Zsófia Maka*

The Interrelation between Privacy and Competition Law with Special Regard to the Obligations under the Digital Markets Act**

Abstract

The study analyses the relationship between privacy and competition law, with a particular focus on digital platforms. Digital technology is the fundamental backbone of all sectors of the modern economy. The digital platform economy is characterised by the dominance of large tech giants, acting as gatekeepers in the digital market for business users and end-users of certain products and services. Accordingly, the paper seeks to illustrate some of the regulatory efforts and the necessary link between privacy and competition law in digital markets by focusing on the failures and problems of the digital marketplace. Thus, the article first provides a brief overview of the role of data in competition law assessments. Then, the study proceeds to introduce the regulatory concept of the Digital Markets Act. Finally, the article analyses the privacy-relevant obligations of the Digital Markets Act, comparing the European Commission's original proposal and the regulatory standpoints of the European Parliament and the Council of the European Union.

Keywords: digital platforms, privacy, competition law, Digital Markets Act

* The author is a legal counsel at Vodafone Intelligent Solutions (e-mail: zsofia.maka@vodafone.com).

** At the time of the writing of this article, the proposal for a regulation on digital markets was only available as a legislative proposal of the European Commission; see 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. Since then, regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1 was adopted. However, the comparative findings of the article remain valid as a reflection of the principles of the obligations under the now adopted Regulation.

I Introduction

Digital technology is part of our daily lives, providing a vital framework for all sectors of the modern economy. The digital society is characterized by four basic characteristics, namely the irrelevance of geographical location, the key role of platforms, the importance of interconnectivity and the use of big data.[1]

As a user, the impact of the operation of tech giants, such as Google, Apple, Facebook (Meta), Amazon, and Microsoft has become more and more unavoidable. This impact is primarily reflected in the amount of available information, products, and services. At the same time, there is a price for speed, efficiency and the idea of infinite growth and innovation. This price is perceived also by the competitors and business partners of the above-mentioned platforms, which have become quasi-regulators in their markets, and also by us, as users and consumers.

As the Organisation for Economic Co-operation and Development (hereinafter OECD) remarks, the 'the use of consumer data has brought, and will continue to bring, a wide range of new and innovative goods, services and business models, often at a zero (monetary) price'; however, 'while the benefits to consumers are clear, business use of consumer data also raises concerns, such as how to preserve privacy and ensure that businesses and other actors do not use consumer data in ways that disadvantage consumers', and emphasises that 'business models based on the collection and use of consumer data also raise new questions for competition policy'.[2]

This paper defines consumer data as data concerning consumers, where such data have been collected, traded or used as part of a commercial relationship.[3] However, privacy intends to protect the proper handling of personal data, which is 'any information relating to an identified or identifiable natural person',[4] and, as a result, a narrower category than consumer data.[5]

In the following, this article aims to focus on the interrelation between the effects of two of the above-mentioned basic parameters of digital society, namely the effect of platforms

---

1 Julia Charrié, Lionel Janin, 'Le numérique, comment réguler une economie sans frontière' (2015) La note d'analyse 35, France Strategie, 67.

2 OECD Competition Committee, 'Consumer Data Rights and Competition – Background note' (2020) OECD Secretariat, 5 <https://www.oecd.org/daf/competition/quality-considerations-in-zero-price-markets-2018.pdf> accessed 14 May 2022.

3 Ibid 7.

4 The definition of personal data under 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 [2016] OJ L119/1 (hereinafter GDPR) Article 4(1).

5 Consumer data can be classified according to (i) the type of data collected, (ii) origin of the data collected, or (iii) whether consumer data can be personally identifiable. For more information see the OECD Competition Committee, Consumer Data Rights and Competition – Background notice, 7–11. It is important to note that there is a significant overlap between the categories of personal data and consumer data according to the data typology, e.g. biometric data.

and data on the relationship between competition law and privacy under the law of the European Union. Therefore, the article first briefly explores the role of data in competition law assessments. Then, the paper aims to focus on the privacy-related, but competition-law based obligations of the Digital Markets Act (hereinafter DMA), intended by the European Commission (hereinafter the Commission) to ensure contestable and fair markets in the digital sector.

II The Role of Data in Competition Law Assessments

As firms collect an increasing range of data on consumers based on the interactions with the platform's products and ancillary services, consumer privacy is a growing source of concern in digital markets; therefore, these developments 'may strengthen the argument in favour of considering privacy a dimension of competition'.[6]

Meanwhile, privacy tends to focus on the 'protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data,' competition policy aims to prohibit firms from engaging in conduct that will distort the competitive process and thus harm competition. Goals of competition policy mostly include (economic) efficiency and consumer welfare; however,

> the increasing market concentration and astronomical valuation of a small cluster of star technology firms […] re-ignited the debate on whether competition law is strictly limited to economic goals or whether it also pursues broader socioeconomic goals such as wealth redistribution and fairness.[7]

However, competition policy and privacy also share a number of interconnected goals, such as building trust in markets, advocating for data portability which also encourages switching between platforms, resulting in a renewed emphasis on the role of data in competition.[8] Competition law thus seeks to benefit consumers through a broad, economic efficiency prescription, rather than the individualised rights or interests that are characteristic of privacy law. So while competition policy is not framed in terms of individualised rights or

[6] OECD Competition Committee, 'Quality considerations in the zero-price economy', (2018) OECD Secretariat, 12 <https://www.oecd.org/daf/competition/quality-considerations-in-zero-price-markets-2018.pdf> accessed 14 May 2022.

[7] Konstantinos Stylianou, Marios Iacovides, 'The goals of EU competition law – A Comprehensive empirical investigation' (2020) Konkurrensverket 4 <https://www.konkurrensverket.se/globalassets/dokument/kunskap-och-forskning/forskningsprojekt/19-0407_the-goals-of-eu-competition-law.pdf> accessed 14 May 2022.

[8] Erika M. Douglas, 'Digital Crossroads – The Intersection of Competition Law and Data Privacy, Report to the Global Privacy Assembly Digital Citizen and Consumer Working Group' (2021) Temple University 34–62.

interests, it seeks to achieve the benefits of individual consumers collectively through the protection and promotion of competition and thus ensuring economic efficiency.[9]

In addition, competition law and privacy both share the policy interest in advocating consumer choice, but for distinct reasons. Privacy promotes consumer choice by granting the individual data subject the right to give their consent to the data-processing activities of platforms described in their privacy notice,[10] meanwhile. competition law considers (consumer) choice concerning products from the point of view of consumer welfare.

However, certain demand-side problems (collectively termed *demand-side distortions*) may hamper the functioning of markets and the free, effective choice of consumers, namely information asymmetries and consumer behavioural biases.[11]

Consumers tend not to read long and ubiquitous terms and conditions of service before giving their consent to data processing. However, as the products offered on digital markets are complex and consumers may not be able to grasp the implications of allowing data collection, consumer-decision making may not be able to discipline firms' behaviour in general.[12] Consumers may be susceptible to manipulation also thanks to the use of so-called *dark patterns,* which are manipulative user interface designs that nudge consumers to take unintended actions that may not be in their interest and thus precluding them from exercising their consent in a meaningful way.[13]

There are also significant consumer behavioural biases, as consumers may decide that they do not need to consider any variation in quality, since they receive the product for free thus overvaluing the zero-priced product (the *free effect*); this is especially true when the free product is tied to a positively-priced good, so it may be used by companies to drive a competitor out of the market.[14] Coupled with the free effect, the 'privacy paradox' refers to the practice when consumers claim to be concerned about their privacy but they are ready to give consent to the collection of their (personal) data for minimal rewards. Finally, consumers also have 'inertia bias,' whereby they stick to the use of a service or product for convenience even when the quality of the service or product is declining.[15]

To conclude, privacy and competition law share many goals and common challenges. This statement is especially true considering that the collection and use of consumer data is

[9] Douglas (n 8) 38.

[10] Article 6(1)(a) point of the GDPR lists consent as one of the six grounds for lawful data processing stating, that 'processing shall be lawful only if and to the extent that at least one of the following applies: (…) the data subject has given consent to the processing of his or her personal data for one or more specific purposes'.

[11] Douglas (n 8) 56–62.

[12] OECD Competition Committee (2018) (n 6) 24–26.

[13] Norwegian Consumer Council-Forbrukerrådet, 'Report, Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy' (2018) 4 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 14 May 2022.

[14] OECD Competition Committee (2018) (n 6) 26.

[15] See also Vladimir Bastidas Venegas, 'Consumer Inertia, the New Economy and EU Competition Law' (2018) 2 (1) Market and Competition Law Review 47–53. https://doi.org/10.7559/mclawreview.2018.332

the core business of many firms[16] therefore the collection and ownership of data, and access to that information might impact competition, and privacy may be a factor in competition law, 'where companies compete to offer privacy products or features to consumers in a market.'[17] It is also important to note that 'price is only one dimension of competition between firms', and, in zero-price markets such as digital markets, quality is the only parameter that affects consumer welfare.[18] Therefore, traditional drivers of competition, such as price efficiency and low cost, are now being replaced by data-related innovation and differentiation in connection with digital platforms.[19]

III The Regulatory Concept of the Digital Markets Act

On 15 December 2020, the Commission published the Digital Services Package, one element of which is the draft proposal for the DMA, which aims to ensure fair and competitive markets in the digital sector.

Furthermore, problems in digital and related markets, such as network effects,[20] lock-in effects such as consumer lock-in[21] and the lack of multi-homing[22] coupled with the potentially abusive behaviour of companies with market power in digital markets, can pose a serious threat to competition on digital platforms. At the same time, certain established market structural characteristics, such as high concentration or excessive data collection, may lead to a partial or complete absence of competition in the relevant markets despite the absence of anti-competitive behaviour by undertakings.

There were many attempts throughout the years to address the above-mentioned problems at the level of market regulation, whether through competition law, consumer protection or data protection. However, the aim of the DMA is to ensure that these abuses can be addressed not only after the event, but before the abusive situations arise. As was the case with the liberalisation of the telecommunication or energy markets, the DMA seeks to limit the risks arising from the economic power of large platform providers, essentially by ensuring the conditions for competition in the wholesale market and by a form of access regulation.[23]

---

16 OECD Competition Committee (2020) (n 2) 24.

17 Douglas (n 8) 62.

18 OECD Competition Committee (2018) (n 6) 6.

19 Frédéric Jenny, 'Competition law enforcement and regulation for digital ecosystems: Understanding the issues, facing the challenges, and moving forward' (2021) (3) Concurrences 50.

20 The more people use a platform, the higher is its value, which attracts even more users.

21 A firm's strategy, which makes it significantly more difficult for customers to switch to another firm's service.

22 Consumer behaviour whereby the consumers use multiple rival bilateral markets (e.g., parallel use of Foodpanda and Wolt).

23 Polyák Gábor, Pataki Gábor, Gosztonyi Gergely. Szalay Klára. 'Versenyjogi előzmények és piacszabályozási eszközök a digitális piacokról szóló európai rendelet tervezetében' (2021) (1) Verseny és Szabályozás 148.

Thus, the DMA intends to define *ex ante* the obligations inspired by competition law proceedings, and the so-called gatekeeper undertakings must comply with these obligations in any event. Abuse of dominance proceedings based on individual fact-finding are not sufficiently effective or swift, and the fines imposed as a result of the proceedings are often only a cost of doing business for the undertakings. In order to prevent this, the DMA systemically prohibits certain types of business practices, thereby providing less opportunity for the undertakings concerned to rely on individual and specific market circumstances in a given case, thus having a greater deterrent effect than fact-specific antitrust proceedings.[24]

It is important to stress, however, that the DMA builds on an approach that accepts the role of platforms as market regulators as an inevitable part of their business model and focuses on and seeks to address market failures in digital markets rather than dismantling them.[25]

The DMA can also be described as a sector-specific competition law legislative product, since, as indicated in recital 10 of the DMA:

> [...] the purpose of this Regulation is complementary to, but different from, the objective of protecting undistorted competition in any given market from a competition law perspective, as it seeks to ensure that the markets in which gatekeepers are present are and remain contestable and fair markets, irrespective of the actual, likely or perceived effects that the conduct of a particular gatekeeper covered by this Regulation may have on a given market. [...].

Regarding the form of the act, the Commission considered that a Regulation was necessary because of the cross-border, global nature of the functioning of online platform services; this is the only way to ensure uniform minimum standards across Member States to avoid regulatory fragmentation. This is also reflected in Article 1(5) of the DMA, which states that

> Member States shall not, by their laws, regulations or administrative measures, impose additional obligations on gatekeepers in order to ensure contestable and fair markets. This is without prejudice to other legitimate public interest rules in conformity with Union law.

IV Privacy-relevant Obligations under the Digital Markets Act

Digital platforms or ecosystems generate specific problems that need to be tackled. As highlighted by the German Commission for 'Competition Law 4.0':

---

[24] Nicolas Petit, 'The proposed Digital Markets Act (DMA): A legal and policy review' (2021) 12 (7) Journal of European Competition Law & Practice 530. https://doi.org/10.1093/jeclap/lpab062

[25] Martin Eifert, Axel Metzger, Heike Schweitzer, Gerhard Wagner, 'Taming the giants: The DMA, DSA package' (2021) 58 (4) Common Market Law Review 994. https://doi.org/10.54648/COLA2021065

> The combination of dominance on the platform market with a gatekeeper position and rule-setting power gives rise to the risk of distorted competition on the platform and the expansion of market power from the platform market to neighbouring markets. In view of the strong steering effect that platforms can exert on their users' behaviour, the often rapid pace of development on digital markets and the importance of first-mover benefits, non-intervention or late intervention against abusive behaviour typically comes at a very high price.[26]

Additionally, the timeliness and effectiveness of *ex ante* competition policy and enforcement also aims to address *structural features* of digital markets that may prevent entry and expansion by new players, both supporting competition in the market and competition *for*[27] the market.[28] This approach led to the *asymmetric nature* of the DMA, as it only applies to some companies in the market, rather than evenly across the board.[29]

This resulted in the preamble (5) of the DMA, stating

> Whereas Articles 101 and 102 TFEU remain applicable to the conduct of gatekeepers, their scope is limited to certain instances of market power (e.g., dominance on specific markets) and of anti-competitive behaviour, while enforcement occurs *ex post* and requires an extensive investigation of often very complex facts on a case by case basis. Moreover, existing Union law does not address, or does not address effectively, the identified challenges to the well-functioning of the internal market posed by the conduct of gatekeepers, which are not necessarily dominant in competition-law terms.

Thus, Articles 5 and 6 of the Commission's proposal for the DMA contain a number of obligations and prohibitions with which gatekeepers will need to comply. While the purpose of these obligations is to ensure contestable and fair markets in the digital sector, some of them are relevant from a privacy aspect as well. This is not surprising in the light of the extensive academic analysis, as competition law and privacy are increasingly intertwined in the digital sector; some of the obligations under the DMA even make clear references to the GDPR.

Hence, it is already important to emphasise that the DMA and the GDPR need to interact with each other in a way that does not undermine the effectiveness of neither legislative act, bearing in mind that the two legislative acts work with different enforcement

---

[26] Kommission Wettbewerbsrecht 4.0, 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bundesministerium für Wirtschaft und Klimaschutz' (2019) 19 <https://www.bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.html> accessed 14 May 2022.

[27] In the digital economy, firms strongly compete for the market and not in the market.

[28] OECD Competition Committee, 'Ex ante regulation and Competition in Digital Markets' (2021) OECD Secretariat 13 <https://www.oecd.org/daf/competition/ex-ante-regulation-and-competition-in-digital-markets-2021.pdf> accessed 14 May 2022.

[29] Marco Botta, 'Sector Regulation of Digital Platforms in Europe: Uno, Nessuno e Centomila' (2021) 12 (7) Journal of European Competition Law & Practice European University Institute 505. https://doi.org/10.1093/jeclap/lpab046

mechanisms and regimes. While the DMA indicates its provisions are 'without prejudice' to the GDPR,[30] nothing indicates how these situations need to be addressed.

Instead of prescribing *ex ante* obligations, several academics advocated a principles-oriented approach, which looks like 'a random selection of past and ongoing cases'. The following principles were considered by the expert panel assisting the European Parliament's (hereinafter Parliament) Committee on Internal Markets and Consumer Protection *contestability of markets, fairness of intermediation and independence of decision*.[31]

As part of the third principle, the study also stresses that gatekeepers must not undermine the independent decision-making of economic actors, as it is the basic liberty of everyone engaging in markets and the 'cornerstone of the market economy'. In addition, it considers that if core platform services set their own markets and restrict user sovereignty with their technical abilities then, eventually, the code of tech-giants may hold more importance than the 'legal obligations set by democratic institutions'.[32]

The study aims to tackle these problems by stating that consumers must enjoy data sovereignty over the 'use of their data', have a real choice regarding products and services, and users (even business users) must enjoy free communication. Thus, it introduces 'additional obligations', restricting the gatekeeper from undermining 'real choice' and 'free communication', while prescribing that 'the gatekeeper must give real choice to users, based on adequate information and a neutrally designed menu of choices before connecting further products, tools or services with the core platform service'.[33]

However, it must be noted that while the principle-based approach provides much flexibility, its uncertainty may undermine the effective implementation of the DMA, as it leaves too much room for interpretation and possible efficiency claims of gatekeepers for non-compliance, in contrast to the rigid clarity of *ex ante* obligations.

The following subchapters analyse the privacy-relevant obligations of the DMA, starting with the Commission's proposal, then covering both the proposals of the Council of the European Union (hereinafter Council) and the Parliament, if relevant.

1 The Obligation to Refrain from the Combination of Personal Data

According to Article 5(a) of the DMA, gatekeeper undertakings must

[30] Preamble (11) of the 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.

[31] Rupprecht Podszun, Philipp Bongartz, Sarah Langenstein, 'Proposals on how to improve the Digital Markets Act Policy paper in preparation of the information session on the Digital Markets Act in the European Parliament's Committee on Internal Market and Consumer Protection (IMCO) on 19 February 2021' (2021) Heinrich Heine University of Düsseldorf, 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3788571> accessed 14 May 2022.

[32] Ibid 6.

[33] Ibid 7.

> refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679

in respect of each of its core platform services identified pursuant to Article 3(7).

The roots of the obligation can be traced back to the already analysed Facebook case, whereby Facebook applied terms and conditions that made the use of its social network conditional upon Facebook's possibility to collect and combine user data from multiple sources. Additionally, the Impact Assessment conducted in relation to the DMA[34] (hereinafter Impact Assessment) listed another relevant case, whereby the Italian National Competition Authority fined WhatsApp 3 million euro for having *de facto* forced its users to share their personal data with Facebook, by inducing them to believe that, unless they granted such consent, they would no longer have been able to use the service.[35]

Additionally, the European Data Protection Board (hereinafter EDPB) noted in its Guidelines that the ability of certain social media providers to combine a higher quantity and diversity of personal data may increase the ability to offer more advanced targeting campaigns, which may be relevant regarding the in-depth profiling of the persons concerned and the fact that unrivalled insight capabilities provided by the platform may make it an 'unavoidable trading partner' for online marketers.[36]

It is also important to note that the GDPR already prohibits the re-use of data collected for purposes other than those for which they were originally collected, unless the option of opt-out is provided.[37] However, big platform may circumvent it by applying re-use clauses in their offered Terms of Service.[38]

The European Data Protection Supervisor (hereinafter EDPS) welcomed the provision in its Opinion 2/2021 on the Digital Markets Act (hereinafter EDPS Opinion) but suggested it must be clarified that gatekeepers still need to obtain consent from data subjects, and that

---

[34] Commission Staff Working Document, 'Executive summary of the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' (2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0364> accessed 14 May 2022.

[35] 'WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook', press release <https://en.agcm.it/en/media/press-releases/2017/5/alias-2380> accessed 14 May 2022.

[36] EDPB, Guidelines 8/2020 on the targeting of social media users Version 1.0 Adopted on 2 September 2020 <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf> accessed 14 May 2022.

[37] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP 203) (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2013/wp203_en.pdf> accessed 14 May 2022.

[38] Daniele Condorelli, Jorge Padilla, 'Harnessing platform development in the digital world' (2020) 16 (2) Journal of Competition Law & Economics, Oxford University Press, 30. https://doi.org/10.1093/joclec/nhaa006

'the functionalities for giving information and offering the opportunity to grant, modify or revoke consent should be as user-friendly as possible'.[39]

The Council's General approach did not make many amendments to the provision, but clarified that the gatekeepers may also rely on the legal basis included under Article 6(1) points (c), (d) and (e) of the GDPR, where applicable, and included the recommended user-friendly solution to request consent in preamble (36).[40]

However, the Parliament's Plenary Position (hereinafter: Plenary Position) included additional requirements on the use of data for targeted or micro-targeted advertising and the interoperability of services, e.g. number-independent interpersonal communication services and social network services [Article 6(aa)].[41] The relevant amendment stipulates that a gatekeeper should, for its own commercial purposes and the placement of third-party advertising in its own services, refrain from combining personal data for the purpose of delivering targeted or micro-targeted advertising, except if there is a clear, explicit, renewed, informed consent, in line with the General Data Protection Regulation. Moreover, according to the Plenary Position, personal data of minors must not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. In this way, the Parliament made a more ambitious step towards weakening the impact of gatekeepers, but there is no available impact assessment on the possible effects of the provision, which may be part of an extensive debate during the trialogues.

To conclude, platforms' access to personal data has ambiguous effects, as it can offer a better and wider variety of relevant products and services through personalisation, but less competition can enter the market, possibly resulting in higher costs for consumers. Hence, intervention is necessary, but the milder position of the Council may have fewer unintended effects in the long run.

2 The Prohibition of Requiring Business-users and End-users to Subscribe to or Register with Any Other Core Platform Service

Article 5(f) of the Commission's proposal prescribes gatekeepers to

> refrain from requiring business users or end users to subscribe to or register with any other core platform services identified pursuant to Article 3 or which meets the thresholds in Article 3(2)

[39] EDPS, 'Opinion 2/2021 on the Proposal for a Digital Markets Act' (2021) 9-11 <https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf> accessed 14 May 2022.

[40] Council of the European Union 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) – General approach' <https://data.consilium.europa.eu/doc/document/ST-13801-2021-INIT/en/pdfy> accessed 14 May 2022.

[41] European Parliament 'Amendments adopted by the European Parliament on 15 December 2021 on the 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)0842 – C9-0419/2020 – 2020/0374(COD))(1)' <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0499_EN.html> accessed 14 May 2022.

(b) as a condition to access, sign up or register to any of their core platform services identified pursuant to that Article.

The Impact Assessment also lists the Google Android case as the inspiration for the obligation. The Commission fined Google as it abused its dominant position in the market for general internet search services, licensable smart mobile operating systems and app stores for the Android mobile operating system.[42] The abuse happened due to the fact that Google required manufacturers to pre-install the Google Search app and browser app (Chrome) as a condition for licensing Google's app store (the Play Store), made payments to certain large manufacturers and mobile network operators on condition that they exclusively pre-installed the Google Search app on their devices; and prevented manufacturers wishing to pre-install Google apps from selling even a single smart mobile device running on alternative versions of Android that were not approved by Google (so-called 'Android forks').[43]

The Commission found that Google's practice had reduced the incentives for manufacturers to pre-install competing search apps, as well as the incentives of users to download such apps. This reduced the ability of rivals to compete effectively with Google. As can be seen, tying and bundling[44] or other related practices like pre-installed apps may be used as a means to foreclose competition. There are some welfare effects of tying and budling, for example, Google mandates users of their location-based services to use a Google-approved version of Android as well.[45]

The EDPS Opinion also welcomes Article 5(f) of the DMA, as it both 'mitigates competition concerns' with regard to compulsory 'bundling of services' and 'reduces excessive collection and combination of personal data' without encroaching upon the GDPR, as the prohibition is justified due to the unique position of gatekeepers and the functioning of the platform economy.[46] The obligation also enjoyed support from the other legislators, as only minor amendments were made in relation to the relevant obligation.

---

[42] Case AT.40099-Google Android-Commission Decision of 18 July 2018, <https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf> accessed 14 May 2022.

[43] Press release: Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine: <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581> accessed 14 May 2022.

[44] Tying occurs when a supplier makes the sale of one product (the tying product) conditional upon the purchase of another (the tied product) from the supplier (i.e. the tying product is not sold separately). Bundling refers to situations where a package of two or more products is offered at a discount.

[45] Luís Cabral, Justus Haucap, Geoffrey Parker, Georgios Petropoulos, Tommaso Valletti, Marshall Van Alstyne, 'The EU Digital Markets Act: A Report from a Panel of Economic Experts' (2021) Luxembourg Publications Office of the European Union, 12 <https://publications.jrc.ec.europa.eu/repository/handle/JRC122910> accessed 14 May 2022.

[46] EDPS Opinion paragraphs (n 39) 25–26.

3 The Obligation to Allow End-users to Un-install Any Preinstalled Software Application

Article 6(1)(b) of the Commission's proposal would

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

The relevant obligation shares the same background as the prohibition under Article 5(f). As the Impact assessment also mentions, there is a strong consumer bias towards pre-installed software and names the previously cited Google Android and the famous Microsoft (tying) antitrust decisions[47] as examples.[48]

Compared to the Commission's proposal, the General approach also mandates the gatekeepers to 'technically enable end users to un-install any software applications on an operating system the gatekeeper provides or effectively controls as easily as any software application installed by the end user at any stage'. In addition, gatekeepers have to provide for end users to be able to change default settings on an operating system that direct or steer end users to products or services offered by the gatekeeper. The gatekeeper may restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third parties.

In contrast, the Parliament moved the relevant obligation under Article 5. According to the new obligation under Article 5(gb), in addition to making un-installing possible, 'from the moment of end users' first use of any pre-installed core platform service on an operating system,' gatekeepers 'have to prompt end-users to change the default settings for that core platform service to another option from among a list of the main third-party services available'. While it is not clear from the wording of the Article what 'prompting' end users would mean in practice, the obligation could be fulfilled in the form of a choice screen/preference menu, also referencing the already cited Google Android decision.[49]

Therefore, while the Parliament's position is aligned with the Commission's practice, the obligation under Article 5(gb) would apply to any core platform service, thereby possibly having a negative impact on user experience. Thus, the Parliament's position could be a step in the right direction, but the scope of the obligation should be limited to online search engines.

---

[47] Case AT.39530 Microsoft (Tying), Commission Decision of 16 December 2009 <https://ec.europa.eu/competition/antitrust/cases/dec_docs/39530/39530_2671_5.pdf> accessed 14 May 2022.

[48] Impact assessment 56.

[49] Case AT.40099-Google Android-Commission Decision of 18 July 2018, 222, paragraph 971.

4 The Obligation to Provide Effective Portability of Data Generated through the Activity of a Business-user or End-user

Article 6(1)(h) of the Commission's proposal requires the gatekeeper to

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

As previously indicated in the study, granting access to data through data portability is critical in handling the negative consequences of network effects, as consumers are allowed to switch between services, without losing all the benefits linked to the use of the same product or service and competitors may gain access to the necessary (personal) data.[50]

Article 6(1)(h) is greatly inspired by the data portability right for natural persons in Article 20 of the GDPR and grants a similar right to business users to access their commercial transactions and interaction data.[51] However, the obligations under Articles 6(1)(h) and 6(1)(i) go *beyond* the GDPR in the sense that they mandate 'continuous and real-time access'. Considering the 'number of technical, legal, and economic obstacles'[52] granted to data subject under Article 20 of the GDPR, several critics advocated for an alternative approach, granting individuals *in-situ rights* to access end user data.

Thus, instead of transferring the relevant data from a gatekeeper to the given business user, the latter would have the possibility of running third party algorithms on the data available on the gatekeeper's server.[53] This approach would mean that the data would retain their multiparty context not losing their original interpretation, and the data being recent and not separated from the relevant infrastructure, retain their adaptability.[54] However, this approach also needs to be complemented by a sound regulatory approach regarding algorithm interoperability.

The EDPS Opinion recalled that under Article 20 of the GDPR, as clarified by the Article 29 Working Party and later confirmed by the EDPB,[55]

---

[50] OECD Competition Committee (2021) (n 28) 40.

[51] Cabral, Haucap, Parker, Petropoulos, Valletti, Van Alstyne (n 45) 21.

[52] For more information, see Jan Krämer 'Personal data portability in the platform economy', (2020) 17 (2) Journal of Competition Law and Economics and Emmanuel Syrmoudis, Stefan Mager, Sophie Kuebler, Wachendorff, Paul Pizzinini, Jens Krosslags, Johann Kranz, 'Data Portability between Online Services – An Empirical Analysis on the Effectiveness of GDPR Art. 20' (2021) (3) Proceedings on Privacy Enhancing Technologies 351–372. https://doi.org/10.2478/popets-2021-0051

[53] Cabral, Haucap, Parker, Ptropoulos, Valletti, Van Alstyne (n 45) 22.

[54] Ibid.

[55] Guidelines on the right to data portability, Adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233> accessed 14 May 2022.

> the scope of the personal data which can be 'ported' encompass the personal data provided knowingly and actively by the data subject, as well as the personal data generated by his or her activity (provided the legal basis of the processing is consent or contract [...].[56]

Therefore, the EDPS Opinion welcomed the phrasing of 'generated through his activity' clause of the Commission's proposal.

However, the EDPS Opinion considered that the wording of the obligation should be more precise as to who would be entitled to port personal data and what data, if personal or non-personal. Therefore, the EDPS recommended specifying that a gatekeeper shall provide the end-user with tools to facilitate the effective portability of the personal data relating to them, 'including personal data generated through her or his activity as end-user of platform services in accordance with Article 20 of Regulation 2016/679, including by the provision of continuous and real-time access'.[57]

Neither the General approach of the Council, nor the Plenary Position of the Parliament opted for the 'personal data' clause but included the 'provide end users or third parties authorised by an end user, upon their request and free of charge with effective portability of data' reacting partly to the critics and making a step forward.

5 The Obligation to Provide Real-time Access and Use to Aggregated and Non-aggregated Data

According to Article 6(1)(i) of the Commission's proposal, gatekeepers must

> provide business users, or third parties authorised by a business user, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users; for personal data, provide access and use only where directly connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end user opts in to such sharing with a consent in the sense of the Regulation (EU) 2016/67.

The obligation is an example whereby 'consumer privacy rights take precedence'; consent is an essential precondition to businesses accessing end user data. Article 6(1)(i) is important from this point of view, as, per the obligation, *free access* is provided to all types of data, including the data provided by end users and generated through their activity and aggregated

[56] EDPS Opinion (n 39) 21.
[57] Ibid.

However, the EDPS Opinion raised some concerns as to the wording of the obligation, which could be inconsistent with the GDPR. According to the EDPS, the draft obligation of the Commission's proposal could create the misconception that aggregated data or non-aggregated data might not include personal data.

The EDPS also called for a more specific reference to the GDPR in the sense that access should be provided to generated and provided *non-personal data*, and that gatekeepers shall provide *in full compliance with the GDPR,* business users the possibility to obtain the consent of the data subject, allowing to the business users the access to and use of the *personal data* 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.[58] Therefore, there would have been an important distinction between the two aspects of the obligation.

In contrast, the General approach clearly extended the first part of the obligation to personal data, while the Plenary position did not mention it. However, the General approach mainly maintained the Commission's wording but added, that consent and opt-in is a precondition to access and use of personal data. The Plenary Position did similarly but made a more specific reference to the GDPR.

Thus, the Council's General approach was more specific regarding to the first aspect of the obligation, meanwhile, the Plenary position was more precision as to the second part of the obligation.

6 The Obligation to Provide Third-party Providers of Online Search Engines with Access to Query, Click and View Data

Article 6(1)(j) of the Commission's proposal mandates the gatekeepers to

> provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data.

By providing access to ranking, query, click and view data under fair, reasonable and non-discriminatory terms, contestability may be ensured through granting third-party providers the possibility to improve their services and thus compete with the core platform service of the gatekeeper.[59] In practice, Google Search data would be available to competitors struggling to enter the market and 'would redistribute users' across smaller search engines,

[58] EDPS Opinion (n 39) 11.

[59] Recital 56 of the DMA states, that the obligation under Article 6(1)(k) aims to allow 'third-party providers [to] optimise their services and contest the relevant core platform services'.

a minor part of the impact of network effects could be eroded.[60] In addition, by combining the obligations under Article 6(1)(i) and Article 6(1)(j), business users will have free real-time continuous access to data generated by them and by end users when using their services in the context of the gatekeeper's core platform.[61]

The EDPS Opinion made the important remark that query, click and view data in relation to searches generated by individuals constitute personal data and may even be of a 'highly sensitive nature because they can contribute to building up a profile of individuals' preferences, status (including health status), interests (including religious and political beliefs) and convictions'.[62] The EDPS also recommended specifying in a recital that the gatekeepers should be able to demonstrate that 'anonymised query, click and view data have been adequately tested against possible re-identification risks', as re-identification may happen due to the carelessness of data controllers in practice.

It is worth noting, that both the Council and the Parliament approved the relevant obligation. Additionally, the Council also included in preamble (56),

> that the relevant data is anonymised if personal data is irreversibly altered in such a way that information does not relate to an identified or identifiable natural person or where personal data is rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The Council honoured the recommendation of the EDPS in this way.

7 The Obligation to Submit an Independently Audited Description of Any Techniques for Profiling Consumers

According to Article 13 of the Commission's proposal, the gatekeeper shall submit to the Commission an independently audited description of any techniques for profiling consumers that the gatekeeper applies to or across its core platform services identified pursuant to Article 3 within six months after being designated as a gatekeeper. This description should be updated at least annually.

Per the EDPS Opinion, the obligation under Article 13 'provides another clear example of the strong complementarity between competition law and data protection law'.[63] The EDPS Opinion also welcomed the obligation as it may reduce the 'data driven advantage' of the gatekeeper and the information asymmetry between it and public authorities and data subjects on the processing of personal data. Therefore, the obligation could also contribute to identifying consumer profiling that is not proportionate, or otherwise not compliant with the GDPR.

---

[60] Cabral, Haucap, Parker, Petropoulos, Valletti, Van Alstyne (n 45) 23.
[61] OECD Competition Committee (2021) (n 28) 43.
[62] EDPS Opinion (n 39) 12.
[63] EDPS Opinion (n 39) 13.

In the spirit of effective coordination, the EDPS also recommended sharing 'any relevant materials that are collected in the context of supervising the gatekeepers that relate to the processing of personal data'[64] with any competent supervisory authority represented in the European Data Protection Board, upon its request. The EDPS Opinion also suggested adding a reference to Article 4 (4) of the GDPR insofar as the profiling of end users or consumers is concerned, as the two definitions should have the same meaning.

In the course of the legislative negotiations, both the Council and the Parliament recommended adding an obligation for gatekeepers to 'make publicly available an overview of the audited description, taking into account possible limitations involving business secret'.

The Parliament also suggested adding that 'the Commission shall develop, in consultation with the EU Data Protection Supervisor, the European Data Protection Board, civil society and experts, the standards and procedure of the audit'.

As the relevant obligation is closely associated with both privacy and competition law, the Parliament's Plenary Position is forward-looking. Meanwhile, the 'publication' of the audited description is also progressive, as it could remove data-driven advantages and information asymmetry regarding profiling, in line with the remarks of the EDPS Opinion.

V Conclusions

Competition law aims to maintain the competitive process with economic efficiency and fairness in hindsight. Meanwhile, privacy protects the individual's right to 'be left alone' and the inner layer of an individual's life and its fundamental right of protection of personal data. However, privacy and competition law have continued to interact more and more in the recent decades, thanks to the peculiarities of the digital revolution.

The regulatory environment tried to address these challenges and market failures using the tools of competition law, consumer protection and data protection. This led to the creation of the DMA, which can be regarded as a sector-specific *ex ante* competition law instrument. Thus, the DMA accepts the quasi-regulatory role of platforms, and it specifies the obligations under Articles 5 and 6 inspired by previous competition law proceedings *ex ante,* thus providing for a swift intervention.

The obligation to refrain from the combination of personal data stems from the Facebook case pursued by the *Bundeskartellamt*. The Council's General approach only added minor amendments and clarifications to the provision, but the Parliament took an ambitious but ambiguous step without an available impact assessment on the possible effects of the provision, which may be debated.

The DMA also seeks to address the 'tying and bundling' practices of gatekeepers in relation to privacy in the form of *the prohibition to require business and end users to*

[64] Ibid.

subscribe to or register with any other core platform service and the obligation to allow end users to un-install any pre-installed software application. As previously indicated, these practices may also have positive effects on consumer welfare but have a great possibility of foreclosing competition on the market. However, the Plenary position moved the un-installing obligation under Article 5, thus precluding the chance for regulatory dialogue. In addition, the Parliament extended the relevant obligation to any core platform service, which may have negative effects on user experience and competition.

The obligation to *provide effective portability of data generated through the activity of a business user or an end user* and *the obligation to provide real-time access and use to aggregated and non-aggregated data* also work hand in hand. The first obligation has a strong resemblance to the aims of Article 20 of the GDPR and would also share its fate when it comes to the difficult application of the provision. Therefore, several critics considered granting in-situ rights, meanwhile the other two European legislators mainly considered the original approach of the Commission. In the case of the latter obligation, the General approach added that consent and opt-in are preconditions to access and use of personal data and made it clear that the first part of the obligation also covers personal data.

The obligation to provide third-party providers of online search engines with access to query, click and view data is also important from position that query, click and view data may be of a highly sensitive nature. Therefore, it is forward-looking to point out that effective anonymisation is essential.

Finally, the *obligation to submit an independently audited description of the techniques applied by gatekeeper undertakings for profiling customers* may be crucial in removing data-driven advantages and information asymmetry regarding the profiling of customers. Both the Council and the Parliament included an obligation for gatekeepers to 'make publicly available an overview of the audited description, taking into account possible limitations involving business secret'.

To conclude, the DMA may play a decisive role in shaping the rules of the game in the digital sphere. Hopefully, the DMA will shake up the digital sector in its core and will lead to more customer and competition-friendly, privacy-respecting digital markets.