, 2, 65 (Ger.); Bundesgerichtshof [BGH] [Federal Court of Justice], Jan. 24, 2017, 47/14 VBL-Gegenwert II, 1, 35 (Ger.).

345. Bundeskartellamt, Feb. 6, 2019, B6-22/16 at ¶ 527 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

346. Bundesgerichtshof [BGH] [Federal Court of Justice], June 7, 2016, 6/15, Pechstein/International Skating Union, 1, 48 (Ger.).

347. *Id.*

348. Bundeskartellamt, Feb. 6, 2019, B6-22/16 at ¶ 528 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5; Bundesverfassungsgericht [BVerfG] (Federal Constitutional Court) 1 BvR 2160/09, Sept. 7, 2010, at ¶ 34.

349. *Id.*

350. *See German Civil Code: BGB*, FEDERAL MINISTRY OF JUSTICE, https://www.gesetze-im-internet.de/englisch_bgb (last visited Feb. 7, 2022) (offering an official English translation of the BGB).

351. Bundeskartellamt, Feb. 6, 2019, B6-22/16 at ¶ 529 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

determination[352] and the fundamental right to data protection" and, consequently, principles "relating to the appropriateness of data use must . . . be directly applied, as they are based on the fundamental right to data protection under Art. 8(2) EU Charter and weigh up the fundamental right to data protection against the rights and interests of the data processor."[353] The FCO further considered data policies to be akin to general business terms since, "from the perspective of users, they have a regulatory character."[354] The FCO found it appropriate to apply this principle to the imposition of terms which do not comply with the GDPR and found that they are capable of directly constituting an abuse of dominance under §19(1) GWB.[355] On the facts, the FCO held that Facebook did not have a lawful basis for the processing of user data, since the "consent" given to Facebook's terms of service was not truly *voluntary* within the meaning of the GDPR[356] and—contrary to Facebook's position—the processing of user data was *not* required for the performance of Facebook's

352. The right to *informational self-determination* was established by the German Federal Court of Justice (FCJ) in its 1983 *Volkszählungsurteil* decision (1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 (in German) https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/1983/12/rs19831215_1bvr020983.pdf;jsessionid=9F05DD4D0D18D28F4E3915C48D9EB77E.2_cid377?__blob=publicationFile&v=1. The case concerned a law proposed in 1982 for a population census in Germany, which included provisions on the processing of the obtained information. It also prescribed the purposes for which the obtained information ought to be used. In a landmark decision, the FCJ struck down the law as unconstitutional, holding that it infringed the *constitutional right to informational self-determination*. This was because the proposed law's provisions on the form and processing violated individuals' right to decide on the provision and processing of their personal data. In the FCJ's opinion, this right is grounded in Art. 1(1) of the German Basic Law (GG) ("Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority") in conjunction with Art. 2(1) GG ("Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law"). The FCJ held that limitations of the right to informational self-determination are only allowed in cases where the public interest prevails, and the rule of law and principle of proportionality are complied with. It also drew a distinction between personalized and anonymized, statistical data, finding that the purpose limitation on the collection and processing of the latter type of data could be less narrow. Overall, the FCJ noted that the proposed census law would lead to a registration and cataloging of individuals' personalities which is incompatible with respect for human dignity (Art. 1(1) GG). Among other things, stronger procedural safeguards for the implementation and organization of the data collection were needed to ensure the protection of individuals' fundamental rights. The FCJ was cautioning against a social order in which citizens do not know who knows what about them at which point in time. In the FCJ's view, such a situation would pose a risk to the liberal-democratic order by discouraging individuals from developing their personalities, since they would not know whether their behavior is being recorded and permanently saved as information. The FCJ found that the free development of individuals' personalities in (1983) modern conditions required the protection of individuals against unlimited collection, storing and processing of personal data and, as such, was covered by Art. 2(1) in conjunction with Art. 1(1) GG. Overall, this fundamental right guarantees the right of individuals to decide over the provision and use of their personal data.

353. Bundeskartellamt, Feb. 6, 2019, B6-22/16 at ¶ 529 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5. Interestingly, the cited Article 8(2) of the Charter of Fundamental Rights of the European Union merely requires that personal data be "processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."

354. *Id.* at ¶ 534.

355. *Id.* ¶ 531; Of note, the FCO rejected Facebook's objection that the antitrust caselaw developed in relation to violations of §19(1) through the imposition of unfair contract terms cannot simply be extended to data protection laws, such as the GDPR. Facebook argued that, unlike the conclusion of a contract, data processing "was not subject to contractual freedom but had to comply with data protection legislation, whereas the [BGB] provisions on unfair contract terms merely limited the scope of contractual freedom."

356. GDPR, *supra* note 39, at 36, 38.

contract with them.[357] The FCO also noted that, in its view, data protection law generally has as its objective "to counter power asymmetries between organizations and individuals and to carry out an appropriate balancing of interests" between them, and provides individuals with "the right to decide freely and without coercion on the processing of [their] personal data"—including on the combination of their data across services.[358]

Of note, the FCO recognized and explicitly admitted that the competition law "concept of protection," which it was applying in its present decision against Facebook, "so far found no equivalent in European case law or application practice."[359] For instance, while Article 102 of the TFEU prohibits abuses of dominance consisting of the "imposition of unfair purchase or selling prices or other unfair trading conditions,"[360] it does not rely on "values based on both fundamental rights and ordinary law" in determining whether a dominant company's conduct is abusive, which the FCO applied under §19(1) of the GWB.[361] The FCO therefore decided to rely on Article 3(2) of Regulation 1/2003[362] which allows EU Member States to adopt or apply "stricter national provisions in their territory in order to prevent or punish unilateral actions by undertakings" than those applicable under EU competition law.[363]

The FCO ordered Facebook to terminate or adjust its terms of service to comply with the FCO's decision within twelve months.[364] In particular, it prohibited making the use of *Facebook.com* conditional on the collection of user and device-related data of private users on WhatsApp, Oculus, Masquerade, Instagram, and external websites through *Facebook Business Tools* ("off-Facebook" data).[365] It further prohibited the combination of any such "off-Facebook" private user and device data with data collected *on* Facebook.com ("on-Facebook" data).[366]

Following an appeal to the FCO's decision, it was initially reversed by the Düsseldorf Higher Regional Court (DHRC).[367] The DHRC's decision mostly rested on observations relating to the duplicability of data[368] and that users were

357. *Id.* at 36.

358. Bundeskartellamt, Feb. 6, 2019, B6-22/16 at ¶ 530 (Ger.), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

359. *Id.* at ¶ 914.

360. *Id.*

361. *Id.*

362. Council Regulation 1/2003, 2003 O.J. (L 1) 1.

363. *Id.*

364. FCO B6-22/16 (2020) (Ger.), ¶ 3a.

365. *Id.* at ¶¶ 1–3.

366. *Id.* at ¶ 2.

367. Oberlandesgericht [OLG] [Higher Regional Court] Aug. 26, 2019, Oberlandesgerichte inOberlandesgericht Düsseldorf [OLGD] Case VI-Kart 1/19 (V), pt. II (Ger.), *translated at* https://www.d-kart.de/wp-content/uploads/2019/08/OLG-D%C3%BCsseldorf-Facebook-2019-English.pdf.

368. *Id.* at pt. II[B][1][b][bb][(1)]; Duplicability refers to the idea that users could provide their data for an unlimited number of times to as many providers as they wish, without incurring any economic loss. As pointed out earlier in this paper in relation to data portability and sharing in Section II.B.3, this idea in its different variations is flawed since it fails to account for data which is inferred from a user's interaction with a platform, and which exceeds the data a user can herself provide to a platform. *See also* Gal & Rubinfeld, *supra* note 23,

not coerced into using Facebook's services, and many consumers who valued data protection exercised their choice not to use Facebook's platform.[369] However, on June 23, 2020, the Federal Court of Justice (FCJ) annulled the DHRC's decision.[370] In a lengthy decision, the FCJ found that, where a dominant operator of a social network conditions itself in its terms of service to provide its users a "personalized experience" for which the users' personal data gathered outside of the social network is to be used (*data combination*), this may constitute an exploitative abuse of dominance.[371] Emphasizing the German constitutional right to "informational self-determination," the FCJ found that the FCO did not need to show a violation of the GDPR to succeed in this case,[372] since an abuse of dominance could be established *directly* on the basis that Facebook deprived users of genuine, voluntary choice.[373] The FCJ further explained that the lack of user options as to the level of data collection and personalization in Facebook's terms of service did not only deprive users of their "right to informational self-determination," but—given the high "lock-in effects"—also exploited users on the basis that "competition [was] unable to effectively exercise its controlling function" with respect to the quantities of processed user data.[374] Additionally, the FCJ pointed out that the concept of *abusive terms of service* did not presuppose that consumers are *entirely* unable to do without agreeing to a contract.[375] On the facts, an "autonomous decision" of users existed only in the sense that their decision to use Facebook was not *vital for life*.[376] However, the protection of consumers from an exploitation by a dominant undertaking was not limited to products and services which were vital for life.[377]

It is submitted that the *Facebook* case offers a highly relevant insight into how the future overlap between the DMA and competition enforcement in Germany may recalibrate data relations.[378] For instance, the FCO's reliance on

---

at 758 (citing MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 186 (2016)) (discussing a similar idea, "feedback network effects").

369. VI-Kart 1/19 (V) OLGD pt. II[B][1][b][bb][(3.1)].

370. Bundesgerichtshof [BGH] [Federal Court of Justice] June 23, 2020, Entscheidungen des Bundesgerichtshofes in Karlsruhe [BGHK] KVR 69/19 (Ger.), https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=c353eb015ca7fa0ec3e380d469956f7f&nr=109506&pos=0&anz=1; *see also* Press Release, Federal Court of Justice, Federal Court of Justice Provisionally Confirms Allegation of Facebook Abusing Dominant Position (June 23, 2020) (available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf?__blob=publicationFile&v=2).

371. Bundesgerichtshof [BGH] [Federal Court of Justice] June 23, 2020, Entscheidungen des Bundesgerichtshofes in Karlsruhe [BGHK] KVR 69/19 (Ger.) at Abs. 1 c).

372. *Id.* at ¶ 109.

373. *Id.* at ¶ 123.

374. *Id.* This is based on an "as-if standard" of competition, whereby the Court considered that—in a competitive social network market—Facebook's extent of data collection would be constrained by actual or potential competitors' products. The assumption is that the extent of data collection (i.e., how narrow it is) would be a competitive factor which would allow competitors to distinguish themselves from Facebook and its products.

375. *Id.* at ¶ 102.

376. *Id.*

377. *Id.*

378. *See generally* OECD Directorate for Financial and Enterprise Affairs Competition Committee, *supra* note 315 (discussing competition enforcement and abuse in the context of dominance in digital markets).

the domestic constitutional right to "informational self-determination" in competition enforcement, and the subsequent confirmation of this strategy by the FCJ, could make this domestic law standard a widely used tool for the assessment of data-related practices of dominant undertakings in digital markets in Germany.[379] While the Facebook case will be referred to the CJEU,[380] it may nevertheless raise difficult questions for future enforcement under the DMA and a harmonious application of its requirements across the EU.[381] For instance, the *right to informational self-determination* as a concept used in determining abusive contractual terms, the imposition of which may constitute an abuse of dominance under German competition law, may be relied on by the FCO to bring cases that exceed the scope of the obligations imposed on *gatekeepers* by the DMA.[382] In light of the national competition law carveout in the DMA, this is unlikely to give rise to direct conflicts between EU and national law.[383] However, the lack of clarity on how DMA enforcement by the Commission relates to national competition law enforcement by the competent national competition authorities which may undermine the DMA's goal of preventing a fragmentation of the Single Digital Market, especially as it concerns the conditions for the collection, processing, and mandatory sharing of data by *gatekeepers*.[384] Even if such fragmentation could be avoided, for example due to a "Dusseldorf effect," whereby the standard applied by the FCO could become the standard followed by (large) companies across the Digital Single Market, this would be undesirable because it could de-facto allow the member states with the most active and resourceful enforcement to set a new "floor" of obligations across the single market.[385] This would raise problems of democratic legitimacy, since the balance struck by legislators in Germany would, in practice, apply in member states whose legislators did not impose a similarly high level of obligations on dominant providers of such services.[386] Furthermore, practical difficulties of an institutional kind may arise in data-related investigations and enforcement actions against *gatekeepers* where the Commission will view itself

379. *See* KVR 69/19 BGHK ¶ 123 (Ger.) (discussing the right to informational self-determination).

380. *See* Press Release, Oberlandesgericht Düsseldorf, Facebook vs. Federal Cartel Office: Results of the Hearing (Mar. 24, 2021), https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2021/20210324_PM_Facebook2/index.php (announcing the referral).

381. *See* DMA, *supra* note 6, at 31 (giving broad authority to request any relevant data, regardless of its location or format).

382. *See infra* Section II.B.2 (discussing gatekeeper obligations).

383. There will also be no conflict between EU competition law and national competition law since Regulation 1/2003 allows member states to adopt and apply "stricter national provisions in their territory in order to prevent or punish unilateral actions by undertakings" than those applicable under EU competition law. *See* Council Regulation 1/2003, Art. 1 § 8, 2002 O.J. (L 1) (EC) (discussing implementation of the rules on competition laid down in Articles 101 and 102 [formerly Articles 81 and 82] of the Treaty establishing the European Community).

384. *See* DMA, *supra* note 6, at 1–14 (discussing the risks of a "fragmentation of the Single Market" and "regulatory fragmentation of the platform space.").

385. *See* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD, 142 (2020) (discussing a similar "Brussels effect" for how EU regulations set a global floor). Special thanks to Thomas Streinz for pointing out that a fragmentation of the Single Digital Market is not inevitable on this set of facts, and a "Düsseldorf" effect may be an alternative development.

386. *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 64 (2012) (discussing issues of democratic legitimacy created by EU regulation).

as the sole, centralized enforcer of the obligations imposed by the DMA, while the FCO will view itself as the competent national enforcer, as supported by the *Facebook* decision of the FCJ and the recently amended GWB.[387]

A hypothetical example of this overlap would be a situation where the FCO and Commission both start an investigation into the conduct of a *gatekeeper* who, in violation of the *ex ante* obligations of the DMA, imposes terms of service which allow for the combination of end user data from different sources without obtaining "voluntary consent" required under the German constitutional right to "informational self-determination," as confirmed in *Facebook*. In such a situation, it will be unclear whether the Commission could condemn the gatekeeper's violation across the entire Single Market, or only the Single Market without Germany, where the FCO has already ordered remedies against the gatekeeper for its violations of German competition law by the same exact conduct. Among other things, it is unclear whether, should there be an overlap and the gatekeeper's conduct be condemned across the single market, this could raise *ne bis in idem* questions, to the extent that the latter doctrine applies to matters of EU competition law.[388] Furthermore, it is unclear what effect the DMA's national competition law carveout will have exactly in cases where the Commission brings a case against a gatekeeper under both the DMA *and* Article 102 TFEU, given that Article 11(6) of Regulation 1/2003 mandatorily "relieve[s] the competition authorities of the Member States of their competence to apply Art. [101] and [102] of the Treaty" where the Commission has already initiated proceedings.[389] For instance, it is conceivable that the result of this will be that where the Commission decides to bring a case merely under the DMA, national competition authorities will be able to apply national competition law to the gatekeeper's conduct, which may result in a stricter standard being applied than the one applied by the Commission under the DMA.[390] However, if the Commission decides to bring a case in relation to the same exact conduct under both, the DMA and Article 102 of TFEU, the national competition authority may be precluded from being able to bring a case under the applicable national equivalent of Article 102 TFEU.[391] If this view will turn out to be correct after (or if) the DMA is adopted, the Commission's power vis-à-vis national competition authorities will be increased significantly.[392]

Overall, it can be said that the DMA's substantive and institutional overlap with national competition law and the bodies tasked with enforcing it may cause

387. *See* KVR 69/19 [BGHK] (Ger.) (exercising regulatory authority independent of the GDPR); *infra* Section III.D.1 (discussing the GWB).

388. *See* Case C-17/10, Toshiba Corp. et al., v. Úřad pro ochranu hospodářské soutěže, ECLI:EU:C:2012:72, ¶ 49 (Feb. 14, 2012) (applying the *ne bis in idem* doctrine in EU competition law, formulated as a prohibition on "the cumulation of fines").

389. Council Regulation 1/2003, Art. 11 § 6, 2002 O.J. (L 1) (EC); *see also* DMA, *supra* note 6, at 34 (noting that DMA merely requires Member State authorities "not [to] take decisions which would run counter to a decision adopted by the Commission under [the DMA]," which, however, does not fully address the identified ambiguity).

390. *See generally* Oana Andreea Stefan, *European Competition Soft Law in European Courts: A Matter of Hard Principles*, 14 EUR. L.J. 753 (2008) (discussing how European courts weigh conflicts between the laws of member states and European Union Commission sources of law).

391. *Id*.

392. *Id.*

a failure to harmonize the legal assessment of the collection, processing and sharing of *personal data* as a subcategory of data across the EU. This may cause additional difficulties since data-protection related obligations may be interpreted differently under EU and Member State laws, despite the harmonizing provisions of the GDPR. Overall, this may undermine legal certainty and complicate the question of the Commission's competency and national competition agencies. It is therefore unclear to what extent the DMA will *actually* recalibrate data relations viewed against competition law in Germany and other EU Member States that are actively engaged in national competition enforcement in digital markets.

IV. RECALIBRATION OF DATA RELATIONS BETWEEN GATEKEEPERS—THE TRUE BENEFICIARIES OF THE DMA?

A recalibration of data relations in favor of parties with less market power than gatekeepers who often have an inferior bargaining position, such as SMEs and consumers, appears to be a *desideratum* of the obligations imposed by the DMA.[393] By granting access to data relevant to competition and limiting the abusive uses of data obtained by gatekeepers by virtue of their powerful position, smaller companies are to be able to compete better in digital markets, and consumers are to be able to exercise a genuine choice as to the level of collection of their data across services as a precondition for the use of a particular service offered by a gatekeeper.[394] Digital markets are to be brought closer to an *as-if competitive* state with an increased privacy-elasticity of demand allowing for a more level playing field that limits gatekeepers' ability to leverage their power over other parties due to their dependency and genuine competition of different business models.[395] Parties with an inferior bargaining position and less market power are to be strengthened in their ability to contest the markets on the merits, rather than based on the degree of their involuntary exploitation by gatekeepers.[396] However, so far, this paper has left unaddressed the question of how gatekeepers *themselves* may try to rely on the obligations imposed by the DMA not only on them individually, but also on *other* gatekeepers with whom they are in actual or potential competition. It is submitted that gatekeepers, rather than SMEs and consumers, may turn out to be the largest beneficiaries of the data sharing and access obligations of the DMA as it is currently drafted, allowing them to strengthen their bargaining position vis-à-vis each other, and to leverage their market power to expand into adjacent digital markets.

393. *See* Mark MacCarthy, *Enhanced Privacy Duties for Dominant Technology Companies*, 47 RUTGERS COMPUT. & TECH. L.J. 1, 27–30 (2020) (discussing dominant position in news referral business and competitive advantages).

394. *See id.* at 15–17 (discussing likely consumer behavior if given the choice to not agree to Facebook's data combination practices).

395. *See id*. at 21–22 (discussing lessons learned from recent FCC and FCO decisions, including how there was not meaningful choice for customers, limiting the availability of alternative business models that protect privacy rights).

396. *See id.* (noting the limited availability of marketplace alternatives).

The obligation under Article 6(1)(j) DMA is a particularly good example of this concern.[397] On its face, one is likely to assume that this obligation to provide search data to competing search engines will benefit smaller search engine providers, including those who collect less data from their users and are therefore unable to make comparable profits from targeted advertising and improve the accuracy of their services to the same extent as the gatekeepers they compete with.[398] This view would support the assumption that online search providers such as, for example, DuckDuckGo would be able to request "raking, query, click and view data in relation to . . . search generated by end users"[399] from Google, so as to improve its services and attract more users. While this is correct, it is certainly not the whole picture. This view neglects the use that competing *gatekeepers*, some of whom do not use a meaningfully different business model, could make use of this provision to improve their services using the data from the interactions of users with the search engine services of other gatekeepers.[400] This is because the wording of Article 6(1)(j) of the DMA is very broad.[401] It requires gatekeepers offering online search services to provide "ranking, query, click and view data in relation to free and paid search generated by end users" to "*any* third party providers of online search engines, upon their request . . . ."[402] There is nothing to suggest, for example, that Microsoft as the operator of the existing online search service Bing, or Amazon as the operator of a hypothetical future general online search engine, would be unable to rely on DMA Article 6(1)(j) to request search data from Google to improve their services and market positions vis-à-vis the latter.[403] While, as this paper pointed out, the utility of such data may be limited in practice, gatekeepers will arguably be able to extract more value from access to search data than smaller providers of online search services.[404] This is because many gatekeepers have business models that are similar in that they rely on the monetisation of "insights from user data," so that the data collected by search service providers using a similar business model may be more useful to them than to smaller search service providers with a "radically different service."[405] Furthermore, gatekeepers are more likely to have the funds and the scale to be able to incorporate the data provided to them by other gatekeepers than smaller providers.[406]

397. DMA, *supra* note 6, at 41.

398. *See id.* ("provide to any third party providers of online search engines . . . .").

399. *Id.*

400. *See id.* ("provide to *any* third party . . . .") (emphasis added).

401. *Id.*

402. *Id.*

403. *See supra* Section II.B.2 (discussing gatekeeper designations gatekeeper under DMA Art. 3, assuming the DMA is passed and both Google and Microsoft are designated as gatekeepers by the European Commission).

404. *See supra* Section II.B.3.c (discussing DMA Art. 6(1)(j) and the potential limitations on the utility of search data provided by gatekeepers to their competitors, upon their request).

405. *See* Nicholas & Weinberg, *supra* note 305, at 2–3 (discussing the higher utility of data for competitor social networks from user interaction collected on Facebook, an entity likely to be designated a gatekeeper, although not for providing search services).

406. *See* Matt Asay, *How DuckDuckGo Makes Money Selling Search, Not Privacy*, TECHREPUBLIC (July 23, 2021, 10:56 AM), https://www.techrepublic.com/article/how-duckduckgo-makes-money-selling-search-not-privacy (comparing the business models of DuckDuckGo and Google).

Similarly, it is likely that the obligation in DMA Article 6(1)(h) requiring gatekeepers to "provide effective portability of data generated through the activity of a business user or end user"[407] will ultimately benefit other gatekeepers more than their non-gatekeeper competitors. Of course, the idea behind Article 6(1)(h) is that it will encourage business users to port their data to competing operators, leading "to an increased choice for … users and an incentive for gatekeepers and business users to innovate."[408] However, this is, again, not the full picture in the sense that the ease of portability may encourage business users to switch from one gatekeeper's service to another gatekeeper's service, rather than to a service offered by a smaller provider.[409] While the increased risk of users switching to other gatekeepers' services is likely to exercise pressure on gatekeepers to innovate and, in some instances, probably even to compete on price (where applicable), the portability-facilitating obligation in Article 6(1)(h) may fail to have a significant effect on the contestability of digital markets for smaller service providers.[410] This is because the latter may lack the funds and scale needed to build an affordable and innovative service and to advertise it sufficiently, so as to make it attractive for users of a gatekeeper's service to switch to the small provider's service, rather than switching to a service provided by another gatekeeper.[411]

A similar effect may occur where gatekeepers decide to make public non-personal data generated through activities by business users and their end users, so as to avoid the prohibition in Article 6(1)(a) on using such data in competition with business users.[412] Here, the recalibrating effect between gatekeepers would not be embedded in the prohibition itself, but rather may result from the ability of gatekeepers to extract more value from any given set of data made public by another gatekeeper than smaller competitors or, in some instances, even business users.[413] Of course, this rests on the assumption that gatekeepers will be able to and decide to make public the aforementioned data, rather than simply refraining from using it in competition with their business users.[414] This is only likely to occur where the long-term value of using the data in competition with other business users will be higher than the loss of data-derived advantages resulting from the publication of the data at issue and will be subject to legal constraints on such publication, for example, resulting from the underlying contractual

407. DMA, *supra* note 6, at 40.

408. *Id.* at 27.

409. *See* Nicholas & Weinberg, *supra* note 305, at 2–3 (noting exported Facebook data would be more likely to be brought to a platform also based on "invasive, highly targeted advertising").

410. *See* Asay, *supra* note 406 (noting Google makes most of its money without knowing anything about who is searching, just their keywords).

411. *See* Section II.B.3.a (noting that any switch using data ported pursuant to DMA Art. 6 § 1(h) is of a kind that can be used by smaller, or even just competitor, providers in the first place); *see also* Asay, *supra* note 406 (discussing DuckDuckGo's advertising push).

412. DMA, *supra* note 6, at 41.

413. *See* Section II.B.3.c (discussing DMA Art. 6(1)(j) and the potential limitations on the utility of search data provided by gatekeepers to their competitors, upon their request).

414. *See* Section II.B.4.a (discussing the obligation in DMA Art. 6 § 1(a) and the possibility of publication of such data).

relationship between the gatekeepers and the business users which led to the generation of such data in the first place.[415]

Overall, it is unclear whether small companies and consumers are actually going to be the main beneficiaries of the DMA and the obligations imposed by it on *gatekeepers*. It appears likely that *gatekeepers* will, at the same time, be the biggest winners and losers of the DMA, in the sense that they will have to provide access to data relevant to competition and to their business model, while at the same time being able to access such data provided by competing gatekeepers and to process and incorporate such data in an efficient way that may improve their services to advertising customers and some other groups of business users. This is likely to recalibrate data relations between gatekeepers in a significant way. In this sense, the effects of the DMA may also have a geopolitical implication, in that Chinese tech companies may be able to gain access to data from established European and U.S. gatekeepers under the DMA, so as to expand their offering in the European Economic Area.[416] Similarly, existing European and U.S. *gatekeepers* may rely on the DMA provisions to expand into adjacent product markets which they do not currently have a strong market position in. To curtail these developments may be the role of competition law.[417] At this early stage, it is hard to tell which group of gatekeepers will benefit the most from such recalibration and whether a developed interpretation of some of the obligations in the DMA by the Commission's future enforcement actions or guidelines will help to clarify this question. However, consumers and small business users may be able to benefit from these provisions even if they primarily strengthen gatekeepers.[418] For instance, it is conceivable that the data made available to gatekeepers will allow them to offer consumers and business users improved or cheaper services due to the competitive pressure exercised on gatekeepers by other gatekeepers—especially if the additional data will facilitate entry into some digital markets by gatekeepers who were not present in them before, or will facilitate users switching providers from one gatekeeper's service to another gatekeeper's service with a previously low market share.[419]

V. CONCLUSION

Overall, the DMA is an important step in addressing data-related competition problems in digital markets, which will significantly widen the European Commission's enforcement toolbox in taming the data-derived dominance of gatekeepers for years to come. The DMA will recalibrate data relations between *gatekeepers* and the users of their services in favor of the latter, who—due to their dependence on the gatekeepers—would not otherwise

415. *Id.*

416. *See* Glenn S. Gerstell, *China Is the Elephant in the Room as Europe Targets American Tech*, BARRON'S (June 7, 2021, 7:00 AM), https://www.barrons.com/articles/china-is-the-elephant-in-the-room-as-europe-targets-american-tech-51622843886 (discussing the tensions between American, European, and Chinese data policy).

417. *See id.* (discussing competition policy).

418. *See* Section II.B.3.c (discussing the provision of search data to competitors).

419. *Id.*

have effective recourse against gatekeepers' leveraging of data-derived advantages, and, due to the specific characteristics of digital markets, would lack any reasonable prospect of independently gaining access to data needed for effective competition. However, as this paper has shown, a closer factual look at the details of the DMA's overlap with existing EU and Member State laws and competition decisions brings to light significant ambiguities and tensions which may jeopardize the practical utility of many of the DMA's newly designed obligations and undermine legal certainty where it would be needed the most. While the DMA will probably succeed in sending an important signal to "Big Tech" that the fight against data-related abuses is a priority for the European Commission and the EU as a whole, the actual impact of the DMA on competition in digital markets will largely depend on how the Commission will make use of its new powers. One crucial factor will be whether the Commission will seek to actively engage with business users, end users, and national competition enforcers in the Member States in publishing guidelines and enforcing the obligations in the DMA, as well as balancing the competing interests of these different actors.[420] In the short term, it will be important for the Commission to engage not only with national competition authorities (NCAs), but also with Member State data protection agencies (DPAs) and the European Data Protection Board (EDPB) to ensure that its application of the DMA does not undermine the fundamental rights to data protection under EU and national laws—in particular, as regards the enforcement of data access rights created by the DMA, and gatekeepers' compliance with anonymization and sharing requirements. In the long term, however, legislators in the EU may have to strike a union-wide balance between data protection and the free movement of data as a precondition for competitive digital markets of the future, at least where a tension between the two exists. The Council and the European Parliament are arguably best positioned to make such a decision from a point of view of democratic legitimacy.

As for the current form of the DMA, the data-related access and sharing obligations on the one hand and its limitations on the collection, combination, and use of certain kinds of data on the other hand will certainly recalibrate data relations in the EU. However, as this paper has shown, it is conceivable that *gatekeepers*, rather than SMEs and consumers, will be the largest beneficiaries of the obligations imposed on other gatekeepers under the DMA. This may give rise to difficult geopolitical questions, should the main beneficiaries of data access and sharing under the DMA be Chinese tech companies wishing to enter European digital markets or to strengthen their positions vis-à-vis their U.S. competitors. Despite all this, the adoption of the DMA will be a good first move in the direction of recalibrating data relations in the EU. Once the data sharing obligations imposed on gatekeepers are teased out by future Commission guidelines, enforcement, and case law, the DMA may become an effective tool

420. The idea of seeking dialogue with members of the industry and the general public has been expressed as a priority by Alexandre De Streel in his lecture on the DMA and DSA organized as part of the NYU School of Law Global Data Law class.

for the Commission to ensure a more active contestation of digital markets, and, in some respects, a freer flow of data across the single market.

In any case, the DMA's data-sharing and access obligations are likely to result in an increased pressure on gatekeepers (even if this stems from other gatekeepers' access to data relevant to competition) to innovate and differentiate their products, benefitting consumers and business users of the gatekeepers' services. Furthermore, the DMA's recalibration of data relations between gatekeepers and the Commission is likely to allow for broader and more effective enforcement in digital markets, which may, in some cases, spill over into matters of competition law and fill the gap between competition law and economic regulation.[421] It remains to be seen whether the DMA will be adopted, what changes will be made to it in the legislative process, and how effectively the Commission will enforce the newly imposed gatekeeper obligations to improve the contestability of digital markets on fair and transparent terms.

421. *See* Schweitzer, *supra* note 15, at 5; Motta & Peitz, *supra* note 16, at 2.