Digital Competition Law and Data Privacy in the EU

The Overlap and Interplay between GDPR, Article 102 TFEU, and DMA

Oskar Nilsson

Master's Thesis in European and International Trade Law

HARN63

Spring 2023

LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

Table of Contents

Abstract

Large digital platforms impact the entire internal market of the EU. In particular, three challenges characterise their relationship with businesses and end-users, "access to data", "imbalanced bargaining power", and "degrading data privacy", where the common denominator is personal data. This thesis investigates to what extent these challenges are regulated in the GDPR, Article 102 TFEU and the DMA, together with the plausible overlap and interplay between the three legal frameworks. The study is thus framed in three regulation specific questions and one comparing and analysing question. The purpose-oriented part of the thesis is divided into three chapters, one for each research question, together with the corresponding fourth research question. The overarching approach is to move from "practical" to "theoretical", i.e., initiating with case-law by the EU Courts, then viewpoints by relevant EU institutions, and finishing with theories by legal scholars, when investigating each challenge. Due to a relevant and financially strong sector, the material is of both high quality and current.

Each legal framework could theoretically be applicable to each challenge, but to various extents and practical vs theoretical depth. The study further concludes that the predominant overlap is between the data portability provisions in the GDPR and the DMA respectively, questioning the "without prejudice" clause of the DMA. Furthermore, the predominant interplay is between the Article 102 TFEU and the GDPR, by using lack of "choices" and data protection principles as benchmarks for determining abuse. Beyond this, the thesis broadly investigates, if the three legal frameworks could theoretically be applied to the same challenge, following the *bpost* case the CJEU enabled the Commission to apply two legal frameworks side-by-side (competition rules and sector-specific rules), thus raising the question if a third could be possible. Either way, it can be concluded that the three provisions can be applicable to similar situations, but in accordance with EU law, the CJEU has the final say in the interpretation and application of the three legal frameworks, according to Article 19(1) TEU.

Foreword

Initially, I want to thank the Department of Business Law at Lund University, for both current and captivating learning opportunities. In particular, I want to express my gratitude to Professor Jörgen Hettne, for interesting comments on the thesis' Competition Law aspects, and Senior Lecturer Jonas Ledendal, for our intriguing discussion on the thesis' Data Privacy aspects. Finally, I want to thank my supervisor, Senior Lecturer Johan Axhamn, for invaluable feedback and guidance throughout the writing process.

Abbreviations

AG	Advocate Generals
WP29	Article 29 Working Party
CJEU	Court of Justice of the European Union
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
DMA	Digital Markets Act
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
GDPR	General Data Protection Regulation

1. Introduction

1.1 Background

The question "Is privacy a competition problem?" has been intensely debated, for[1] and against[2], in competition circles.[3] The fact that personal data has become a fundamental component of the digital economy,[4] has undoubtedly led to the increased interaction between the two fields.[5]

Behavioural data (i.e., data gathered about human behaviour)[6] collected by large digital platforms are mostly personal data, and this data is both hard to anonymise and that anonymisation would reduce its value significantly.[7] Digital platforms' main use of personal data is to connect consumers to businesses, the data is thus monetized through the selling of sponsored posts and targeted advertising.[8]

From a traditional competition law perspective, large digital platforms often holds a dominant position,[9] that activates Article 102 in the *Treaty on the Functioning of*

[1] See e.g., European Data Protection Supervisor, Preliminary Opinion, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy* (2014); Francisco Costa-Cabral and Orla Lynskey, *Family Ties: The Intersection between Data Protection and Competition in EU Law* (Kluwer Law International, 2017), p. 11.

[2] See e.g. Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, C(2014) 7239 final, para. 164; Maureen K. Ohlhausen and Alexander Okuliar, *Competition, Consumer Protection, and the Right (Approach) to Privacy* (Antitrust Law Journal, Forthcoming, 2015), p. 43-44.

[3] Ariel Ezrachi and Viktoria H.S.E. Robertson, *Competition, Market Power and Third-Party Tracking* (Oxford Legal Studies Research Paper, 2018), p. 8.

[4] Samuel Goldberg, Garrett Johnson and Scott Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR* (Law & Economics Center at George Mason University Scalia Law School Research Paper Series, 2019), p. 1.

[5] Erika Douglas, *The New Antitrust/Data Privacy Law Interface* (The Yale Law Journal Forum, 2021), p. 34.

[6] Wenbo Li et al, *A multimodal psychological, physiological and behavioural dataset for human emotions in driving tasks* (Scientific Data, 2022).

[7] Heike Schweitzer and Robert Welker, *A Legal Framework for Access to Data – A Competition Policy Perspective* (German Federal Ministry of Justice and Consumer Protection, 2020), p. 144-145.

[8] Dirk Bergemann and Alessandro Bonatti, *Data, Competition, and Digital Platforms* (MIT Sloan Research Paper, 2022), p. 2.

[9] See e.g. COMMISSION DECISION of 4.5.2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (TFEU) and Article 54 of the EEA Agreement Case AT.40153 – E-book MFNs and related matters, para. 56; COMMISSION DECISION of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)), para. 271; T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 119.

the European Union[10] (TFEU), which gives them a special responsibility not to behave in a way that impair genuine, undistorted competition on the internal market of the *European Union* (EU).[11] Through the new competition tool, *Digital Markets Act* (DMA)[12], the *European Commission* (Commission) aims to regulate these digital platforms through a more effective approach than with Article 102 TFEU (the digital sector in the EU have been called the "wild west")[13],[14] and although the DMA will only be applicable to a few undertakings it will still greatly affect both business users and end users.[15] The two legal frameworks could still be applicable to practically the same situations with regard to digital platforms (*inter alia*, because the DMA has been inspired by the investigations and cases of Article 102 TFEU)[16]. Beyond this, due to the processing of personal data within the behaviour of digital platforms, the *General Data Protection Regulation* (GDPR)[17] is also applicable (as also indicated by the DMA, "[t]he data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users"[18]).[19]

Since these three legal frameworks are supposed to be applicable "without prejudice" to each other,[20] questions emerge regarding their application to similar "challenges" (term used by the DMA)[21]. In the impact assessment to the DMA (with accompanying consultation of national competition authorities and open public

[10] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47-390.

[11] C-322/81 - *Michelin v Commission*, ECLI:EU:C:1983:313, para. 57; C-202/07 P - *France Télécom v Commission*, ECLI:EU:C:2009:214, para. 105; C-209/10 - *Post Danmark*, ECLI:EU:C:2012:172, para. 23; C-23/14 - *Post Danmark*, ECLI:EU:C:2015:651, para. 71; C-413/14 P - *Intel v Commission*, ECLI:EU:C:2017:632, para. 135; Manuel Kellerbauer, 'Article 102 TFEU', in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press, 2019), p. 1049.

[12] 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) OJ L 265/1.

[13] Anne Witt, *The Digital Markets Act – Regulating the Wild West* (Common Market Law Review, 2023).

[14] Recital 5 DMA.

[15] See e.g., Article 3 and Recital 1 DMA.

[16] Assimakis Komninos, *The Digital Markets Act: How Does it Compare with Competition Law?* (2022) Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136146>, p. 1.

[17] 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) OJ L 119/1.

[18] Recital 72 DMA.

[19] Article 2(1) GDPR.

[20] Article 1(6) and Recital 10-12 DMA.

[21] Recital 5 and 32 DMA.

consultation)[22] and the Preamble of the final version of the DMA, two challenges, (i) "access to data" (e.g. creating barriers to both entry and exit),[23] and (ii) "imbalanced bargaining power" (e.g. leaving consumers no other choice than to accept data privacy policies),[24] has been identified as "problem drivers"[25] on digital markets. Furthermore, a third challenge, that have been discussed by multiple legal scholars,[26] and mentioned in reports from international organizations (such as World Bank and United Nations)[27] is (iii) "degrading data privacy" (e.g. lowering the data privacy, such as limits to data collection, in order to increase profits and competitive edge).[28] Different dimensions of these three challenges could theoretically be regulated under all three legal frameworks. The first challenge can be regulated under data portability (both DMA[29] and GDPR[30]), and the refusal to supply doctrine (Article 102 TFEU). The second and third challenge can, *inter alia*, be regulated under data protection principles and legal basis for personal data

[22] European Commission, *Summary of the contributions of the National Competition Authorities to the impact assessment of the new competition tool* (2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/summary_contributions_NCAs_responses.pdf> (visited 2023-05-25); European Commission, *Factual summary of the contributions received in the context of the open public consultation on the New Competition Tool* (2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/summary_stakeholder_consultation.pdf> (visited 2023-05-25).

[23] See e.g., Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the digital era Final report* (Directorate-General for Competition, 2019), p. 76; Massimo Motta and Martin Peitz, *Intervention triggers and underlying theories of harm Expert advice for the Impact Assessment of a New Competition Tool Expert study* (Directorate-General for Competition, 2020), p. 6-38;

Commission, Summary of the contributions of the National Competition Authorities to the impact (n. 22), p. 1-2; COMMISSION STAFF WORKING DOCUMENT 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), SWD/2020/363 final, para. 76; Recital 3, 41 DMA; Anca D. Chirita, *Data-Driven Unfair Competition in Digital Markets* (Durham Law School Research Paper, 2022), 31-32.

[24] See e.g., Maurice E. Stucke, *Should We Be Concerned About Data-opolies?* (University of Tennessee Legal Studies Research Paper, 2018), p. 289; Crémer, de Montjoye and Schweitzer (n. 23), p. 28;

Commission, Summary of the contributions of the National Competition Authorities to the impact (n. 22), p. 2; Commission, Factual summary of the contributions received in the context of the open public consultation on the New Competition Tool (n. 22), p. 5; SWD DMA (n. 23), para. 85; Recital 4, 33 DMA.

[25] SWD DMA (n. 23), para. 67.

[26] See e.g. Robert H. Lande, *The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern* (University of Baltimore School of Law Legal Studies Research Paper, 2008); Inge Graef, *EU competition law, data protection and online platforms data as essential facility* (Kluwer Law International, 2016); Viktoria H.S.E. Robertson, *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data* (Common Market Law Review, 2019); Erika M. Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (Temple University Legal Studies Research Paper, 2021).

[27] WORLD BANK GROUP, *World Development Report 2021: data for better lives,* p. 109.

[28] See e.g., Graef (n. 26), p. 356; Ezrachi and Robertson (n. 3), p. 8-9; Stucke (n. 24), p. 289; Robertson (n. 26), p. 9.

[29] Article 6(9) DMA.

[30] Article 20 GDPR.

processing (GDPR[31]), tying/bundling or excessiveness (Article 102 TFEU), and opt-in restrictions for personal data use (DMA[32]). Overall, the common denominator is "personal data". These dimensions and challenges will be further explained under Chapter 3-5 below.

When applicable to the three challenges presented above, the three legal frameworks have characteristics of both "overlap" and "interplay". The relationship between Article 102 TFEU and the DMA, can on the one hand be thought to have an overlapping character,[33] because they cover "part of the same space" i.e. large digital platforms, and because the DMA has been inspired by the investigations and cases of Article 102 TFEU,[34] but are still applicable "without prejudice" (which might create both tension and uncertainty).[35] On the other hand, the relationship between the GDPR and competition rules (Article 102 TFEU and the DMA) can be interpreted as an interplay,[36] when the situation concerns personal data, because of the effect the legal frameworks can have on each other, e.g. the data privacy has been suggested as an alternative dimension to the traditional price-based approach of competition law.[37]

Competition rules and the GDPR should also apply "without prejudice" to each other.[38] Likewise, according to the DMA, both Article 102 TFEU,[39] and the GDPR,[40] should apply "without prejudice" to the Regulation. But this "without prejudice" clause has been questioned by legal scholars (e.g., regarding data

[31] Article 5-6 GDPR.

[32] Article 5(2) DMA.

[33] Giorgio Monti, *The Digital Markets Act – Institutional Design and Suggestions for Improvement* (TILEC Discussion Paper, 2021), p. 14; Marco Cappai and Giuseppe Colangelo, *Applying ne bis in idem in the Aftermath of bpost and Nordzucker: The Case of EU Competition Policy in Digital Markets* (a modified version is forthcoming in Common Market Law Review, 2023), p. 20.

[34] Komninos (n. 16), p. 1.

[35] Inge Graef, Thomas Tombal and Alexandre de Streel, *Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law* (TILEC Discussion Paper, 2019), p. 30; Konstantina Bania, *Fitting the Digital Markets Act in the existing legal framework: the myth of the "without prejudice" clause* (European Competition Journal, 2022).

[36] Damien Geradin, Konstantina Bania and Theano Karanikioti, The interplay between the Digital Markets Act and the General Data Protection Regulation (2022), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203907>

[37] See e.g., Lande (n. 26), p. 714.

[38] Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704, Footnote 21.

[39] Article 1(6) DMA; Recital 10 and 11 DMA.

[40] Recital 12 DMA.

portability as indicated above with similar provisions).[41]

Scholars have raised concerns regarding the costs of individuals' privacy compared to the created value of digital firms in the EU.[42] Thus raising the question if the potential threefold regulation could have a positive or negative impact on consumers and the digital single market of the EU. To this date, the dimensions of the legal frameworks applicable to the presented challenges, have been investigated two-and-two (naturally, due to its novelty of the DMA). This contribution studies the new development where the DMA is also applicable, and thus investigating the legal frameworks application, on the challenges, three-and-three. Either for or against, the perceived uncertainty, overlap and interplay between the three legal frameworks could have high implications on consumers, business users and digital platforms, which will be investigated through a legal competition and data privacy perspective in this thesis.

1.2 Purpose and Research Questions

The purpose of this thesis is to describe and analyse how the above-mentioned challenges of "access to data", "imbalanced bargaining power", and "degrading data privacy" are regulated in the GDPR, Article 102 TFEU and the DMA, and the plausible overlap and interplay between the stipulated legal frameworks regarding these challenges, in the context of large digital platforms.

To achieve this purpose, the following questions will be answered in the context of large digital platforms:

I. To what extent is the challenge "access to data" regulated in the GDPR, Article 102 TFEU and the DMA?
II. To what extent is the challenge "imbalanced bargaining power" regulated in the GDPR, Article 102 TFEU and the DMA?
III. To what extent is the challenge "degrading data privacy" regulated in the GDPR, Article 102 TFEU and the DMA?
IV. What is the plausible overlap and interplay between the legal frameworks, with regard to question I, II and III?

[41] See e.g., Bania (n. 35).

[42] Goldberg, Johnson and Shriver (n. 4), p. 1.

1.3 Delimitations

As can be derived from Section 1.2 together with Section 1.1, the study is limited to the three described challenges, i.e. three common situations conducted by large digital platforms where all three legal frameworks (theoretically) can be applicable. It can also be derived that within the legal frameworks, limitations are made to only investigate violation of each legislation (i.e. breach of the GDPR, abuse under Article 102 TFEU, and non-compliance with the obligations in the DMA), thus assuming that each legislation is applicable (i.e. the data is personal data, the digital platforms have a dominant position and are designated gatekeepers, under Article 102 TFEU and the DMA respectively).

1.4 Method and Material

The subject area of this thesis is EU law, as can be derived from Section 1.2 above, therefore an *EU legal method* will be used throughout the study. In the famous *van Gend en Loos*[43] case from 1963, the Court stipulated that EU law "(...) constitutes a new legal order of international law (...)"[44] and established the fundamental principle of direct effect.[45] That the EU constitutes a separate "legal order" is of importance when interpreting a EU legal method, in the same way that there is not one single method for interpreting Member States' legal orders, there is not a single unifying (EU legal) method for interpreting the EU legal order.[46] Thus, other legal methods can be used when investigating EU law.[47] The EU legal method can be regarded as an approach for the investigation of EU legal sources, their respective hierarchy and how they are interpreted.[48] Although there is one "unifying interpretation method" by the *Court of Justice of the European Union* (CJEU) (see described below), the Courts do not refer to (or publicly consider) sources outside the EU provisions.[49]

In this thesis, the EU legal method will be used within the framework of a *legal*

[43] C-26/62 - *Van Gend en Loos v Administratie der Belastingen*, ECLI:EU:C:1963:1.

[44] ibid., p. 2.

[45] ibid., ruling para. 1; Jane Reichel, 'EU-rättslig metod', in Maria Nääv & Mauro Zamboni (eds), *Juridisk metodlära* (2nd Edition, Studentlitteratur, 2018), p. 109.

[46] Reichel (n. 45), p. 109.

[47] ibid.

[48] Jörgen Hettne, and Ida Otken Eriksson, *EU-rättslig metod - Teori och genomslag i svensk rättstillämpning*, (2nd Edition, Norstedts Juridik, 2011), p. 38; Reichel (n. 45), p. 109.

[49] Hettne and Eriksson (n. 48), p. 120.

dogmatic method (when investigating for the CJEU unchartered or unclear territory). The purpose of this method is to find answers to legal problems through the application of legal materials (from binding rules to literature by legal scholars).[50]

Both the legal dogmatic method and EU legal method will be presented in the two sections below, together with the relevant material for this thesis. Beyond the legal methods, to achieve the purpose of this investigation, uncharted (legal) territory or theories with limited support, will be complemented with a concluding analysis of the presented material, through the personal viewpoint of this thesis' author.

The overarching approach and structure of the thesis is to move from "practical" to "theoretical", i.e. initiating with case-law by the EU Courts, then decisions/viewpoints by relevant EU institutions, and finishing with theories by legal scholars, when investigating each challenge. Within this thesis, a "theory" by legal scholars is interpreted as a standalone approach, formulated by a legal scholar, of applying the legal frameworks to the presented challenges. Furthermore, a chapter is dedicated to each of the three initial research questions, and the fourth research question is embedded within each of these chapters, as it relates to the three initial questions.

1.4.1 Legal Dogmatic Method

There is no clear definition of what constitutes a legal dogmatic method.[51] Likewise, as initiated above, the overarching definition revolves around research that fully explains the principles, rules and concepts within the legal field, and the analysis of their relationship to solve gaps and unclarity in the existing law.[52] Importantly, is the emphasis on the systematisation of present law, which is especially crucial for the legal dogmatic approach, i.e. fit new developments (e.g. legislations and recent case-law) to the current situation.[53] Hence, this method uses legal materials (from binding legislation to literature by legal scholars) to examine

[50] Jan Kleineman, 'Rättsdogmatisk metod', in Maria Nääv & Mauro Zamboni (eds), *Juridisk metodlära* (2nd Edition, Studentlitteratur, 2018), p. 21.

[51] Jan M. Smits, *What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research* (Maastricht European Private Law Institute Working Paper, 2015), p. 5.

[52] Smits (n. 51), p. 5; Kleineman (n. 50), p. 21.

[53] Smits (n. 51), p. 7.

and systematise jurisprudence and apply it to present and future legal problems.[54]

This thesis use of the legal dogmatic method is to analyse the relevant legal material within EU law (see below, Section 1.4.2) and the accompanying literature by legal scholars on that material. The field of study is relatively new, and therefore theories and viewpoints by legal scholars are especially important when investigating the direction of the overlap and interplay between the GDPR, Article 102 TFEU and the DMA.

1.4.2 EU Legal Method

The EU legal method can be regarded, as described above, as a way of approaching EU legal sources, their respective hierarchy and how they are interpreted.[55] This Section will describe the different EU legal sources used in this thesis, their respective hierarchical legal value and examples of the actual source used.

Primary law is at the top of the hierarchy of EU legal sources, i.e. the EU Treaties (*Treaty on European Union*[56] (TEU) and TFEU).[57] In this thesis, the main provision is Article 102 TFEU.[58] Below, and according to, primary law is secondary law, that constitutes Regulations, Directives, Decisions and Recommendations.[59] Within this thesis, the GDPR (Regulation 2016/679) and the DMA (Regulation 2022/1925) constitute the main secondary law. EU Regulations have a general application, are binding in its entirety and have direct application in all Member States.[60]

The CJEU includes both the Court of Justice and the General Court, and it shall ensure that in the interpretation and application of the Treaties (*inter alia*, TFEU) the law is observed.[61] The case-law by the CJEU constitutes to a large part binding EU law.[62] When interpreting the law, the CJEU uses several different methods, such

[54] Kleineman (n. 50), p. 21; Fabiana Avelar Pereira, *Global Framework Agreements: A Response to Urgent Global Labour Concerns* (1st Edition, Lund University, 2021), p. 46.

[55] Hettne and Eriksson (n. 48), p. 38; Reichel (n. 45), p. 109.

[56] Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, p. 13-390.

[57] Hettne and Eriksson (n. 48), p. 40; Johannes Köndgen, 'Sources of law', in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2017), p. 120.

[58] Thomas Ackermann, 'European Competition Law', in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2017), p. 515-516.

[59] Article 288 TFEU; Hettne and Eriksson (n. 48), p. 40; Köndgen (n. 57), p. 120.

[60] Article 288(2) TFEU; Köndgen (n. 57), p. 138.

[61] Article 19(1) in the Treaty on European Union; Hettne and Eriksson (n. 48), p. 49.

[62] Hettne and Eriksson (n. 48), p. 40.

as grammatical (i.e. interpreting in accordance with "generally accepted principles of interpretation" and analysis of the word)[63], systematic (i.e. rules are part of an "outer" and "inner" system of the law, placed to correspond to their context)[64] etc., and the method which the CJEU is most famous for, the teleological (i.e. particular attention to the purpose of the EU law, when multiple interpretations is possible the one favouring the rules aim will be used by the CJEU)[65].[66] For example, the recent *Google Shopping*[67] case, is of special interest for this study.

The legal nature of the Preamble (within, *inter alia*, EU Regulations) is also important for the interpretation of EU law. When determining the intention of a legislature, the Preamble is of large value, but the limit of its importance is also noteworthy.[68] The Preamble cannot establish rights for individuals on its own, to do this the operative part of the legislation must be used, the Preamble is merely used for interpreting the operative parts.[69]

The terminology of both primary and secondary competition law in general is vague, which gives the Commission a central role in the interpretation of competition law. The Commission provides guidance to both its own practice, but also to the competition authorities of Member States and the courts.[70]

Impact assessments are used to "(...) collect evidence (including evaluation results) to assess whether future legislative (...) EU action is justified and, if so, how it can best be designed to achieve relevant policy objectives (...)".[71] In order to ensure high quality, the impact assessment is scrutinized by the Regulatory Scrutiny Board,

---

[63] C-53/81 - *Levin v Staatssecretaris van Justitie*, ECLI:EU:C:1982:105, para. 9; C-251/95 - *SABEL v Puma, Rudolf Dassler Sport*, ECLI:EU:C:1997:528, para. 18; C-404/06 - *Quelle*, ECLI:EU:C:2008:231, paras. 31-32; Karl Riesenhuber, 'Interpreation of EU Secondary Law', in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2017), p. 237.

[64] Hettne and Eriksson (n. 48), p. 167-168; Riesenhuber (n. 63), p. 241.

[65] C-34/74 - *Roquette Frères v French State*, ECLI:EU:C:1974:117, paras. 13-31; Hettne and Eriksson (n. 48), p. 169; Riesenhuber (n. 63), p. 249-254.

[66] Hettne and Eriksson (n. 48), p. 168.

[67] T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763.

[68] Riesenhuber (n. 63), p. 249.

[69] C-215/88 - *Casa Fleischhandel v BALM*, ECLI:EU:C:1989:331, para. 31; Opinion of Advocate General Stix-Hackl in C-222/02 - *Paul and Others*, ECLI:EU:C:2003:637, para. 132; Johan Axhamn, *Databasskydd* (Publit, 2016), p. 17; Riesenhuber (n. 63), p. 249.

[70] Ackermann (n. 58), p. 519.

[71] COMMISSION STAFF WORKING DOCUMENT Better Regulation Guidelines, SWD(2021) 305 final, p. 10; Julian Nowag and Xavier Groussot, *From Better Regulation to Better Adjudication? Impact Assessment and the Court of Justice's Review* (Lund University Legal Research Paper Series, 2017), p. 1.

to proceed with e.g. a new legislation, the board must give a positive opinion.[72] For this thesis, the impact assessment of the DMA is of interest.

The *European Data Protection Board* (EDPB) replaced the *Article 29 Working Party* (WP29),[73] and shall issue guidelines, recommendations and best practices in order to encourage consistent application of the GDPR.[74] Although these are not legally binding, they do have authoritative status.[75] The EDPB has endorsed multiple guidelines created by the WP29.[76] Documents of special interest for this study is the *Guidelines on consent*[77] (WP29 guidelines superseded by EDPB guidelines)[78] and the *Guidelines on the right to data portability*[79] (WP29 guideline endorsed by the EDPB)[80].

Advocate Generals (AG) are enshrined in the Treaty.[81] The proposed solution by the AGs does not constitute a judgement within the meaning of case-law by the CJEU.[82] But if the Court references the AG in a later case or the Court follows the proposed solution and logic, then the legal value will increase.[83] Otherwise, legal scholars regard the proposed solution by AGs as legal literature.[84] In this thesis, the Opinion of AG Rantos, from 20 September 2022,[85] in the *Facebook v. Bundeskartellamt* is of interest (since the judgment by the CJEU has not yet been released).

The importance of legal literature within EU law is mostly through the reference by the AG in their proposed solution and logical reasoning for a case, thus less

[72] Commission, *Better Regulation Guidelines* (n. 71), p. 11; Nowag and Groussot (n. 71), p. 3.

[73] Article 94(2) GDPR.

[74] Article 70(1)(e) GDPR; Christopher Docksey, 'Article 70 Tasks of the Board' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 1076.

[75] Graef, Tombal and de Streel (n. 35), p. 18.

[76] EDPB, Endorsement 1/2018.

[77] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020.

[78] EDPB, Endorsement 1/2018.

[79] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017.

[80] EDPB, Endorsement 1/2018.

[81] Article 255 TFEU; Hettne and Eriksson (n. 48), p. 116.

[82] Hettne and Eriksson (n. 48), p. 117.

[83] ibid.

[84] Axhamn (n. 69), p. 17.

[85] Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704.

important than in the legal order of Member States. But, the analysis, argumentation and opinions of legal scholars can still influence the EU Courts (through e.g. reference by disputing parties).[86] Thus, legal literature is of importance when investigating, for the EU Courts, unchartered or disputed territory.

1.5 Structure

In Chapter 2, the thesis will provide some fundamental starting points for the subsequent chapters, by covering the characteristics of large digital platforms and the three legal frameworks. In addition, the overlap and interplay between the frameworks will be explained.

The purpose-oriented part of the thesis begins in Chapter 3, where the first research question is investigated, together with the corresponding fourth research question. This part will present how each of the legal frameworks could tackle the challenge of "access to data", followed by the frameworks plausible overlap and interplay, and ending with a conclusion which includes indicative answers to the research questions. This structure is subsequently repeated in Chapter 4 and 5, regarding the challenges "imbalanced bargaining power" and "degrading data privacy" respectively (which correspond to the second, third and remaining fourth research question).

Lastly, the thesis will end with a final conclusion in Chapter 6, which will initially answer each research question in a straightforward and summarising fashion, followed by some final thoughts and conclusions.

[86] Hettne and Eriksson (n. 48), p. 121.

2. The Characteristics of Digital Platforms and the Legal Frameworks

2.1 Digital Platforms and the Role of Personal Data

Addressing all characteristics of digital platforms, and in depth, is outside the scope of this study, but a general understanding is still necessary to understand the following sections. The main characteristics will be addressed briefly, from a legal perspective.

2.1.1 Big Tech and Platforms

Big Tech generally refers to Google, Amazon, Facebook (now Meta), Apple and Microsoft,[87] and are the largest companies in the world,[88] and one of the most prestigious employers.[89] These companies is further characterised by the platform economy, they facilitate platforms to both business users and end users (e.g. Google search engine and Facebook social media), where they act as both regulators (determine what is allowed and not) on the platforms, have insider information of the competitive landscape on their platform, and at the same time compete on the platform.[90]

2.1.2 Multi-sidedness and Network Economy

Multi-sided businesses and network effects are complicated and debated topics.[91] But can generally be regarded as a business model with multiple purposes, e.g.

[87] Chirita (n. 23), p. 11.

[88] Statista, *The 100 largest companies in the world by market capitalization in 2022* <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/> (visited 2023-04-14).

[89] LinkedIn, *Top Companies 2022: The 50 best workplaces to grow your career in the U.S.* <https://www.linkedin.com/pulse/top-companies-2022-50-best-workplaces-grow-your-career-us-/> (visited 2023-04-14).

[90] Crémer, de Montjoye and Schweitzer (n. 23), p. 19 and 60.

[91] See e.g., Graef (n. 26), p. 18-32; Crémer, de Montjoye and Schweitzer (n. 23), p. 19.

Facebook is both a social media for consumers and an advertising platform (on the social media) for businesses.[92] The network effects, the value for the individual increase with the number of users (e.g. all my co-workers have LinkedIn, therefore the value of being on LinkedIn increase),[93] makes one side large enough to be profitable from the other side, e.g. the more potential consumers for a product will increase the sales for the business users and thus increase the profit for the advertisement platform. This network effect and multi-sidedness is a barrier to entry from a competition perspective, raising the classic question of the "chicken and egg problem".[94] Both multisided-businesses and network effects have been discussed by multiple legal scholars.[95]

2.1.3 Ecosystems, Lock-in and Switching Costs

Especially in consumer facing markets, the competition revolves around drawing in the consumers in ecosystems (i.e. product and services only function within that system). This business model is both good and bad, on the one hand it can offer higher quality within the ecosystem due to e.g. interoperability (private "application programming interface") and accumulated personal data (offering more customisation).[96] But on the other hand, the controller of such an ecosystem can steer demand (e.g. through biased rankings, nudges and use of default settings), which is more controversial.[97] Moreover, the invested time and money spent on accessing the ecosystem, also creates both lock-in effects and switching costs for the given technology or platform (the lock-in and switching costs are connected, higher switching costs equals higher lock-in effects).[98]

2.1.4 Zero-price Markets and the Value of Personal Data

Personal data has become a new form of asset class,[99] and data have special characteristics compared to more traditional inputs.[100] Although determining the

[92] Graef (n. 26), p. 29-30.

[93] Graef (n. 26), p. 33-34.

[94] Crémer, de Montjoye and Schweitzer (n. 23), p. 36.

[95] See e.g., Graef (n. 26), p. 18-53; Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 78-81.

[96] Crémer, de Montjoye and Schweitzer (n. 23), p. 47.

[97] ibid.

[98] Graef (n. 26), p. 40.

[99] WORLD ECONOMIC FORUM, *Personal Data: The Emergence of a New Asset Class* (2011).

[100] OECD, *The evolving concept of market power in the digital economy* (2022), p. 14.

value of personal data is very complicated,[101] the existence of a value is undeniable. Services such as search engines (Google) and social media (Facebook) are perceived as free, but the individual users are required to pay with their personal data to access the "free" services, therefore personal data operates as a currency (often the sole currency type) for many digital platforms.[102] This "zero-price" market model is linked to the multi-sided business model (described above), the non-paying side provides data to the digital platform, which use the data to both increase the quality of the service for consumers and to increase the quality of the paying side.[103] For competition law, when "price" is out of the equation, other measures such as privacy is needed for the market power analysis.[104] Multiple legal scholars have discussed the special characteristics of zero-price markets and the value of personal data.[105]

2.1.5 Privacy Policies, Third-party Tracking, and the Privacy Paradox

Digital platforms often use "take-it-or-leave-it" data privacy policies,[106] which often include third-party tracking, thus so-called "tracking walls" stop users from accessing the websites or services unless they agree to the tracking.[107] In third-party tracking, company A (third-party) hooks onto the website or application of company B (first-party) and then collects personal data about the users, through this activity comprehensive profiles can be built about the users.[108] The privacy dimension on digital platforms are further complicated by the so-called "privacy paradox": consumers do not (or cannot) take action on their data privacy concerns, despite valuing the privacy (many users do not read privacy policies)[109].[110]

---

[101] Reuben Binns and Elettra Bietti, *Dissolving Privacy, One Merger at a Time: Competition, Data and Third Party Tracking* (Computer Law & Security Review, 2018), p. 13-14.

[102] EDPS (n. 1), para. 10; Crémer, de Montjoye and Schweitzer (n. 23), p. 44.

[103] Crémer, de Montjoye and Schweitzer (n. 23), p. 44.

[104] Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 75.

[105] See e.g., Binns and Bietti (n. 101), p. 13-14; Samson Esayas, *Data Privacy in European Merger Control: Critical Analysis of Commission Decisions Regarding Privacy as a Non-Price Competition* (European Competition Law Review, 2019).

[106] Stucke (n. 24), p. 289.

[107] Ezrachi and Robertson (n. 3), p. 9.

[108] ibid., p. 2.

[109] Bo Bian, Xinchen Ma, Huan Tang, *The Supply and Demand for Data Privacy: Evidence from Mobile Apps* (2021), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3987541>, p. 37.

[110] Ezrachi and Robertson (n. 3), p. 9.

2.2 The Three Legal Frameworks and Digital Application

Addressing all characteristics of the three legal frameworks, and in depth, is outside the scope of this study, but a general understanding is still necessary to understand the following sections. The main characteristics will be addressed briefly and complemented with reference to scholars that provide detailed elaborations.

2.2.1 Processing of Personal Data under the GDPR

The GDPR is a Regulation,[111] and all data that can be related to an identified or identifiable natural person (data subject) fall under the GDPR.[112] Data that has been anonymised do not fall within the GDPR,[113] but data scientists have shown that it is very difficult to anonymise individual-level personal data to the degree that it is impossible to "re-identify" (thus the data is only characterised as pseudonymisation)[114].[115] A considerable amount of data produced today (on e.g. digital platforms) pertains to consumer behaviour,[116] which thus falls under the GDPR. The processing of personal data is only possible in six different ways,[117] and the lawfulness of *consent*[118] and *legitimate interests*[119] are most relevant for this thesis.[120]

2.2.2 Abuse under Article 102 TFEU

Article 102 TFEU is primary law, and does not forbid undertakings from having a dominant position,[121] the violation occurs when the undertaking abuse this position.[122] The CJEU has set relatively wide objectives for Article 102 TFEU, which have shaped the scope of abuse.[123] There is no clear definition of the "abuse" term in Article 102 TFEU, and the provision provides a non-exhaustive list of

[111] GDPR (n. 17).

[112] Article 4(1) GDPR.

[113] Recital 26 GDPR.

[114] Recital 26 GDPR.

[115] Crémer, de Montjoye and Schweitzer (n. 23), p. 77.

[116] ibid.

[117] Article 6(1) GDPR.

[118] Article 6(1)(a) GDPR.

[119] Article 6(1)(f) GDPR.

[120] Crémer, de Montjoye and Schweitzer (n. 23), p. 79.

[121] C-209/10 - *Post Danmark*, ECLI:EU:C:2012:172, para. 21; C-23/14 - *Post Danmark*, ECLI:EU:C:2015:651, para. 70; Ariel Ezrachi, *Article 102 TFEU, EU Competition Law: An Analytical Guide to the Leading Cases* (Hart Publishing, 2014), p. 183; Kellerbauer (n. 11), p. 1047.

[122] Ezrachi (n. 121), p. 183; Kellerbauer (n. 11), p. 1047.

[123] See e.g., C-468/06 - *Sot. Lélos kai Sia*, ECLI:EU:C:2008:504; C-52/09 - *TeliaSonera Sverige*, ECLI:EU:C:2011:83; Ezrachi (n. 121), p. 183.

examples.[124] Although the digital sector has different economic characteristics than other sectors of the economy, scholars still believe that the "basic" framework of competition law including, *inter alia*, Article 102 TFEU, remains a solid and adaptable framework for safeguarding competition in the digital era.[125] But, there are still concerns in the way this framework is applied.[126]

2.2.3 Obligations under the DMA

The DMA is a Regulation,[127] and the *digital* application is of course obvious, but can also be derived from the Regulations subject matter.[128] The DMA focuses on regulating companies designated as so-called "gatekeepers"[129], which are large digital platforms that serve as a gateway for end users and businesses, with a durable position on the market.[130] The Regulation imposes a set of obligations on these gatekeepers that prohibit certain common practices among digital platforms.[131] There are also special rules regarding possible circumvention risks that might emerge among the gatekeepers.[132]

2.3 Overlap and Interplay between the Three Legal Frameworks

Legal scholars have raised multiple questions regarding the overlap and interplay of the GDPR, Article 102 TFEU and the DMA, and stated that the "without prejudice" clause in the DMA is probably not feasible in practice.[133] The DMA have been suggested as a lex specialis (i.e. specific rules prevail over general

[124] C-333/94 P - *Tetra Pak v Commission*, ECLI:EU:C:1996:436, para. 37; C-95/04 P - *British Airways v Commission*, ECLI:EU:C:2007:166, para. 57; Kellerbauer (n. 11), p. 1047.

[125] Crémer, de Montjoye and Schweitzer (n. 23), p. 39.

[126] ibid.

[127] DMA (n. 12).

[128] Article 1(1) DMA.

[129] Article 3 DMA.

[130] Article 3(1) DMA; Natalia Moreno Belloso, *The EU Digital Markets Act (DMA): A Summary* (2022), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109299>, p.1.

[131] Article 5-7 DMA; Belloso (n. 130), p.1.

[132] Recital 29 and Article 13 DMA.

[133] Bania (n. 35), p. 148.

rules)[134] to both the Article 102 TFEU,[135] and the GDPR.[136] Furthermore, initial questions regarding the ne bis in idem principle (i.e. cannot be punished twice for the same conduct)[137] have been raised regarding Article 102 TFEU and the DMA.[138]

The suggested lex specialis approach would *de facto* make the DMA prejudice towards Article 102 TFEU and the GDPR. Which the legislator did not intend.[139] Thus raising the question of the relationship between general and sector-specific regulations, could the DMA be regarded as a sector-specific regulation for both Article 102 TFEU and the GDPR (for certain behaviour)? It can be derived from the name of the GDPR that aims at a "general" approach (and legal scholars have suggested the GDPR as a lex generalis to the DMA in certain situations)[140], and it has become customary to refer to Article 102 TFEU as general.[141]

According to the DMA, it will apply "without prejudice" to, *inter alia*, the GDPR and Article 102 TFEU.[142] The wording of the "without prejudice" clauses in the DMA imply that all the legal frameworks will co-exist, work in harmony and complement each other, when regulating large digital platforms (designated as gatekeepers).[143] But Geradin et al, believes that applying rules with such variation will give rise to tension.[144]

Regarding the general interplay between data protection and competition law, it can be illustrated by a Venn diagram (*Figure 1*, below), inspired by *European Data Protection Supervisor* (EDPS) Preliminary Opinion on *Privacy and*

---

[134] C-444/00 - *Mayer Parry Recycling*, ECLI:EU:C:2003:356, para. 57; T-371/03 - *Le Voci v Council*, ECLI:EU:T:2005:290, para. 122; C-280/13 - *Barclays Bank*, ECLI:EU:C:2014:279, para. 44; T-307/12 - *Mayaleh v Council*, ECLI:EU:T:2014:926, para. 198; T-60/06 - *RENV II - Italy v Commission*, ECLI:EU:T:2016:233, para. 81.

[135] Monti (n. 33), p. 15.

[136] Geradin, Bania and Karanikioti (n. 36), p. 1 and 3; Bania (n. 35), p. 132 and 148.

[137] Article 50 of the Charter of Fundamental Rights of the European Union; Article 4 of Protocol No. 7 of the European Convention on Human Rights; C-238/99 P - *Limburgse Vinyl Maatschappij and Others v Commission*, ECLI:EU:C:2002:582, para. 59; C-129/14 PPU - *Spasic*, ECLI:EU:C:2014:586, para. 53; Cappai and Colangelo (n. 33), p. 1.

[138] Bania (n. 35), p. 144; Witt, *The Digital Markets Act – Regulating the Wild West* (n. 13), p. 24.

[139] DMA, Recital 10-12.

[140] Geradin, Bania and Karanikioti (n. 36), p. 3.

[141] Pierre Larouche and Alexandre de Streel, *Interplay between the New Competition Tool and Sector-Specific Regulation in the EU* (Directorate-General for Competition, 2020), p. 13.

[142] Article 1(6), Recital 10-12 and 37 DMA; Geradin, Bania and Karanikioti (n. 36), p. 2.

[143] Geradin, Bania and Karanikioti (n. 36), p. 2.

[144] ibid.

competitiveness in the age of big data[145], the intersection of the diagram includes "data portability" (first challenge, Chapter 3), "choice" (second challenge, Chapter 4), "welfare vs harm" (third challenge, Chapter 5), "compatibility/substitutability", and "trust and the internal market".[146] Competition and data protection law can complement each other, in e.g. consumer choice vis-à-vis dominant undertakings.[147]

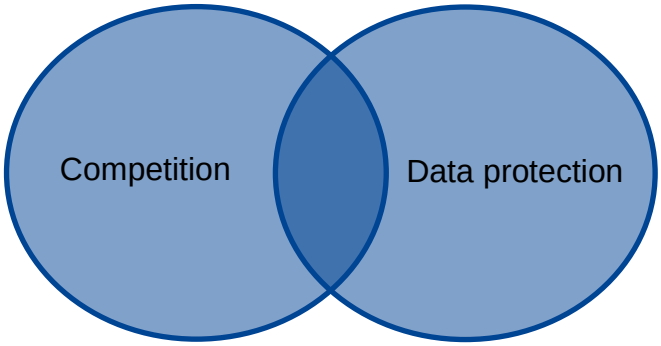

Figure 1

Already back in 2012, the then-Commissioner for Competition, Joaquín Almunia, indicated the possibility that '[a] single dominant company could of course think to infringe privacy laws to gain an advantage over its competitors'[148].[149] More specifically, abuse under Article 102 TFEU and the simultaneous breach of data protection rules is forecasted to increase, as stated by EDPS Giovanni Buttarelli in a 2015 speech that '[w]e should be prepared for potential abuse of dominance cases which also may involve a breach of data protection rules'[150].[151]

Digital platforms typically collect personal data from the users as a form of payment for the provided services, instead of charging money. Therefore, the competition

[145] EDPS (n. 1).

[146] EDPS (n. 1), p. 2.

[147] Crémer, de Montjoye and Schweitzer (n. 23), p. 80.

[148] European Commission, Joaquín Almunia Vice President of the European Commission responsible for Competition Policy, *Competition and personal data protection* (2012, SPEECH/12/860), p. 3.

[149] Graef (n. 26), p. 356.

[150] Giovanni Buttarelli, *Competition Rebooted: Enforcement and personal data in digital markets Keynote speech at Joint ERA-EDPS seminar Brussels* (2015), p. 3.

[151] Graef (n. 26), p. 356.

takes place in other dimensions than "price".[152] These other dimensions, which are influencing components of competition, could be reducing "output", "choice", "quality of goods and services", or "innovation", as acknowledged by both the EU Horizontal Merger Guidelines and Non-Horizontal Merger Guidelines.[153]

As indicated above, many legal scholars believe that the DMA could have a possible regulatory overlap with Article 102 TFEU.[154] According to, *inter alia*,[155] David Dinielli, Gene Kimmelman, Giorgio Monti, Rupprecht Podszun and Alexandre de Streel (in their paper *Enforcing the Digital Markets Act*[156]), there are multiple enforcement options that are possible for conduct which fall within both Article 102 TFEU and the DMA. These enforcement options are dependent on the relationship between the legal framework, i.e., if all components in the competition case completely fall within the rules of the DMA, or some components fall outside. This can be illustrated in a Venn diagram (*Figure 2*, below).[157] In scenario A, all components of Article 102 TFEU fall within the DMA, and in scenario B, some pieces of the gatekeeper's conduct fall outside the DMA but still constitute abuse.[158]

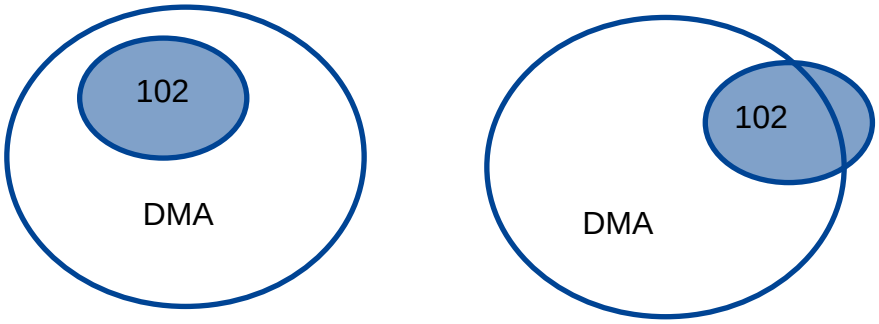

Figure 2

[152] Graef (n. 26), p. 306.

[153] Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2004/C 31/03), para. 8; Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2008/C 265/07), para. 10; Graef (n. 26), p. 309-310.

[154] See e.g., Chirita (n. 23), p. 9.

[155] Emphasis on the legal scholars of the study.

[156] Jacques Crémer, David Dinielli, Paul Heidhues, Gene Kimmelman, Giorgio Monti, Rupprecht Podszun, Monika Schnitzer, Fiona Scott Morton, Alexandre de Streel, *Enforcing the Digital Markets Act: Institutional Choices, Compliance, and Antitrust* (Yale Tobin Center for Economic Policy, 2022).

[157] Crémer, Dinielli, Heidhues et al (n. 156), p. 16.

[158] ibid.

Through recent case-law of *bpost*[159] and *Nordzucker*[160] on 22 March 2022, the CJEU unified the approach of the ne bis in idem principle and removed the threefold condition for competition law (i.e. identity of the facts, unity of offender and unity of the legal interest protected)[161], now the twofold approach (i.e. same offender and same facts) apply to all EU law.[162]

However, importantly for the relationship between Article 102 TFEU and the DMA, both legal frameworks can apply side-by-side *even* if they are regulating the same conduct. This can be done due to the *bpost* case, where the CJEU made it possible for the Commission to investigate while an antitrust case is pending. In that case, the behaviour of *bpost* was first regulated under sector-specific rules and secondly condemned by the competition authority due to abuse of dominant position.[163] When the double regulation was challenged due to the ne bis in idem principle, the CJEU confirmed that parallel application was possible (i.e. not infringing the ne bis in idem) if two criteria (substantive condition and procedural requirements) are met: (i) the legal frameworks pursue different objectives, and (ii) the undertaking can foresee the parallel application, coordination between the competent authorities, the application of the legal frameworks is close in time, and penalty calculation regard the multiple legal frameworks.[164] The objective of the DMA is the "contestability" of digital platforms,[165] and is different from, *inter alia*, Article 102 TFEU (i.e. "protecting undistorted competition on any given market").[166] Through the *bpost* case, the CJEU has opened up the possibility for parallel actions, which likely means that the ne bis in idem principle will not apply.[167] Furthermore, regarding data protection and competition law, the difference in their underlying legal interest also renders the ne bis in idem principle invalid.[168]

---

[159] C-117/20 - *bpost*, ECLI:EU:C:2022:202.

[160] C-151/20 - *Nordzucker and Others*, ECLI:EU:C:2022:203.

[161] C-204/00 P - *Aalborg Portland and Others v Commission*, ECLI:EU:C:2004:6, para. 338; T-322/01 - *Roquette Frères v Commission*, ECLI:EU:T:2006:267, para. 278; Graef (n. 26), p. 360.

[162] Cappai and Colangelo (n. 33), p. 19.

[163] Crémer, Dinielli, Heidhues et al (n. 156), p. 20-21.

[164] C-117/20 - *bpost*, ECLI:EU:C:2022:202, para. 58; Crémer, Dinielli, Heidhues et al (n. 156), p. 21.

[165] See, *inter alia*, Recital 7 DMA.

[166] Rectial 11 DMA.

[167] Crémer, Dinielli, Heidhues et al (n. 156), p. 21.

[168] Graef (n. 26), p. 360-361.

3. Access to Data

3.1 Data Portability under Article 20 GDPR

The right to data portability under Article 20 GDPR is a newcomer in EU data protection law.[169] According to the guidelines of WP29, endorsed by the EDPB,[170] the aim of this right is to give power to the data subjects own personal data, enabling the capability to "move, copy and transmit" personal data between IT environments (e.g., between competitors).[171]

Data portability is highly relevant on digital platform, as is evident by Facebook's White Paper on *Data Portability and Privacy*[172].

3.1.1 Case-law by the CJEU

The right to data portability in the GDPR is new, compared to its predecessor (data protection Directive)[173].[174] Therefore there is no direct case-law concerning this right,[175] although legal scholars have suggested that the case-law on the right to access[176] could be relevant.[177] But it is still important to recall the connection to competition law, where the failure to provide access to data could constitute abuse under Article 102 TFEU, thus the *Microsoft*[178] case-law has been suggested in the context of data portability under the GDPR.[179] For example, Microsoft was ordered

[169] WP 242 (n. 79), p. 4; Graef, Tombal and de Streel (n. 35), p. 18.

[170] EDPB, Endorsement 1/2018.

[171] WP 242 (n. 79), p. 4; Graef, Tombal and de Streel (n. 35), p. 18.

[172] Erin Egan, *CHARTING A WAY FORWARD: Data Portability and Privacy* (Facebook White Paper, 2019).

[173] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[174] Graef, Tombal and de Streel (n. 35), p. 18; Orla Lynskey, 'Article 20. Right to data portability' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 502.

[175] Lynskey (n. 174), p. 502.

[176] Article 15 GDPR.

[177] Lynskey (n. 174), p. 502; See Gabriela Zanfir-Fortuna, 'Article 15. Right of access by the data subject' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 457.

[178] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289.

[179] Lynskey (n. 174), p. 502.

to supply interoperability information for its software by the Commission,[180] which has been upheld by the General Court.[181]

3.1.2 Guidelines and Opinions by the EDPB (ex WP29)

There are multiple limitations to the right of data portability, stipulated in Article 20 GDPR and elaborated in the guidelines of the WP29. According to Article 20(1) GDPR, the data subject has the right to receive their personal data, that was provided by the data subject to the data controller, "in a structured, commonly used and machine-readable format" and also have the right to transmit the data to another controller without hindrance from the controller (under Article 20(2) GDPR the data can be transmitted directly from one data controller to another, if technically possible).[182] The data portability right can only be activated through "automated means",[183] which means that most physical paper files are not covered.[184] Furthermore, the data portability is limited to personal data that is based on consent by the data subject or contractually necessary.[185] These limitations thus concludes that there are no general data portability right,[186] e.g. the data portability right does not apply to financial institutions relating to personal data that is collected to comply with its legal obligations to prevent and detect financial crimes.[187]

Finally, there are limits to the type of personal data which can be subject to portability. The personal data must be "provided by" the data subject, according to the WP29 the term must be interpreted broadly (both actively and knowingly provided, and provided through observation, e.g. search history, traffic and location data), but is limited by "inferred" and "derived" data (i.e. personal data created by the data collector, e.g. algorithmic results).[188] The WP29 also considers data collection through tracking and recording as "provided by" the data subject.[189]

---

[180] COMMISSION DECISION of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft), para. 782; Lynskey (n. 174), p. 502, Footnote 25.

[181] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 648; Lynskey (n. 174), p. 502, Footnote 25.

[182] WP 242 (n. 79), p. 4-5; Graef, Tombal and de Streel (n. 35), p. 18.

[183] Article 20(1)(b) GDPR.

[184] WP 242 (n. 79), p. 9.

[185] Article 20(1)(a) GDPR.

[186] Article 20(3) GDPR; Recital 68 GDPR; WP 242 (n. 79), p. 8; Graef, Tombal and de Streel (n. 35), p. 18.

[187] WP 242 (n. 79), p. 8; Graef, Tombal and de Streel (n. 35), p. 18.

[188] WP 242 (n. 79), p. 10; Graef, Tombal and de Streel (n. 35), p. 18.

[189] WP 242 (n. 79), p. 10, Footnote 21.

3.1.3 Theory by Legal Scholars

There still remains multiple questions and uncertainty regarding data portability under the GDPR. Especially in the digital economy, where personal data is constantly (automatically) processed, every click could be tracked and recorded (i.e. "provided by" according to WP29, and thus subject for data portability, see Section 3.1.2 above).[190] Further clarification on the exact scope of observed data that can be ported upon request is needed, the wider scope is desirable according to the EDBP to stimulate data-driven innovation.[191] Specifically, if tracking, location and clickstream data is categorised as observed data (before analyzation and refinement), how much context should be provided when the data is ported (e.g. type of content clicked on, purpose of shown ads) to assess the information properly?[192] Should there be requirements for the data controller to provide technical measures and tools, to enable every data subject to consent (or not) if another data portability affect their data, e.g. if data subject (A) act on their right to data portability and port images where data subject (B) is also included (the situation is further complicated if data subject (B) do not have contractual relationship with the data controller at hand).[193] Building on the previous scenario, if a data subject does not consent that their data should be ported, will the right to data portability be impossible or will part of the data be portable instead?[194] These are some of the questions raised by large digital platforms, in particular Facebook in their White Paper on data portability.[195]

The right to data portability in Article 20 GDPR was not intended for real-time data transfers (i.e. continuous and/or very frequent), that would give power to the individual user to use more than one service with the same personal data, legal scholars believe this to be necessary to embrace the full effect of data portability in the digital economy and stimulate both competition and innovation.[196] What has

[190] Jan Krämer, Pierre Senellart, Alexandre de Streel, *Making data Portability More Effective for The Digital Economy* (Centre on Regulation in Europe, 2020), p. 78.

[191] ibid.

[192] ibid.

[193] ibid.

[194] ibid.

[195] Egan (n. 172); Krämer, Senellart and de Streel (n. 190), p. 78.

[196] Krämer, Senellart and de Streel (n. 190), p. 80.

been referred to as "continuous data portability".[197]

3.2 Refusal to Supply under Article 102 TFEU

Undertakings with a dominant position, that are data-rich (e.g. digital platforms), may refuse access of data to other firms, which could constitute abuse within the meaning of Article 102 TFEU.[198] Refusal to supply under Article 102 TFEU has been investigated in numerous cases by the EU Courts.[199] Under the "refusal to supply" doctrine by the Court, this conduct can constitute abuse, relating to a neighbouring market, if (i) the refused entity is indispensable to the activity, and (ii) the refusal is liable or likely to exclude any effective competition.[200] But not only outright refusal to supply is covered by Article 102 TFEU, situations where the dominant undertaking does supply but under unreasonable or uneconomic conditions (e.g. unjustified delays, prices or unreasonable restrictions on the request for access) are also covered.[201]

In particular, there are three cases that have shaped the traditional "refusal to supply" doctrine, the *Magill*[202] (prevent the appearance of a new product,[203] reserved the second market to themself through exclusion of competition,[204] and no objective justification for the refusal[205]), *Bronner*[206] (clarified the scope of *Magill*,[207] AG Jacobs provided an overall framework for the "refusal to supply"

[197] Krämer, Senellart and de Streel (n. 190), p. 81.

[198] Crémer, de Montjoye and Schweitzer (n. 23), p. 91.

[199] C-6/73 - *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, ECLI:EU:C:1974:18; C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98; C-7/97 - *Bronner*, ECLI:EU:C:1998:569; T-504/93 - *Tiercé Ladbroke v Commission*, ECLI:EU:T:1997:84; C-418/01 - *IMS Health*, ECLI:EU:C:2004:257; T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289; C-468/06 - *Sot. Lélos kai Sia*, ECLI:EU:C:2008:504; T-301/04 - *Clearstream v Commission*, ECLI:EU:T:2009:317; Ezrachi (n. 121), p. 187.

[200] C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98, para. 56; C-7/97 - *Bronner*, ECLI:EU:C:1998:569, para. 41; T-301/04 - *Clearstream v Commission*, ECLI:EU:T:2009:317, para. 147; T-851/14 - *Slovak Telekom v Commission*, para. 115; Kellerbauer (n. 11), p. 1053.

[201] C-155/73 - *Sacchi*, ECLI:EU:C:1974:40, para. 17; T-301/04 - *Clearstream v Commission*, ECLI:EU:T:2009:317, para. 136; Kellerbauer (n. 11), p. 1054.

[202] C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98; Christian Ahlborn and David S. Evans, *The Microsoft Judgment and its Implications for Competition Policy Towards Dominant Firms in Europe* (Antitrust Law Journal, 2008), p. 7.

[203] C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98, para. 54; Ahlborn and Evans (n. 202), p. 7-8.

[204] C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98, para. 56; Ahlborn and Evans (n. 202), p. 8.

[205] C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98, para. 57; Ahlborn and Evans (n. 202), p. 8.

[206] C-7/97 - *Bronner*, ECLI:EU:C:1998:569; Ahlborn and Evans (n. 202), p. 8.

[207] Ahlborn and Evans (n. 202), p. 8.

doctrine,[208] likely to eliminate all competition on the desired market[209]) and *IMS*[210]. More specifically, the information-related cases (regarding essential facilities) are *Magill*, *IMS* and *Microsoft*.[211]

In relation to digital platforms, the Facebook White Paper acknowledged the importance of access to data to, *inter alia*, promote digital competition.[212]

3.2.1 Case-law by the CJEU

In the *Microsoft* case, the Court validated that access to interoperability information was compulsory.[213] From the cases *Magill*, *IMS* and *Bronner*, the Court derived that only in exceptional circumstances could the refusal to supply constitute abuse under Article 102 TFEU.[214] Furthermore, derived from the case-law, for the circumstances to be classified as exceptional, three conditions must apply: (i) "the refusal relates to a product or service *indispensable* to the exercise of a particular activity on a neighbouring market"[215], (ii) "the refusal is of such a kind as to *exclude any effective competition* on that neighbouring market"[216], and (iii) "the refusal *prevents the appearance of a new product* for which there is potential consumer demand"[217].[218] A fourth condition is also required: (iv) "the absence of objective justification".[219]

In the *Microsoft* case, the information regarding the interoperability with Windows domain architecture was *indispensable*.[220] The market for "work group server operating systems" was characterised by significant network effects, and the *elimination of competition* would therefore be difficult to reverse, thus the

[208] Opinion of Advocate General Jacobs in C-7/97 - *Bronner*, ECLI:EU:C:1998:264; Ahlborn and Evans (n. 202), p. 8.

[209] C-7/97 - *Bronner*, ECLI:EU:C:1998:569, para. 38; Ahlborn and Evans (n. 202), p. 8.

[210] C-418/01 - *IMS Health*, ECLI:EU:C:2004:257; Ahlborn and Evans (n. 202), p. 8.

[211] Graef, Tombal and de Streel (n. 35), p. 13.

[212] Egan (n. 172), p. 3.

[213] Graef, Tombal and de Streel (n. 35), p. 13.

[214] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 331; Ezrachi (n. 121), p. 262.

[215] See T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 332, 369-436 (emphasis added).

[216] See T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 332, 560-563 (emphasis added).

[217] See T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 332, 643, 647-649, 656-658, 664 and 660-665 (emphasis added).

[218] Ezrachi (n. 121), p. 262-264.

[219] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 688-711; Ezrachi (n. 121), p. 264.

[220] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 369-436; Ezrachi (n. 121), p. 262.

application of Article 102 TFEU by the Commission was warranted.[221] It was also concluded that the conduct by Microsoft prevented the appearance of a new product, to the prejudice of consumers.[222] There was also no objective justification for Microsoft's behaviour.[223]

Three interesting facts can be derived from the *Microsoft* case (regarding refusal to supply), compared to previous case-law, that lowered the threshold for intervention. (i) Circumstances relating to the appearance of a new product, described in *Magill* and *IMS*, "(...) cannot be the only parameter which determines whether a refusal to license an intellectual property right is capable of causing prejudice to consumers within the meaning of [Article 102(b) TFEU] (...)"[224].[225] Which means that the Court used Article 102(b) TFEU to "import" the innovation dimension to the given situation, and lowered the threshold for abusive refusal.[226] (ii) The notion of indispensability was widened, prior to the *Microsoft* case the requirement was "objectively indispensable". But, in *Microsoft*, even if access to market was technically possible, the refusal removed the economic viability of entering the market (i.e., the concept of indispensability was broadened to also include economic viability).[227] (iii) Lowered the requirement for the elimination of "all competition in the secondary market. The Court held that it is not "(...) necessary to demonstrate that all competition on the market would be eliminated. What matters (...) is that the refusal at issue is liable to (...) eliminate all effective competition on the market (...)"[228].[229]

In the recent judgement of *Google Shopping*, currently on appeal,[230] the CJEU discussed the refusal to supply doctrine. The Court described the conditions brought

[221] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 560-563; Ezrachi (n. 121), p. 263.

[222] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 665; Ezrachi (n. 121), p. 263.

[223] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 688-711; Ezrachi (n. 121), p. 264.

[224] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 647.

[225] Ezrachi (n. 121), p. 264.

[226] ibid.

[227] ibid.

[228] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 563.

[229] Ezrachi (n. 121), p. 264.

[230] C-48/22 P - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:C:2022:207; Request for a preliminary ruling from the Tribunal du travail francophone de Bruxelles (Belgium) lodged on 20 January 2022 — HK v Service fédéral des Pensions (SFP) (Case C-45/22) (2022/C 191/13).

through the *Bronner* case.[231] Important conditions are the elimination of competition and the indispensability of access to an "essential facility" or infrastructure, for services that do not have real substitutes. If the access is granted, the exclusive right that rewards innovation or investment, can be hindered.[232]

Google's general results page has characterised as an "essential facility" by the CJEU,[233] as there is no actual or potential substitute available that could replace it in an "economically viable" way on the market (with reference to the *Microsoft* case)[234].[235] But the Court dismissed the notion of a "refusal to supply", stating that there must be an "expressed request" which is denied.[236] If this criterion is not needed, most exclusionary practices could be categorized as an "implicit" refusal to supply.[237]

3.2.2 Decision and Viewpoint by the Commission

Although not relating it to abuse *per se*, the Commission mentioned the challenge of "access to data" in its impact assessment to the DMA, as a "problem driver".[238]

The Commission investigated refusal to supply in the *Microsoft* case,[239] and concluded that Microsoft's refusal to supply interoperability information violated Article 102 TFEU.[240] Although this decision, like many other "refusal to supply" decisions (e.g., Google Shopping decision by the Commission,[241] that was recently decided by the CJEU), was appealed to the CJEU (as seen in the section above) and

[231] T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, paras. 213 and 215; Chirita (n. 23), p. 31.

[232] T-321/05 - *AstraZeneca v Commission*, ECLI:EU:T:2010:266, para. 679; T-814/17 - *Lietuvos geležinkeliai v Commission*, ECLI:EU:T:2020:545, para. 87; T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 215; Chirita (n. 23), p. 31.

[233] T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, paras. 224-225; Chirita (n. 23), p. 31.

[234] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 208, 388, 390, 421 and 436; T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 224.

[235] T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 445; Chirita (n. 23), p. 31.

[236] T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, paras. 229 and 232; Chirita (n. 23), p. 31.

[237] Opinion of Advocate General Saugmandsgaard Øe in C-152/19 P - *Deutsche Telekom v Commission*, ECLI:EU:C:2020:678, paras. 85-89; T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 234; Chirita (n. 23), p. 31.

[238] SWD DMA (n. 23), paras. 67 and 76.

[239] COMP/C-3/37.792 Microsoft (n. 180), paras. 546-791.

[240] COMP/C-3/37.792 Microsoft (n. 180), para. 784.

[241] Google Shopping, AT.39740 (n. 9).

thus rendered less important.

The Commission referenced the *Microsoft* case, by the CJEU, in its Guidance on the enforcement priorities of Article 102 TFEU.[242] Competitors that a dominant undertaking foreclosed due to "refusal to supply", will be prevented from bringing innovative services or goods to the market and likely stifle follow-on innovation, which could lead to consumer harm, that will be considered by the Commission.[243]

The challenge of access to data was discussed by the Commission in, *inter alia*, the *Google/DoubleClick*[244] decision, where it was observed that "(...) [c]ompetition based on the quality of collected data thus is not only decided by virtue of the sheer size of the respective databases, but also determined by the different types of *data the competitors have access to* and the question which type eventually will prove to be the most useful for internet advertising purposes"[245].[246]

3.2.3 Theory by Legal Scholars

Dominant undertakings that refuse to give access to their data, could fall under Article 102 TFEU. Multiple legal scholars have argued for this.[247] More specifically, a dominant digital platform that refuse to give access to personal data, could fall within the "essential facility" doctrine of Article 102 TFEU.[248] Although it is important to remember, that competition law only oblige an undertaking to share data under very limited circumstances.[249]

It is primarily when the access to data is essential, that Article 102 TFEU can

---

[242] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02), para. 87; Ezrachi (n. 121), p. 264.

[243] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 643, 647, 648, 649, 652, 653 and 656; Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02), para. 87; Ezrachi (n. 121), p. 264.

[244] COMMISSION DECISION of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 – Google/ DoubleClick), C(2008) 927 final.

[245] COMP/M.4731 – *Google/ DoubleClick* (n. 244), para. 273 (emphasis added).

[246] Graef, Tombal and de Streel (n. 35), p. 6.

[247] See e.g., Crémer, de Montjoye and Schweitzer (n. 23), p. 100-101; Schweitzer and Welker (n. 7), p. 113-114.

[248] Damien Geradin and Monika Kuschewsky, *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue* (2013), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088>, p. 13-15; EDPS (n. 1), paras. 40 and 66-68; Graef (n. 26), p. 154.

[249] Michal S Gal and Oshrit Aviv, *The Competitive Effects of the GDPR* (Oxford Academic, 2020), p. 377.

apply.[250] It is thus important to consider at what stage of the "big data value chain" the request of access is conducted (i.e. raw data, structure, structured data, analysed data), when applying the four conditions for the essential facilities doctrine (see explained above, Section 3.2.1) to the challenge of data access. This consideration will identify the upstream market (where the indispensability is evaluated) and the downstream market (where the new product creation and competition elimination are evaluated).[251]

First condition, indispensability, may occur due to legal, economic, and technical barriers. Furthermore, much data is often produced by the end users, thus often rendering it personal data, which can make it easier to constitute as indispensable in accordance with the case-law of *IMS*. Additionally, following *IMS*, it will not be an obstacle to applying this doctrine even if the requested personal data has not been traded before (frequent in practice), because it is enough that there is a demand and that it can be practically and legally met.[252]

The second condition, excluding any effective competition on the downstream market, is very difficult to assess in the case of big data. On the one hand, the downstream market is often unknown, because big data often involves experimenting and processing a lot of data without knowing beforehand what knowledge or information to be discovered and how to use it. The refusal could thus lead to the potential elimination of competitors on future and undefined markets (which could ultimately create both difficulties and increase antitrust errors).[253] On the other hand, the data owner often does not (yet) operate on the downstream market, data is often collected for one purpose but could prove to be useful for other firms in a different purpose of completely different sectors. There are divided opinions on whether the second condition requires the data owner's presence on the downstream market, and the case-law is unclear.[254]

The third condition, preventing the appearance of a new product and consumer harm, can be unclear to interpret. The CJEU has applied the condition at various

[250] See e.g., Graef (n. 26); Gal and Aviv (n. 249), p. 377.
[251] Graef, Tombal and de Streel (n. 35), p. 14.
[252] ibid.
[253] ibid., p. 15.
[254] ibid.

degrees of strictness in different cases, and the Commission has integrated the condition to the more general "consumer harm" assessment.[255] This condition also has similar challenges as described in the conditions above, namely that the product that is being prevented is unknown and data owners generally do not (yet) compete with that product. Therefore, Graef et al suggest that, for the characteristics of the data economy, the more general approach of consumer harm proposed by the Commission is more appropriate.[256]

Finally, the fourth condition, absence of objective justification, is where dominant undertakings could oppose compulsory data sharing. They could, *inter alia*, argue that the sharing could violate privacy regulations, either way Graef et al believes that a proportionality test needs to be applied to any of the justifications.[257] Therefore, applying the four conditions of the essential facilities doctrine on access to data, may in some circumstances be possible and render the denial of such access as abuse under Article 102 TFEU, but it must be kept in mind that even if these conditions are met, Graef et al still points out that this might not prove any exceptional circumstances (which would be needed to trigger Article 102 TFEU).[258]

Furthermore, the abusive nature of refusal to give access to data on digital platforms was explained in-depth by Graef in her PhD thesis.[259]

3.3 Obligation under the DMA

The DMA contains a data portability provision in Article 6 DMA. In general, this Article imposes obligations for gatekeepers which are "susceptible of being further specified", the Article stipulates 12 complex rules that govern interoperability, switching, self-preferencing, the use and sharing of data, and general access terms for business users.[260] This "further clarification" can occur in two different ways, (i) through the adoption of implementing acts by the Commission with further specification to comply with Article 6 DMA,[261] or (ii) requests by the gatekeeper

[255] ibid.
[256] ibid.
[257] ibid., p. 16.
[258] ibid.
[259] See Graef (n. 26), p. 269-277.
[260] Witt, *The Digital Markets Act – Regulating the Wild West* (n. 13), p. 15.
[261] ibid., p. 16.

to engage the Commission in a regulatory dialogue.[262]

The data portability provision can be found in Article 6(9) DMA.[263] According to the Preamble of the DMA, that the data portability rule is based on,[264] the large amount of data collected through gatekeepers' digital platforms put them in a beneficial position. In order to ensure positive competition, through e.g., switching and multi-homing by end users, both end users and third parties authorised by the end user, the gatekeeper should enable effective and immediate data access (both provided and generated) on the relevant digital platform. This data portability should be in an accessible format, and the gatekeeper should also create the technical possibility for the data to be continuously ported in real time.[265] Stipulated in Article 6(9) DMA is also the fact that this data portability shall be free of charge. According to legal scholars, the data portability in the DMA appears to have the same core elements as the corresponding right in the GDPR (see elaborated Section 3.4 below).[266]

In order to avoid that gatekeepers circumvent the obligations in the DMA, Article 13 DMA provides anti-circumvention measures.[267] Any behaviour that undermines the compliance of the obligations is prohibited, that involves, *inter alia*, technical nature (e.g. the technical requirements for data portability).[268]

3.4 Plausible Overlap and Interplay

Generally, about data portability and competition law, WP29 acknowledges, on the one hand, the connection between the two legal frameworks, that the free flow of personal data under proper data portability right will foster competition between data controllers.[269] But on the other hand, emphasise that the GDPR regulate personal data and not competition.[270]

[262] ibid.
[263] Tambiama Madiega, *Digital Markets Act* (European Parliamentary Research Service, 2022), p. 9.
[264] Geradin, Bania and Karanikioti (n. 36), p. 2; Bania (n. 35), p. 131.
[265] DMA, Recital 59.
[266] Geradin, Bania and Karanikioti (n. 36), p. 2; Bania (n. 35), p. 131.
[267] Madiega (n. 263), p. 10.
[268] Article 13(4) DMA.
[269] WP 242 (n. 79), p. 3.
[270] ibid., p. 4.

In the intersection between data protection law and competition law, the right to data portability has become one of the most prominent.[271] Dominant digital platforms could justify the refusal to give access to personal data, otherwise mandated by Article 102 TFEU, through the objective justification of data protection law, i.e., there could be tensions between the two legal frameworks.[272]

As explained by Graef et al, to make the remedy of data sharing by dominant digital platforms compliant with data protection law, the digital platform (data holder) and the competitor (data recipient) must both rely on a legal basis under the GDPR (e.g. consent), and both parties must follow the general principles of data privacy (*inter alia*, inform the data subject in a transparent way)[273]. First the digital platform shall inform the data subject that it must grant access to certain data due to a competition law infringement,[274] and secondly the competitor must inform the data subject regarding the new processing.[275] Overall, Graef et al do not believe that the two legal frameworks are incompatible, although they point out that there might emerge some tension. These tensions can be mitigated through incorporating data protection rules and principles with the obligation to grant access to data, i.e. competition and data protection authorities would need to collaborate during this stage.[276]

The relationship between the data portability provision in the GDPR[277] and in the DMA[278] have been discussed in detail by Geradin et al[279] and Bania[280]. To begin with, the data portability under the DMA is not limited to "personal data".[281] Furthermore, Article 6(9) DMA states that the portability applies to "(...) data

[271] Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 48.

[272] Graef (n. 26), p. 317; Graef, Tombal and de Streel (n. 35), p. 21; Thomas Tombal, *GDPR As Shield to a Data Sharing Remedy* (CPDP 2020 and ASCOLA 2020 Conferences, 2020), p. 3-4; Wolfgang Kerber and Louisa Specht, *Synergies between Data Protection Law and Competition Law* (2021), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3977039>, p. 45.

[273] Articles 5(1)(a) and 12-14 GDPR.

[274] Article 13 GDPR.

[275] Article 14 GDPR.

[276] Graef, Tombal and de Streel (n. 35), p. 30.

[277] Article 20 GDPR.

[278] Article 6(9) DMA.

[279] Geradin, Bania and Karanikioti (n. 36), p. 3-7.

[280] Bania (n. 35), p. 129-135.

[281] Geradin, Bania and Karanikioti (n. 36), p. 4; Bania (n. 35), p. 132.

provided by the end user *or generated through the activity of the end user* (...)"[282]. This would suggest that the DMA also could cover "inferred and derived" data (which could question the compliance with the proportionality principle).[283] Generally, the right to data portability in the DMA is more far-reaching than that of the GDPR.[284]

In short, regarding the transactional and technical conditions, the DMA states "free of charge", while the GDPR states that there could be "a reasonable fee". Furthermore, the data portability of the DMA should be possible in real time and continuous, while the GDPR is limited to "where technically feasible".[285]

Interestingly, regarding the "without prejudice" clause of the DMA, the WP29 guidelines on data portability explicitly states that "if it is clear from the request made by the data subject that his or her intention is not to exercise rights under the GDPR, *but rather to exercise rights under sectorial legislation only, then the GDPR's data portability provisions will not apply to this request*"[286], which suggest that the right to data portability under the GDPR is not applicable if the request to port personal data was made with reference to the DMA (since it, *inter alia*, is a sectorial legislation).[287] The above mentioned characteristics of the provisions in the two legal frameworks, proves uncertainties regarding their application and overlap, but what is certain, according to Geradin et al and Bania, is that the DMA is not necessarily applicable "without prejudice" to the GDPR.[288]

The DMA will regulate digital platforms ex ante (i.e. before the event)[289],[290] compared to Article 102 TFEU which regulates ex post (i.e. after the event)[291].[292] Which is in line with the regulatory evolution of the digital market, many commentators agree that the traditional ex-post rules are not the right tools to

[282] Emphasis added.

[283] Geradin, Bania and Karanikioti (n. 36), p. 5; Bania (n. 35), p. 133.

[284] Geradin, Bania and Karanikioti (n. 36), p. 5; Bania (n. 35), p. 134; Madiega (n. 263), p. 6.

[285] Geradin, Bania and Karanikioti (n. 36), p. 6; Bania (n. 35), p. 134.

[286] WP 242 (n. 79), p. 7-8 (emphasis added).

[287] Geradin, Bania and Karanikioti (n. 36), p. 6; Bania (n. 35), p. 135.

[288] Geradin, Bania and Karanikioti (n. 36), p. 7; Bania (n. 35), p. 135.

[289] Jonathan Law, *A Dictionary of Business and Management* (5th Edition, Oxford University Press, 2009), ex ante.

[290] Komninos (n. 16), p. 5; Recital 73 DMA.

[291] Law (n. 289), ex post.

[292] SWD DMA (n. 23), para. 115; Komninos (n. 16), p. 5; Recital 5 DMA.

resolve the challenges regarding access to data and portability issues.[293]

3.5 Conclusion on Access to Data

From the above sections, it was concluded that the challenge "access to data" can be regulated under each legal framework, but to different extents. The right to data portability in the GDPR is a possibility, if requested (and provided) by the data subject, importantly for digital platforms the right should also include "observed data" (i.e., how the consumer behave on the platform), but is limited to not include "inferred" and "derived" data. Although multiple concerns still exist (as suggested by both digital platforms and legal scholars), when multiple data subjects are affected, the fees, and the timeframe for porting (Section 3.1). Furthermore, the essential facilities doctrine within refusal to supply under Article 102 TFEU, could under rare circumstances be applicable (as suggested by legal scholars). But to activate such rules, and conclude an abuse, is a complicated (multiple conditions must be met) and time-consuming task (general assumption about Article 102 TFEU), which to this date has not been done (Section 3.2). Lastly, the data portability provision in the DMA is the newest addition to tackle the presented challenge. It has not yet been applicable in practice, but stipulates that the data should be ported free of charge and continuously (Section 3.3). Which would tackle the challenge of "access to data" to a large extent.

The most distinct overlap is between the GDPR and the DMA, where the "without prejudice" clause in the DMA vis-à-vis the GDPR is raising questions. Theoretically, both rules could clearly be applicable to the same data portability request, but the DMA would probably be favoured due to its more user-friendly approach. Finally, from a competition standpoint, for the sake of receiving "access to data" within a reasonable timeframe (which do not disturb, *inter alia*, innovation), there will probably not be much practical overlap between the DMA and Article 102 TFEU. Before the application of Article 102 TFEU is realised, the initial purpose for the "access to data" is probably long gone.

[293] Krämer, Senellart and de Streel (n. 190), p. 80.

4. Imbalanced Bargaining Power

4.1 Consent, Lawfulness of Processing and Conditions for Consent under Article 4(11), 6 and 7 GDPR

The GDPR defines "consent" in Article 4(11) as "(...) any *freely* given, *specific*, *informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[294], and describe it in multiple Recitals,[295] Article 4(11) GDPR is closely related to both Article 6(1)(a) and 7 GDPR (described below).[296] From this definition, four key criteria can be identified, as per the added emphasis.[297] The identified criteria are cumulative, which impose a high threshold, in order to obtain a valid consent (and the data protection authorities' favour a strict interpretation of these criteria).[298]

The "lawful processing" of personal data is stipulated in Article 6 GDPR, with accompanying Recitals,[299] and is only lawful in six different ways according to the list of Article 6(1) GDPR (i.e., the list is exhaustive)[300]. Article 6(1) GDPR is also based on corresponding Article in the data protection Directive and is nearly identical to its predecessor.[301] Article 7 GDPR stipulates the conditions for consent and acts as a complement for the definition of consent (described above), and describes the four components: (i) demonstrating consent,[302] (ii) obtaining

[294] Emphasis added.

[295] Recital 32-33, 42-43 and 51 GDPR; Lee A. Bygrave and Luca Tosoni, 'Article 4(11). Consent' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 174-175.

[296] Bygrave and Tosoni (n. 295), p. 175.

[297] Bygrave and Tosoni (n. 295), p. 181.

[298] ibid.

[299] Recital 40-41, 43-50 GDPR; Waltraut Kotschy, 'Article 6. Lawfulness of processing' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 322-323.

[300] C-468/10 - *ASNEF*, ECLI:EU:C:2011:777, paras. 30 and 32; C-582/14 - *Breyer*, ECLI:EU:C:2016:779, para. 57; C-673/17 - *Planet49*, ECLI:EU:C:2019:801, para. 53; C-61/19 - *Orange Romania*, ECLI:EU:C:2020:901, para. 34; Kotschy (n. 299), p. 325.

[301] Kotschy (n. 299), p. 327.

[302] Article 7(1) GDPR; Eleni Kosta, 'Article 7. Conditions for consent' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 349.

consent,[303] (iii) withdrawal of consent,[304] and (iv) freely given.[305]

For this study, the legal basis of *consent*[306] and *legitimate interests*[307] are most relevant for digital platforms.[308] Although, following the DMA, legitimate interest will not be possible for large digital platforms (which meet the threshold for gatekeepers, see Section 4.3).

4.1.1 Case-law by the CJEU

The CJEU has currently not explicitly tackled the definition of "consent", under Article 4(11) and 6(1)(a) GDPR, in its case-law, but multiple cases can still be used as guidance according to legal scholars.[309] In *Planet49*[310], the Court conclude, in conjunction with the AG,[311] that the wording of Article 4(11) GDPR is even more stringent than that of the corresponding Article in the prior Directive.[312] Which led the Court to conclude that "active consent" is now expressly laid down in the GDPR.[313] The same clarification was made in *Orange Romania*[314], referring to *Planet49*.[315] Together with Recital 32 GDPR, the Court concludes that "silence, pre-ticked boxes or inactivity" do not constitute consent.[316]

"Legitimate interest" as a legal basis, now stipulated in Article 6(1)(f) GDPR, was

[303] Article 7(2) GDPR; Kosta (n. 302), p. 350.

[304] Article 7(3) GDPR; Kosta (n. 302), p. 351.

[305] Article 7(4) GDPR; Kosta (n. 302), p. 351.

[306] Article 6(1)(a) GDPR.

[307] Article 6(1)(f) GDPR.

[308] Crémer, de Montjoye and Schweitzer (n. 23), p. 79.

[309] See e.g., C-397/01 - *Pfeiffer and Others*, ECLI:EU:C:2004:584; C-543/09 - *Deutsche Telekom*, ECLI:EU:C:2011:279; C-40/17 - *Fashion ID*, ECLI:EU:C:2019:629; C-673/17 - *Planet49*, ECLI:EU:C:2019:801; C-61/19 - *Orange Romania*, ECLI:EU:C:2020:901; *Bygrave and Tosoni* (n. 295), p. 176.

[310] C-673/17 - *Planet49*, ECLI:EU:C:2019:801.

[311] Opinion of Advocate General Szpunar in C-673/17 - *Planet49*, ECLI:EU:C:2019:246, paras. 69-70.

[312] C-673/17 - *Planet49*, ECLI:EU:C:2019:801, para. 61.

[313] ibid., para. 62.

[314] C-61/19 - *Orange Romania*, ECLI:EU:C:2020:901.

[315] C-61/19 - *Orange Romania*, ECLI:EU:C:2020:901, para. 36; Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704, para. 72, Footnote 95.

[316] C-673/17 - *Planet49*, ECLI:EU:C:2019:801, paras. 61-63; C-61/19 - *Orange Romania*, ECLI:EU:C:2020:901, para. 36; CJEU Fact sheets on "Protection of personal data", <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf> p. 27-28.

mentioned in the *Fashion ID*[317] case.[318] There are three cumulative conditions for the lawfulness of legitimate interest, (i) "(...) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed (...)", (ii) "(...) the need to process personal data for the purposes of the legitimate interests pursued (...)", and (iii) "(...) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence".[319]

Article 7 GDPR is new, compared to the prior Directive, therefore no case-law is directly applicable, but the CJEU have still ruled in several cases regarding lack of a valid consent, which can still be of guidance for Article 7 GDPR.[320]

4.1.2 Guidelines and Opinions by the EDPB (ex WP29)

The EDPB has provided guidelines on "consent" under the GDPR.[321] The Board reiterates that consent is one of six lawful bases under Article 6(1) GDPR,[322] that consent is only appropriate as legal basis when the data subject is offered both control and a genuine choice to accept or decline the terms (without detriment),[323] and the four cumulative criteria of Article 4(11) GDPR (described above, Section 4.1) is met.[324]

Of special interest for this study, the EDPB gives guidance on the aspect of "imbalance of power".[325] The Board referred to Recital 43 GDPR, where it is stated that an imbalance between the data subject and the controller is unlikely to constitute freely given consent (using public authorities as a clear example).[326] More specifically, the EDPB states that imbalance of power are not only limited to

[317] C-40/17 - *Fashion ID*, ECLI:EU:C:2019:629.

[318] Waltraut Kotschy, 'Article 6. Lawfulness of processing ' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 328.

[319] C-13/16 - *Rīgas satiksme*, ECLI:EU:C:2017:336, para. 28; C-40/17 - *Fashion ID*, ECLI:EU:C:2019:629, para. 95.

[320] Kosta (n. 302), p. 349.

[321] EDPB Guidelines 05/2020 (n. 77).

[322] ibid., para. 2.

[323] ibid., para. 3.

[324] ibid., para. 11.

[325] ibid., paras. 16-24.

[326] ibid., para. 16.

authorities[327] and employers[328] (the two examples provided), and could occur elsewhere.[329] The important components when determining the validity of a consent is to ensure that the data subject can "exercise a real choice", there should not be any significant negative consequences (e.g. considerable extra costs) if the data subject do not consent, furthermore there should be no risk of intimidation, deception or coercion.[330] Therefore, the EDPB states that the consent will not be free (and thus invalid), if any element of "compulsion, pressure or inability to exercise free will" exists.[331]

Furthermore, the EDPB dedicates attention to the "conditionality" element of a consent, as explicitly stated in Article 7(4) GDPR. This Article indicates that, *inter alia*, both "bundling" (with e.g. other terms or conditions) and "tying" (e.g. to a provision of a contract or a service, when not necessary) a consent is highly undesirable, and such a given consent is presumed to not be freely given.[332] The EDPB clearly states that a compulsion to agree with additional use of personal data (outside of what is strictly necessary), does not constitute a free consent. With reference to the link between data protection law and the protection of fundamental rights, the Board elaborated on this point, by stating that consenting to unnecessary processing of personal data should not be a required condition in exchange for the fulfilment of a contract or access to a service.[333]

The EDPB recently issued a binding dispute resolution decision regarding Facebook and Instagram, with concerns, *inter alia*, about the legal basis for processing, where the Board found that Meta (parent company) had infringed Article 6(1) GDPR (although under the legal basis of a contract).[334] Even though data protection principles might be too "intangible" for the challenge in Section 4, it should be noted that the EDPB considered the principle of fairness[335] in relation

[327] ibid., paras. 16-20.

[328] ibid., paras. 21-23.

[329] ibid., para. 24.

[330] ibid.

[331] ibid.

[332] ibid., para. 26.

[333] ibid., para. 27.

[334] See, *inter alia*, EDPB, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR) Adopted on 5 December 2022, para. 314.

[335] Article 5(1)(a) GDPR.

to "take-it-or-leave-it" services on digital platforms.[336]

4.1.3 Theory by Legal Scholars

In the context of digital platforms, the most common legal basis for processing personal data is to obtain a consent from the data subject, as defined, *inter alia*, in Article 4(11) GDPR (described above). Obtaining this consent, in a correct way, can be difficult in highly concentrated markets where "take-it-or-leave-it" offers are common, and where consumers do not have any real substitute and must accept the provided conditions if they want to access the service.[337]

Through "free" online services, there might not be an alternative service where less personal data is required, and the consumers of these services (provided by digital platforms) have seldom or no bargaining power, to e.g. negotiate privacy policies, which constitute a "significant imbalance", thus questioning the genuine choice of the data subject to consent.[338] Multiple legal scholars have raised the complex question of a valid consent (within the GDPR) in relation to a strong market power.[339]

AG Rantos discussed the question of a valid consent in the context of market power, in the recent Opinion to the *Facebook v Bundeskartellamt* case from September 2022, where Article 4(11), 6(1)(a) and 7 GDPR and Recital 43 GDPR was described, in the context of digital platforms.[340] AG Rantos is of the opinion that the dominant position of a personal data controller should be considered when assessing the validity of a consent by the consumers, as this relationship is a clear imbalance of power.[341] Important to note, is that AG Rantos do not think the same level of market power is required to enforce the GDPR, compared to Article 102 TFEU (see Section 4.4 below).[342] On its own, AG Rantos does not believe that a dominant position should render a consent invalid, but reiterates that the dominance

[336] EDPB, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR) Adopted on 5 December 2022, paras. 156-157.

[337] Graef (n. 26), p. 294.

[338] EDPS (n. 1), para. 79; Graef (n. 26), p. 294-295.

[339] See e.g., Graef (n. 26), p. 295; Crémer, de Montjoye and Schweitzer (n. 23), p. 79; Gal and Aviv (n. 249), p. 364; Geradin, Bania and Karanikioti (n. 36), p. 8.

[340] Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704, paras. 71 and 74.

[341] ibid., para. 75.

[342] ibid.

does play a role and creates a clear imbalance of power between the data controller and subject, components such as "strictly necessary", "specific" and that the withdrawal of such consent should not negatively impact the end user is important considerations.[343]

4.2 Tying and Bundling under Article 102 TFEU

Generally, tying and bundling, within Article 102 TFEU, are situations where the dominant undertaking "connects" the sale of separate products, and customers are forced to buy both products (i.e., one of the products is not accessible without the other). This behaviour makes it possible for the dominant undertaking to leverage the market where it holds a dominant position to e.g., compete where it does not have such market power.[344] There are multiple dimensions to tying and bundling, it can be done through discounts, contracts, or other means. It could also be a mixture, where the separate products are available individually, but if bought together there are added benefits (e.g., discounts).[345] Thus, the two products are the "tying" and the "tied", generally the undertaking holds a dominant position on the market for the "tying product".[346]

4.2.1 Case-law by the CJEU

Abusive tying consists of three essential elements.[347] (i) The "tying" and "tied" products must be separate products, e.g. if the majority of customers would not buy the tied product when buying the tying product.[348] (ii) There is no choice to get the tying product without the tied product, this includes commercial disadvantages from not getting the products together, e.g. withdrawing the benefits of a guarantee from customers using a competitors components, or making it technically impossible to uninstall software on an operating system,[349] strong persuasion still exists even if the tied product is free.[350] (iii) The behaviour is capable of restricting

[343] ibid., para. 77.

[344] Ezrachi (n. 121), p. 188.

[345] ibid.

[346] Kellerbauer (n. 11), p. 1055.

[347] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 842 and 869; Kellerbauer (n. 11), p. 1055.

[348] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 917 and 921-922; Kellerbauer (n. 11), p. 1055.

[349] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 63.

[350] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 967-969; Kellerbauer (n. 11), p. 1055.

competition.[351]

Furthermore, there could still be abusive tying of two products even if the products have a natural link or are connected "according to commercial usage" (under the wording of Article 102(d) TFEU), the CJEU justified such a view because the list of abusive behaviour in Article 102 TFEU is not exhaustive.[352]

In the *Microsoft* case, the CJEU concluded that Microsoft had infringed Article 102 TFEU through, *inter alia*, tying and bundling its Windows Media Player (tied product) to its operating system (tying product).[353] The discussion of tying and bundling was also held in the *Google Shopping* case, where the CJEU reiterated its position that the "mere extension" of a dominant position to a neighbouring market does not constitutes anticompetitive behaviour.[354] But, the CJEU still reiterated that this leveraging could create anticompetitive behaviour, *inter alia*, tying or bundling.[355] Although, in the *Google Shopping* case, the CJEU did not rely on leveraging alone.[356]

4.2.2 Decision and Viewpoint by the Commission

Although not relating it to abuse *per se*, the Commission mentioned the challenge of "imbalanced bargaining power" in its impact assessment to the DMA, as a "problem driver".[357]

The Commission have, in particular, investigated three tying situations by digital platforms, *Microsoft Explorer* (failure to comply with its commitment, 2013)[358],

---

[351] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 1031-1090; Kellerbauer (n. 11), p. 1055.

[352] C-6/72 - *Europemballage Corporation and Continental Can Company v Commission*, ECLI:EU:C:1973:22, para. 26; C-395/96 P - *Compagnie Maritime Belge Transports and Others v Commission*, ECLI:EU:C:2000:132, para. 112; C-333/94 P - *Tetra Pak v Commission*, ECLI:EU:C:1996:436, para. 37; T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 860; Ezrachi (n. 121), p. 272; Kellerbauer (n. 11), p. 1056.

[353] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, paras. 842-859; Ezrachi (n. 121), p. 272.

[354] C-209/10 - *Post Danmark*, ECLI:EU:C:2012:172, para. 22; C-413/14 P - *Intel v Commission*, ECLI:EU:C:2017:632, para. 134; T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 162; Chirita (n. 23), p. 17.

[355] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 1344; T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 164; Chirita (n. 23), p. 17.

[356] T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, para. 175; Chirita (n. 23), p. 17.

[357] SWD DMA (n. 23), paras. 67 and 85.

[358] COMMISSION DECISION of 6.3.2013 addressed to Microsoft Corporation relating to a proceeding on the imposition of a fine pursuant to Article 23(2)(c) of Council Regulation (EC) No 1/2003 for failure to comply with a commitment made binding by a Commission decision pursuant to Article 9 of Council Regulation (EC) No 1/2003 Case AT.39530 – Microsoft (Tying).

Google Android (2018)[359] and *Google AdTech* (ongoing)[360].[361] Which have not also been investigated by the CJEU.

In the *Google Android* case, the Commission found that Google Android had tied both Google Search and Google Chrome to its Play Store (android app store).[362] Even if there only is a vague connection between the two services and the Play Store, they could still have been offered separately.[363] This tying gave Google a significant competitive advantage, which consequently degraded innovation,[364] harmed consumers,[365] and strengthen Google's dominant position.[366]

4.2.3 Theory by Legal Scholars

To begin with, it is important to emphasize that the theories of this section (albeit not to say that the theories of the other sections are not) are both novel and highly theoretical.

The concept typically referred to as "take-it-or-leave-it" service offerings (or binary consent terms of services), have recently received more attention by both data privacy and competition authorities. Within this concept, it is conditional for the end user to consent to certain data privacy policies, some digital platforms require the consumer's consent for access (e.g., many social media services), while others provide opt-out options (e.g., many search engines).[367]

The presence of "take-it-or-leave-it" data processing terms have been viewed as an imbalanced bargaining power between the digital platforms and its end users. Furthermore, the concerns for such terms are higher in concentrated markets (e.g., digital platforms), where the concerned services are typically hard for the end user

[359] COMMISSION DECISION of 18.7.2018 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (the Treaty) and Article 54 of the EEA Agreement (AT.40099 – Google Android).

[360] European Commission, *AT.40670 Google - Adtech and Data-related practices* <https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_AT_40670> (visited 2023-05-16).

[361] Crémer, Dinielli, Heidhues et al (n. 156), p. 14.

[362] AT.40099 – Google Android (n. 359), paras. 737 and 751-752.

[363] T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289, para. 939; AT.40099 – Google Android (n. 359), paras. 1011 and 1013; Chirita (n. 23), p. 33.

[364] AT.40099 – Google Android (n. 359), paras. 773, 947, 969 and 979.

[365] AT.40099 – Google Android (n. 359), paras. 971 and 1142.

[366] Chirita (n. 23), p. 33.

[367] Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 121.

to function without.[368] As stated by the UK's Competition and Markets Authority:[369]

> [L]imited choice and competition also have the consequence that people are less able to control how their personal data is used and may effectively be faced with a '*take it or leave it*' offer when it comes to signing up to a *platform's terms and conditions*. For many, this means they have to *provide more personal data to platforms than they would like*.

As stated by Lande back in 2008, and referred to by multiple legal scholars,[370] competition is about consumer choice and price is only one type of choice, consumers also want choices of other non-price dimensions, such as privacy protection.[371] Forcing a decision upon consumers has been suggested as a type of abuse.[372]

Mandrescu has suggested that, when the end users do not have any other choice but to consent to the given terms, this could constitute tying or bundling practices within the meaning of Article 102 TFEU.[373] This has also been indicated by Chirita, in a discussion about behavioural versus contractual tying.[374] Furthermore, Condorelli and Padilla have discussed privacy policy tying in relation to abuse and Article 102 TFEU in two of their papers,[375] but the two scholars are unfortunately not legal scholars (albeit Associate Professor of Economics)[376] and the paper which received comments and suggestions by legal scholars,[377] did not explicitly mention

---

[368] Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 121-122.

[369] Competition and Markets Authority, *Online platforms and digital advertising Market study final report* (2020), p. 8 (emphasis added); Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 122.

[370] See e.g., Ezrachi and Robertson (n. 3), p. 8, Footnote 39; Agustin Reyna, *The Psychology of Privacy - What Can Behavioral Economic Contribute to Competition in Digital Markets?* (International Data Privacy Law, 2018), p. 246.

[371] Lande (n. 26), p. 714.

[372] Reyna (n. 370), p. 249.

[373] Daniel Mandrescu, *Tying and bundling by online platforms – Distinguishing between lawful expansion strategies and anti-competitive practices* (Computer Law & Security Review, 2020), p. 24.

[374] Chirita (n. 23), p. 32-34.

[375] See Daniele Condorelli and Jorge Padilla, *Harnessing Platform Envelopment in the Digital World* (2020), Available on SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504025>; Daniele Condorelli and Jorge Padilla, *Data-Driven Envelopment with Privacy-Policy Tying* (2021) Available on SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600725>.

[376] University of Warwick, *Daniele Condorelli* <https://warwick.ac.uk/fac/soc/economics/staff/dcondorelli/> (visited 2023-05-22).

[377] Condorelli and Padilla (n. 375), p. 1, Footnote 1.

Article 102 TFEU (only "abuse").[378] Although, the close ties between competition law and economics,[379] is an indication of potential exploration.

4.3 Obligation under the DMA

Article 5 DMA stipulate provisions which do not require any further specification, i.e. the rules are categorised as clear enough to not need any further guidance from the Commission.[380] More specifically for this study, Article 5(2) DMA creates an "opt-in obligation" for the use of personal data.[381] Hence, there are four types of conducts that gatekeepers cannot do without, *inter alia*, consent from the end user: (i) "process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper"[382], (ii) "combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services"[383], (iii) "cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa"[384], and (iv) "sign in end users to other services of the gatekeeper in order to combine personal data"[385]. For example, Meta cannot combine the personal data generated from its social media platform Facebook, with the personal data generated from its other services, such as Instagram or WhatsApp, without the consent of the end users.[386]

In Article 5(2) DMA a clear reference is made to the GDPR and specifically Article 4(11) and 7 GDPR, when the Article clarifies that a consent is required to do any of the personal data processing in Article 5(2)(a-d) DMA. Furthermore, if a consent is withdrawn by the end user, the gatekeeper is not allowed to request for a new

[378] Condorelli and Padilla (n. 375), p. 45.

[379] See e.g., Damien J. Neven, Competition economics and antitrust in Europe (Economic Policy, 2006); David J. Gerber, Competition Law and Antitrust (Oxford University Press, 2020), p. 19.

[380] Witt, *The Digital Markets Act – Regulating the Wild West* (n. 13), p. 15.

[381] Belloso (n. 130), p. 2.

[382] Article 5(2)(a) DMA.

[383] Article 5(2)(b) DMA.

[384] Article 5(2)(c) DMA.

[385] Article 5(2)(d) DMA.

[386] Belloso (n. 130), p. 2.

consent (for the same purpose) more than one time per year.[387] It is also stated that Article 5(2) is "without prejudice" for the gatekeeper to use the legal basis, "legal obligation"[388], "vital interests"[389] or "public interest"[390].[391] Interestingly, the gatekeeper do not have the option to rely on "legitimate interests"[392] or "performance of a contract"[393] as a legal basis under the GDPR and within the DMA.[394]

The Preamble to the DMA mention the "serious imbalances in bargaining power", that can lead to unfair practices and conditions for both business and end users,[395] as well as the "superior bargaining power" of the gatekeepers vis-à-vis its users, which makes it possible to engage in abusive behaviour.[396] Furthermore, the Preamble also mention the "consent component", that it should present a user-friendly solution in order to conduct all the requirements for a valid consent (provide, modify and withdraw), with clear reiteration to the GDPR.[397] The Preamble also clarifies that the end user should, in a proper way, be informed that not providing a consent can result in less personalised offers (although no other degradation should occur).[398]

Two Articles in particular prohibits tying (or bundling) under the DMA.[399] Gatekeepers are not allowed to tie "identification service", "a web browser engine" or "a payment service" to its digital platforms, according to Article 5(7) DMA.[400] Furthermore, Article 5(8) DMA appears, according to Cremer et al, to be the "anti-tying provision" which prohibits the requirement of, *inter alia*, end users to register within one service in order to get access to another (but it has also been called a

[387] Article 5(2)(2) DMA.
[388] Article 6(1)(c) GDPR.
[389] Article 6(1)(d) GDPR.
[390] Article 6(1)(e) GDPR.
[391] Article 5(2)(3) DMA.
[392] Article 6(1)(f) GDPR.
[393] Article 6(1)(b) GDPR.
[394] Geradin, Bania and Karanikioti (n. 36), p. 7, Footnote 31.
[395] Recital 4 DMA.
[396] Recital 33 DMA.
[397] Recital 37 DMA.
[398] Recital 37 DMA.
[399] Madiega (n. 263), p. 9; Crémer, Dinielli, Heidhues et al (n. 156), p. 14.
[400] Madiega (n. 263), p. 9.

"bundling" provision)[401].[402]

To avoid circumventions by the gatekeepers, the DMA includes a specific anti-circumvention provision, under Article 13.[403] Specifically, Article 13(5) DMA stipulates that the no circumvention measures are allowed when a consent is required, and the gatekeepers are not allowed to, *inter alia*, degrade the conditions when the end-users exercise the right to, *inter alia*, consent or not.[404]

4.4 Plausible Overlap and Interplay

As mentioned above (Section 2.3), reducing "choice" could be a dimension of competition.[405] According to Graef, consumer "choice" or product variety (which ultimately offer more choices) is the most appropriate non-price dimension of competition law. Through this approach, the heterogeneity of consumers (regarding data privacy preferences) is considered, but not making assumptions regarding their preferences, simply concluding that there is an added benefit of having multiple choices, and that it is up to the consumer to choose between an adequate level of data privacy and personalisation (etc.) of the provided service.[406] Reiterating the above mentioned (Section 4.2.3) statement from Lande, that competition is about consumer choices, including data protection.[407]

Furthermore, according to Graef, by incorporating "consumer choice or product variety" as part of competition law, this enables the possibility to account for undertakings that offer different levels of heterogeneity in their products and services with regard to data privacy. Even if consumers may not always choose wisely due to externalities and biases, data protection can still be a valid choice or variety under competition law, as long as data protection law guarantees a minimum standard of protection. Thus, competition and data protection law must work together to create a well-functioning market where consumers can make informed choices.[408] Graef thus concludes that data protection could become a dimension in,

[401] Madiega (n. 263), p. 9.
[402] Crémer, Dinielli, Heidhues et al (n. 156), p. 30.
[403] Madiega (n. 263), p. 10.
[404] Article 13(6) DMA.
[405] Graef (n. 26), p. 309.
[406] ibid., p. 314.
[407] Lande (n. 26), p. 714.
[408] Graef (n. 26), p. 314.

inter alia, abuse cases under Article 102 TFEU, if the behaviour by the dominant undertaking is likely to harm "consumer choice or product variety".[409] It is still important to note, as emphasised by Graef, that competition enforcement is not used as a tool to increase data protection, it simply facilitates a market where the consumer can decide their level of data privacy.[410]

AG Rantos acknowledged, in the Opinion for *Facebook v Bundeskartellamt*, that a dominant position of a digital platform is a factor when determining if a consent for data processing was "freely given". But AG Rantos also clearly emphasizes that the "dominant position" required to render a consent invalid within the GDPR, is not necessarily equal to a "dominant position" within Article 102 TFEU, and also that consent cannot be invalid on this account alone.[411] For this reason, AG Rantos states that the validity of a consent should be determined on a case-by-case basis.[412]

The interplay between the GDPR and the DMA, regarding the challenge of "imbalanced bargaining power", is self-explanatory, because e.g. a consent within the DMA is solely based on what the GDPR constitutes as a valid consent (the DMA refers to the GDPR to constitute legal basis for processing).[413] The gatekeepers can rely on four of the six legal bases for the processing of personal data, and (as stated above, Section 4.3) the DMA exclude the legal basis "legitimate interests" and "performance of a contract", making the DMA "stricter" in some sense, albeit still completely relying the GDPR.

Since tying and bundling could be regulated under Article 102 TFEU (see Section 4.2) and the DMA has clear tying-provision (Section 4.3), there could be an overlap between these two legal frameworks (which will be elaborated in the conclusion, below).

4.5 Conclusion on Imbalanced Bargaining Power

From the above sections, it can be concluded that the challenge "imbalanced bargaining power" can be regulated under each legal framework, but to different

[409] ibid., p. 314-315.

[410] ibid., p. 315.

[411] Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704, para. 75.

[412] ibid., para. 76.

[413] Article 5(2) DMA.

extents. If a consent by the data subject is not valid, then there will be no legal basis for processing, thus breaching the GDPR. This leads to the difficult task of determining what a valid consent involves, from the investigation, it can be concluded that a consent is invalid if the data subject does not have any other choice but to accept (i.e., no bargaining power). Which could question the "take-it-or-leave-it" privacy conditions of some digital platforms, (following the DMA, consent is the most relevant legal basis for digital platforms, as it does not allow "legitimate interest" or "contract" as legal basis). Furthermore, the tying dimension of Article 102 TFEU has been suggested as a possibility to tackle "privacy policy tying", but it must be noted that this is a highly theoretical theory. Lastly, regarding the DMA, consumers must make an active "choice" (consent, opt-in) in order for gatekeepers to process personal data in certain situations, and are not allowed to degrade the conditions for an end-user who e.g. do not consent (Section 4.3), this could be interpreted as an attempt to tackle the above described "take-it-or-leave-it" conditions, although it do not affect the imbalance bargaining power on the digital platform alone, only processing beyond the platform. Furthermore, the anti-tying provision stipulate that other "services" are not allowed to be tied, which leads to the question of what the "further processing of personal data" should be defined as. If the further processing of personal data (to improve the main service by creating more personalisation etc.) constitutes a service, it could be argued that a privacy policy, by analogy, is a "service", which does fall within the DMA provision. This definition would, although highly theoretical, also increase the possibility of applying Article 102 TFEU under an abusive tying situation.

The most distinct interplay within this challenge is between the GDPR and Article 102 TFEU. This interplay is probably the most realistic approach to applying Article 102 TFEU in a data privacy setting. By using, *inter alia*, the number of available "choices", the validity of a consent could be determined, and if the consent is invalid, this could be used as a benchmark for determining abuse under Article 102 TFEU (although it is still worth noting that this is highly theoretical). Furthermore, if the highly theoretical tying scenarios were possible, there would be an overlap between the DMA and Article 102 TFEU.

5. Degrading Data Privacy

5.1 Data Principles and Informed Consent under Article 4(11), 5, 7 and 13-14 GDPR

The principle of purpose limitation,[414] is regarded as a cornerstone of data protection, and it constitute a prerequisite for many fundamental data privacy requirements.[415] As can be derived from the name, the principle requires each processing to have a purpose (see elaboration below). The principle of data minimisation,[416] is a newcomer compared to the prior Directive. This principle require that the processing of personal data should only be performed if the purposes cannot be fulfilled by other means in a reasonable manner ("limited to what is necessary").[417] The "necessity" criteria refers both to quantity and quality, i.e. a data controller is not allowed to process an excessive amount of personal data and is also not allowed to process a single fraction of personal data if that fraction goes beyond the purpose.[418]

The investigation of a valid consent was performed above (Section 4.1). Specifically important for the challenge investigated in this Section, is the "informed" dimension within a valid consent.

The requirements for information transparency towards the data subject is stipulated in Article 13 and 14 GDPR. The two Articles are very similar, and share the same Recitals in the GDPR,[419] with the difference being how the personal data is obtained. Article 13 GDPR regulates the information that must be provided, to

[414] Article 5(1)(b) GDPR.

[415] Cécile de Terwangne, 'Article 5. Principles relating to processing of personal data' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 315.

[416] Article 5(1)(c) GDPR.

[417] Recital 39 GDPR; Terwangne (n. 415), p. 317.

[418] Terwangne (n. 415), p. 317.

[419] Recital 60-62; Gabriela Zanfir-Fortuna, 'Article 13. Information to be provided where personal data are collected from the data subject' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020), p. 415; Gabriela Zanfir-Fortuna, 'Article 14. Information to be provided where personal data have not been obtained from the data subject' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) (Oxford University Press, 2020),* p. 435.

the data subject, by the controllers when the personal data is directly collected (e.g., subscribing to a service), and Article 14 GDPR when the data is collected from a third party. Providing transparent information is especially important when third parties are involved, since it is likely that the data subject is unaware of the processing.[420]

On the one hand, Article 13 and 14 GDPR provide a list of information that the data controller must provide, which can be complicated, but still a straightforward list of what information the legislator deems necessary in order to be "informed". Whilst, on the other hand, the more abstract dilemma of concluding when the data subject actually *is* informed (i.e., have taken in the information), when consent is the legal basis could be argued as to fall under Article 4(11) and 7 GDPR.[421]

5.1.1 Case-law by the CJEU

The principle of purpose limitation is discussed by the CJEU in the *Digi*[422] case.[423] The CJEU reiterates the substance of the purpose limitation, set out in Article 5(1)(b) GDPR, and describes that personal data shall (i) "be collected for specified, explicit and legitimate purposes", and (ii) not be further processed beyond that purpose.[424] It can thus be concluded, from the wording, that the provision consists of two requirements (as indicated in the previous sentence).[425] The Court describes both the first[426] and the second[427] requirement.

The CJEU has not explicitly investigated the principle of data minimisation in its case-law. But in the *GC and Others*[428] the CJEU reiterated what it had pointed out in the *Google Spain*[429] case, that initially lawful processing of personal data can over time become unlawful due to the processing no longer being necessary, in the light of the initial purposes, especially when they are excessive, irrelevant, or

[420] Zanfir-Fortuna, *Article 14* (n. 419), p. 436.

[421] cf. EDPB Guidelines 05/2020 (n. 77), paras. 62-74.

[422] C-77/21 - *Digi*, ECLI:EU:C:2022:805.

[423] Luca Tosoni, 'Appendix 1: Data Protection Case Law Chart' in by Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary - Update of Selected Articles* (Oxford University Press, 2021), p. 294.

[424] C-77/21 - *Digi*, ECLI:EU:C:2022:805, para. 25.

[425] ibid., para. 26.

[426] ibid., para. 27.

[427] See, *inter alia*, C-77/21 - *Digi*, ECLI:EU:C:2022:805, paras. 29 and 32-34.

[428] C-136/17 - *GC and Others* (De-referencing of sensitive data), ECLI:EU:C:2019:773.

[429] C-131/12 - *Google Spain and Google*, ECLI:EU:C:2014:317.

inadequate.[430]

The case-law that involves providing the data subject with information, mainly discuss situations where the personal data was collected directly from the data subject (i.e Article 13 GDPR), and CJEU often did not make a useful distinction between direct and indirect collection of personal data from the data subject with regard to transparency (Article 13 vis-à-vis Article 14 GDPR).[431] Therefore, the cases are assumed to cover both Articles.

In the *Bara*[432] case, the CJEU reiterated the observation made by the AG of the case, that "(...) requirement to *inform* the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed (...) and their right to object to the processing of those data (...)"[433].[434]

Furthermore, in the *Fashion ID*[435] case, which has a connection to digital platforms, the CJEU concluded that websites which includes prompt-to-action features by a social media platform (e.g., Facebook Like-button plugin) can constitute a joined controlling together with that platform, with regard to the personal data collected on the website. Although, this is not the case, when the personal data has been transmitted to the social media platform and is being processed there.[436]

5.1.2 Guidelines and Opinions by the EDPB (ex WP29)

The WP29 commented on data minimisation and purpose limitation in relation to evolving business opportunities in their *Guidelines on Automated individual decision-making and Profiling*[437] (endorsed by EDPB)[438]. These opportunities, created by the ability to process large amounts of information, profiling and cheaper

[430] C-131/12 - *Google Spain and Google*, ECLI:EU:C:2014:317, para. 93; C-136/17 - *GC and Others (De-referencing of sensitive data)*, ECLI:EU:C:2019:773, para. 74; Terwangne (n. 415), p. 68.

[431] Zanfir-Fortuna, *Article 14* (n. 419), p. 441-442.

[432] C-201/14 - *Bara and Others*, ECLI:EU:C:2015:638.

[433] ibid., para. 33 (emphasis added).

[434] Opinion of Advocate General Cruz Villalón in C-201/14 - *Bara and Others*, ECLI:EU:C:2015:461, para. 74; Zanfir-Fortuna (n. 419), p. 422.

[435] C-40/17 - *Fashion ID*, ECLI:EU:C:2019:629.

[436] C-40/17 - *Fashion ID*, ECLI:EU:C:2019:629, paras. 102-105; Zanfir-Fortuna (n. 419), p. 424.

[437] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6 February 2018.

[438] EDPB, Endorsement 1/2018.

storage costs, can lead to the incentive of collecting more personal data than necessary (in case of future use). This makes both the principle of data minimisation and purpose limitation especially important for the data controllers to abide by, they must explain and justify the processing of personal data in a clear way.[439]

WP29 has also issued an *Opinion on purpose limitation*[440] (although not endorsed by the EDPB,[441] the Board have referred to this WP29 Opinion in their Guidelines 05/2020)[442]. The principle is built on two dimensions, the personal data is required to be collected for (i) "specified, explicit and legitimate purposes" and (ii) "not further processed in a manner that is incompatible with those purposes".[443] This "purpose" should already be stipulated at the time in which the personal data is collected, and processing that has unlimited or undefined purposes is unlawful. Furthermore, the purpose must not be hidden, and instead be both clearly expressed and unambiguous.[444]

The purpose limitation has a close link to Article 6(1)(a) GDPR, regarding consent, where it is stated that the processing for "(...) one or more *specific purposes*"[445].[446] Purposes that are general or vague, e.g. "future research", "improving users' experience", "marketing purposes", or "IT-security purposes", without further details are usually not *specific* enough.[447] The "specific" component of a valid consent, ensures both transparency for the data subject and a degree of control.[448] To comply with the "specific" component, the controller must in sum apply: (i) "purpose specification as a safeguard against function creep"[449], (ii) "granularity in consent requests"[450], and (iii) "clear separation of information related to obtaining

[439] WP 251 (n. 437), p. 11.

[440] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 03/2013 on purpose limitation Adopted on 2 April 2013, WP 203.

[441] EDPB, Endorsement 1/2018.

[442] EDPB Guidelines 05/2020 (n. 77), para. 55, Footnote 28 and 30.

[443] WP 203 (n. 440), p. 11-13; Terwangne (n. 415), p. 315.

[444] WP 203 (n. 440), p. 39; Terwangne (n. 415), p. 315.

[445] Emphasis added.

[446] EDPB Guidelines 05/2020 (n. 77), para. 55.

[447] WP 203 (n. 440), p. 16; EDPB Guidelines 05/2020 (n. 77), para. 55, Footnote 30.

[448] EDPB Guidelines 05/2020 (n. 77), para. 55.

[449] See EDPB Guidelines 05/2020 (n. 77), paras. 56-59.

[450] See EDPB Guidelines 05/2020 (n. 77), para. 60.

consent for data processing activities from information about other matters"[451].[452]

In the *Guidelines on consent*[453] by the EDPB, the Board reiterates the importance of informed consent, and that the requirement for transparency is a fundamental principle (based on Article 5 GDPR). That the data subject receives information before providing a consent is essential to make informed decisions (i.e. understand what is being agreed).[454] If the consent is not "informed", it will be rendered an invalid legal basis for processing, which means that the controller may breach Article 6(1)(a) GDPR.[455]

Furthermore, the EDPB explains the minimum content requirements for a consent to be regarded as "informed": (i) "the controller's identity"[456], (ii) "the purpose of each of the processing operations for which consent is sought"[457], (iii) "what (type of) data will be collected and used"[458], (iv) "the existence of the right to withdraw consent"[459], (v) "information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant"[460], and (vi) "on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46"[461]. As indicated in the references (footnotes), the minimum requirement for an "informed" consent provided by the EDPB, have an overlapping character with the list of Article 13 and 14 GDPR (required information to be provided by the data controller to the data subject).

Importantly, in the concluding paragraph of the "minimum content requirements for consent" of the guidelines by the EDPB, the Board notes that, depending on the circumstances and context of a case, additional information could be needed in order for the data subject to genuinely be "informed".[462]

---

[451] See EDPB Guidelines 05/2020 (n. 77), para. 61.

[452] ibid., para. 55.

[453] EDPB Guidelines 05/2020 (n. 77).

[454] ibid., para. 62.

[455] ibid., paras. 62-63.

[456] Recital 42 GDPR; EDPB Guidelines 05/2020 (n. 77), para. 64. cf. Article 13(1)(a) and 14(1)(a) GDPR.

[457] Recital 42 GDPR; EDPB Guidelines 05/2020 (n. 77), para. 64. cf. Article 13(1)(c) and 14(1)(c) GDPR.

[458] EDPB Guidelines 05/2020 (n. 77), para. 64.

[459] Article 7(3) GDPR; EDPB Guidelines 05/2020 (n. 77), para. 64. cf. Article 13(2)(c) and 14(2)(d) GDPR.

[460] EDPB Guidelines 05/2020 (n. 77), para. 64. cf. Article 13(2)(f) and 14(2)(g) GDPR.

[461] EDPB Guidelines 05/2020 (n. 77), para. 64. cf. Article 13(1)(f) and 14(1)(f) GDPR.

[462] EDPB Guidelines 05/2020 (n. 77), para. 65.

Furthermore, in the same guidelines, the EDPB stipulates *how* to provide the information, with a main reference to Article 7(2) and Recital 32 GDPR.[463] In general, the information should be understandable for "the average person" (i.e. no legal jargon),[464] and together with the WP29 *Guidelines on transparency* (see below), a "layered and granular" method could be a good approach to provide the information.[465]

In the *Guidelines on transparency*[466] by the WP29 (endorsed by the EDPB)[467], the list of categories of information that must be provided to the data subject under Article 13 and 14 GDPR is described. It is also clarified that the WP29 do not believe that there is any difference between the categories of information under sub-article 1 and 2 of Article 13 and 14 GDPR, and all information is of equal importance.[468] The guidelines describe, *inter alia*, "Appropriate measures"[469], "timing for provision of information"[470], "changes to Article 13 and Article 14 information"[471], "timing of notification of changes to Article 13 and Article 14 information"[472], "modalities - format of information provision"[473], "layered approach in a digital environment and layered privacy statements/ notices"[474], "'push' and 'pull' notices"[475], and "information on profiling and automated decision-making"[476]

As mentioned above (Section 4.1.2), the EDPB did conclude that Meta had infringed data protection principles under Article 5(1) GDPR.[477]

---

[463] ibid., para. 66.

[464] ibid., para. 67.

[465] ibid., para. 69.

[466] Article 29 Working Party Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018, WP260 rev.01.

[467] EDPB, Endorsement 1/2018, p. 1.

[468] WP 260 (n. 466), para. 23.

[469] ibid., paras. 24-25.

[470] ibid., paras. 26-28.

[471] ibid., para. 29.

[472] ibid., paras. 30-32.

[473] ibid., paras. 33-34.

[474] ibid., paras. 35-37.

[475] ibid., para. 39.

[476] ibid., para. 41.

[477] EDPB, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR) Adopted on 5 December 2022, para. 157.

5.1.3 Theory by Legal Scholars

AG Rantos mention both the principle of purpose limitation and data minimisation in the Opinion of *Facebook v Bundeskartellamt* (i.e in the context of digital platforms), but regarding the legal basis of a contract for processing. Likewise the AG stated that these principles are particularly relevant in contracts for *online* services, that generally have non-negotiable terms for the individual, and because there is a risk that the data controller seeks to maximise the possibility to collect and use the personal data.[478] Furthermore, Graef regarded both consent and purpose limitation in the context of digital platforms and competition law.[479] It is also worth noting that legal scholars have not taken the information requirements stipulated in Article 13-14 GDPR into consideration while addressing concerns with digital platforms, probably because these constitute a minimum threshold.

5.2 Excessive under Article 102 TFEU

Regarding exploitative abuses under Article 102 TFEU, the CJEU has mainly focused on the exploitation of consumers in the form of excessive pricing.[480] But, exploitative abuse in general, and thus particularly excessive pricing is highly controversial, and the argumentation against this type of intervention (for excessive pricing) through competition law is well debated.[481]

Currently, neither the Commission or national competition authorities have found dominant digital platforms in violation of Article 102 TFEU due to excessive pricing.[482] But in theory, many legal scholars believe this could be possible (especially in the context of large digital platforms), through an analogy from excessive pricing to excessive data collection, among other theories that include data privacy in the competition analysis (as described below, Section 5.2.3).

5.2.1 Case-law by the CJEU

According to the Court in the famous *United Brands*[483] case, excessive pricing is

[478] Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704, para. 51, Footnote 72.

[479] Graef (n. 26), p. 295.

[480] Anne Witt, *Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case* (Jean Monnet Working Paper, 2020), p. 3.

[481] ibid., p. 4.

[482] ibid., p. 6.

[483] C-27/76 - *United Brands v Commission*, ECLI:EU:C:1978:22.

abusive under Article 102 TFEU when a dominant undertaking impose prices that "(...) has *no reasonable relation to the economic value* of the product supplied (...)"[484].[485] Although no specification of how the "economic value" should be calculated have been made by the Court, it is still apparent that the excessiveness can be assessed on two analysis: (i) cost-price analysis,[486] i.e. the actual cost of providing the product/service and the charged price to the customers, and (ii) comparative analysis,[487] i.e. comparing prices on comparable markets or between comparable competitors.[488] Furthermore, the Court also stated that "[o]ther ways may be devised – and economic theorists have not failed to think up several – of selecting the rules for determining whether the price of a product is unfair"[489].[490] If several methods would need to be applied, should be determined on a case-by-case basis.[491]

According to Graef, the EDPS seems to rely on the argumentation of the *United Brands* case, in its Preliminary Opinion on *Privacy and competitiveness in the age of big data*, when stated that exploitative abuse could occur if "(...) the 'price' paid through the surrender of personal information to be considered *excessive in relation to the value of the service consumed* (...)"[492].[493]

5.2.2 Decision and Viewpoint by the Commission

The Commission has only applied Article 102 TFEU to excessive pricing (which basically encompass all exploitative abuse) in a few cases, especially compared to exclusionary abuse.[494] Interestingly, the Commission's *Guidance on Article 102 TFEU*[495] does not even cover exploitative abuse (the only soft law instrument by

[484] ibid., para. 250 (emphasis added).

[485] Kellerbauer (n. 11), p. 1050.

[486] See e.g., C-30/87 - *Bodson v Pompes funèbres des régions libérées*, ECLI:EU:C:1988:225, para. 31

[487] See e.g., C-226/84 - *British Leyland v Commission*, ECLI:EU:C:1986:421, paras. 25-30.

[488] Kellerbauer (n. 11), p. 1050.

[489] C-27/76 - *United Brands v Commission*, ECLI:EU:C:1978:22, para. 253.

[490] Kellerbauer (n. 11), p. 1050.

[491] ibid.

[492] EDPS (n. 1), p. 29 (emphasis added).

[493] Graef (n. 26), p. 356.

[494] Witt, *Excessive Data Collection as a Form of Anticompetitive Conduct* (n. 480), p. 5.

[495] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (Text with EEA relevance), OJ C 45, 24.2.2009, p. 7–20.

the Commission treats exclusionary abuse)[496].[497] The Commission has only in a few cases constitute excessive pricing as an abuse of a dominant position,[498] and rejected complaints in other cases,[499] and beyond "excessive prices" the prohibition of exploitative cases are almost unheard of.[500]

5.2.3 Theory by Legal Scholars

Recently, there has been an uptick in attention regarding exploitative abuse by dominant digital platforms, and the leading theories of exploitative abuse stem from the interaction between competition law and data privacy.[501]

Even though more and more legal scholars are accepting the data privacy dimension of competition law, it is still likely to be difficult to practically apply. The price-based tool and methodology of competition law is deeply rooted,[502] and it will likely be difficult to adapt these to zero-price markets.[503]

Large digital platforms can gain more insight into the preferences of their users by collecting personal data beyond e.g., the consent of the data subject, thus creating better services for both end users and business users (e.g., advertisers). This "excessive" collection of personal data, has been suggested as a potential abuse of dominance under Article 102 TFEU.[504] In the digital environment, personal data is often used as a currency, thus an analogy from the traditional "excessive pricing" to "excessive data collection" could be made (although questions still remain regarding what data threshold should constitute excessive).[505]

As initially indicated, it would probably be difficult to apply the economic test of

[496] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, para. 7.

[497] Witt, *Excessive Data Collection as a Form of Anticompetitive Conduct* (n. 480), p. 5.

[498] See e.g., 75/75/EEC: Commission Decision of 19 December 1974 relating to a proceeding under Article 86 of the EEC Treaty (IV/28.851 - General Motors Continental) (Only the Dutch text is authentic); 84/379/EEC: Commission Decision of 2 July 1984 relating to a proceeding under Article 86 of the EEC Treaty (IV/30.615 - BL) (Only the English text is authentic); 2001/463/EC: Commission Decision of 20 April 2001 relating to a proceeding pursuant to Article 82 of the EC Treaty (Case COMP D3/34493 — DSD) (Text with EEA relevance) (notified under document number C(2001) 1106).

[499] See e.g., Decision of 23 July 2004 (COMP/A.36.568/D3 – Scandlines Sverige AB v Port of Helsingborg).

[500] Witt, *Excessive Data Collection as a Form of Anticompetitive Conduct* (n. 480), p. 5.

[501] Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 117-118.

[502] ibid., p. 67.

[503] ibid., p. 69.

[504] Graef (n. 26), p. 356; Robertson (n. 26), p. 9.

[505] Graef (n. 26), p. 356

"excessive pricing" to the non-price excessiveness of personal data collection. The different data privacy preferences of end users, might require a user-specific analysis, some end users prefer personalisation and higher relevance, on the digital platforms, over strict data protection, while others do not.[506]

Similarly, excessive data collection has been suggested as an "unfair trading condition", as this is also part of Article 102(a) TFEU (alongside excessive pricing).[507] But as the study above shows, both the Commission and the CJEU have been very restrictive on the application of Article 102 TFEU on exploitative abuse, and excessive pricing is evidently the most used (see Section 5.2.1 and 5.2.2 above).

Furthermore, decreased "quality" has been suggested as a potential abuse within Article 102(b) TFEU (which is also considered a widely articulated viewpoint)[508].[509] This theory also meet multiple challenges, more specifically when it comes to data privacy quality, due to the heterogeneous preference by consumers on privacy (similarly as discussed above regarding excessive data collection).[510] Components such as information asymmetry, cognitive biases, the limited or complex choices, and even the fact that the consumers might be unable or unwilling to have changes made to the provided services, will further complicate the matter.[511]

Beyond the multiple problems with the "quality" dimension (as described in detail by Graef)[512], even end users which do value higher data protection, might be willing to opt for lower privacy in exchange for a free service, Graef effectively demonstrated the trade-off between the quality dimensions and the price of the service in a simple figure (see *Figure 3* below).[513]

[506] Graef (n. 26), p. 357.

[507] See Robertson (n. 26), 13-15.

[508] Douglas, *The New Antitrust/Data Privacy Law Interface* (n. 5), p. 654

[509] Aleksandra Gebicka and Andreas Heinemann, *Social Media & Competition Law* (World Competition, 2014), p. 163-164; Reyna (n. 370), p. 249.

[510] Graef (n. 26), p. 310; Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 69.

[511] Douglas, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (n. 26), p. 70.

[512] See Graef (n. 26), p. 310-311.

[513] Graef (n. 26), p. 311.

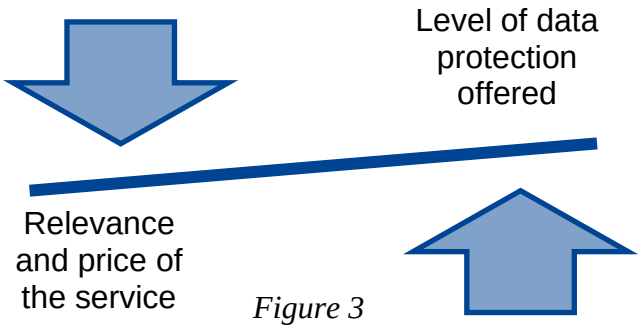

Figure 3

If the competition authorities align an increased data collection with degraded quality, the assumption of consumers preferences would ultimately have to be made, which would not match the reality of the consumers due to their heterogeneity.[514] A similarly argumentation could probably be held with regard to excessive data collection (as indicated above, with regard to different preferences).

5.3 Obligation under the DMA

Article 5(2) DMA is described above (Section 4.3). Specifically relating to the challenge in this section, is the anti-circumvention provision in Article 13(6) DMA, which states that gatekeepers "(...) shall not *degrade* the *conditions* or *quality* (...)"[515], when providing their services to end-users that use any of the rights and choices of, *inter alia*, Article 5 DMA. Furthermore, Article 13(6) DMA stipulates that any of the rights or choices that the end user have, cannot be made "unduly difficult" (including, *inter alia*, non-neutral offer of choices, free choice via the structure, decision-making, subverting the autonomy of end users or business users).

5.4 Plausible Overlap and Interplay

An interplay between the GDPR and Article 102 TFEU, on the grounds of excessive data collection, is to test the abusive behaviour against data protection principles, as a sort of "benchmark".[516] The purpose limitation and data minimisation principle (described above, Section 5.1), could be used as a benchmark for assessing abusive behaviour within the competition analysis and Article 102 TFEU, if e.g. the

[514] Graef (n. 26), p. 311.
[515] Emphasis added.
[516] Graef (n. 26), p. 357.

dominant undertaking breach any of the above mentioned principles, this could be an indication of abuse.[517]

This point can be supported by referring to the *AstraZeneca*[518] and *Allianz Hungária*[519] cases, where the CJEU determined that there had been a violation of competition law, on the basis that another area of law had been breached.[520] Specifically, the *AstraZeneca* case shows that "misuse of regulatory procedures" can amount to abuse, when the conduct can harm competition.[521]

Therefore, for this potential sub-category of Article 102 TFEU, the purpose limitation or data minimisation principles can serve as a criterion to assess whether the data collection by a dominant undertaking (e.g., large digital platform) is excessive and constitutes an abuse under Article 102 TFEU.[522]

Similarly, as to Section 4.4, the interplay between the GDPR and the DMA, regarding the challenge of "degrading data privacy", is somewhat self-explanatory, because the DMA gives the GDPR control regarding its "personal data" provision. Although, Article 5(2) only refers to the legal basis, regarding any circumvention measures that the gatekeeper might impose, Article 13(6) DMA broadly states that the degrading of *conditions* or *quality* is not allowed (which could both refer to data privacy).

Regarding the overlap between Article 102 TFEU and the DMA, the excessive collection of personal data is implicitly contained in Article 5(2) DMA (since it is especially hard to reach "excessive" levels of collection without including third-party sources of personal data) and requires an opt-in by the consumer (i.e. easier to prove), and the excessive abuse under Article 102 TFEU, although highly theoretical, could apply to the same conduct in an overlapping character.

---

[517] Graef (n. 26), p. 358.

[518] C-457/10 P - *AstraZeneca v Commisson*, ECLI:EU:C:2012:770.

[519] C-32/11 - *Allianz Hungária Biztosító and Others*, ECLI:EU:C:2013:160.

[520] C-457/10 P - *AstraZeneca v Commisson*, ECLI:EU:C:2012:770, paras. 107-113; C-32/11 - *Allianz Hungária Biztosító and Others*, ECLI:EU:C:2013:160, paras. 41 and 47; Graef (n. 26), p. 358-359.

[521] C-457/10 P - *AstraZeneca v Commisson*, ECLI:EU:C:2012:770, para. 112; Graef (n. 26), p. 358.

[522] Graef (n. 26), p. 362.

5.5 Conclusion on Degrading Data Privacy

From the above sections, it can be concluded that the challenge "degrading data privacy" can be regulated under each legal framework, but to different extents. The purpose limitation and minimisation principle under the GDPR, could render excessive collection of personal data unlawful. This could also be done if the "informed" criteria within a valid consent is not met (especially common on digital platforms, where the data subjects do not know to what extent their data is being used). Furthermore, in order to tackle excessive collection of personal data under Article 102 TFEU, theories have been proposed where an analogy is made to excessive pricing (because consumers "pay" with their personal data to access "free" services), although it is important to note that these theories where data privacy preference is used as a benchmark (also as a form of quality) is difficult to realise in practice due to the heterogeneity of consumers preferences. Lastly, the anti-circumvention provision of the DMA specifically prohibits gatekeepers from degrading both the conditions and quality of their services, which could be interpreted as including data privacy quality and conditions. Beyond this, further personal data processing is limited in the DMA by the consent of the end-user.

Similarly, as to Section 4.5, the most distinct interplay is between the GDPR and Article 102 TFEU, where the violation of data protection principles could be used as a benchmark for determining abuse, a similar interplay has been presented by the CJEU (using the violation of one rule to determine another). Although, once again worth noting that this is theoretical.

6. Final Conclusions

6.1 Answering the Research Questions

Initially, in Section 1.2, the aim of the thesis is presented as to describe and analyse how the challenges of "access to data", "imbalanced bargaining power", and "degrading data privacy" are regulated in the GDPR, Article 102 TFEU and the DMA, and the plausible overlap and interplay between the stipulated legal frameworks regarding these challenges, in the context of large digital platforms. This was framed in three regulation specific questions (one for each challenge), "To what extent is the challenge [(i) "access to data", (ii) "imbalanced bargaining power", (iii) "degrading data privacy"] regulated in the GDPR, Article 102 TFEU and the DMA?" and one comparing and analysing question (iv) "What is the plausible overlap and interplay between the legal frameworks, with regard to question I, II and III?".

Chapter 3-5 (above) have each ended with a concluding Section of the presented material, and this Section will, in summary, specifically answer each research question.

To answer the first (i) research question, the challenge "access to data" is regulated in the GDPR (data portability) to the extent that the data is requested (and observed) by the data subject. In Article 102 TFEU, for a dominant digital platform to grant access to data, this data must most likely be constituted as an "essential facility" (which requires multiple conditions, and extensive investigation), although theoretically possible, the practical application is extremely limited. Furthermore, the DMA will, naturally (as probably intended by the Commission), be the legal framework that tackles the challenge to the largest extent (in its data portability provision), as it is both free of charge, ported "live", and not limited to "personal data". Finally, the corresponding part of the fourth (iv) research question, is predominantly the overlap between the GDPR and the DMA, since both include data portability provisions, which have especially questioned the "without prejudice" clause of the DMA.

The answer to the second (ii) research question, regarding how the GDPR could regulate the challenge "imbalanced bargaining power", is by, *inter alia*, rendering a consent invalid due to the extent of the power differences. Article 102 TFEU could (under highly theoretical circumstances) prohibit large digital platforms from tying extensive data privacy policies to their services, by rendering this abusive. Furthermore, the DMA contains an anti-tying provision, which could be applicable to data privacy policies, if such a policy constitutes a "service" (for improving and personalising the main service, also highly theoretical). Finally, the corresponding part of the fourth (iv) research question, is predominantly the interplay between the GDPR and Article 102 TFEU, by using the choices and validity of consent as a benchmark to determine abuse. Also, if the highly theoretical tying scenarios where possible, this would create an overlap between Article 102 TFEU and the DMA.

To answer the third (iii) research question, the challenge "degrading data privacy" can be regulated through the purpose limitation and data minimisation principles of the GDPR. To a highly limited extent, Article 102 TFEU could (theoretical) prohibit large digital platforms from collecting excessive amounts of personal data, by regarding the data as a payment and through an analogy to excessive pricing, which can be abusive. The criticism to this approach stem from the heterogeneity of consumer preferences (i.e., difficult to determine what constitutes "excessive" for all consumers). Moreover, further processing of personal data is limited under the DMA to consent by the end-user, and DMA also includes anti-circumvention measures which prohibit gatekeepers from degrading both conditions and quality of their services. Finally, the corresponding part of the fourth (iv) research question, is predominantly the overlap between the GDPR and Article 102 TFEU, where the violation of data protection principles can be used as a benchmark for abuse (similarly as to challenge "imbalanced bargaining power", and also theoretical).

6.2 The Overarching Relationship between the Three Legal Frameworks

Thus, for the overarching conclusion which builds upon the fourth (iv) research question, could all three legal frameworks theoretically be applied to practically the same challenge? If this was the case, (i) infringing the GDPR (broadly speaking)

could result in fines up to 4 % of the total worldwide annual turnover,[523] (ii) infringing Article 102 TFEU could result in fines up to 10 % of the undertakings total turnover,[524] and (iii) infringing the obligations in the DMA could also result in fines up to 10 % of the gatekeepers worldwide turnover.[525] Applying the three legal frameworks to e.g. one of the challenges where all three legal frameworks are applicable, could theoretically add up to a combined fine of almost 1/4 (up to 24 %) of a dominant gatekeepers worldwide annual turnover.

As described in Section 2.3, the *bpost* case is believed to enable the Commission to apply both Article 102 TFEU and the DMA side-by-side *even* if they are regulating the same conduct. Thus, the case opens for two legal frameworks, but could also a third be possible? Given the criteria stipulated by the *bpost* case (i) the GDPR do pursue a different objective then both Article 102 TFEU and the DMA, (ii) when collecting personal data, the undertaking should foresee the application of the GDPR, the coordination between competition and data protection authorities should be possible (according to AG Rantos)[526], the application time is probably similar, and the consideration when calculating the fine should not be different from the relationship with Article 102 TFEU and the DMA. Criticism to this idea, is that the GDPR is probably not considered a "sector-specific" regulation, compared to one of the legal frameworks in the *bpost* case.

Although extremely theoretical, it does not seem to be completely unthinkable to apply the three legal frameworks to e.g., the *same* challenge (as described above in Chapter 3-5). But due to the consideration of multiple fines, the final percentage would probably be reduced. Either way, it can be concluded that the three provisions can be applicable to similar situations, but in accordance with EU law, the CJEU has the final say in the interpretation and application of the three legal frameworks, according to Article 19(1) TEU.[527]

---

[523] Article 83(5) GDPR.

[524] Article 23(3) of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance).

[525] Article 30 DMA.

[526] Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704, para. 33.

[527] Marcus Klamert and Bernhard Schima, 'Article 19 TEU', in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press, 2019), p. 176.

Bibliography

Official Publications

European Union

Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2004/C 31/03).

Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2008/C 265/07).

Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02).

Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (Text with EEA relevance), OJ C 45, 24.2.2009, p. 7–20.

Article 29 Working Party, Opinion 03/2013 on purpose limitation Adopted on 2 April 2013, WP 203.

Article 29 Working Party Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018, WP260 rev.01.

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6 February 2018.

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017.

EDPB, Endorsement 1/2018.

COMMISSION STAFF WORKING DOCUMENT 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), SWD/2020/363 final.

COMMISSION STAFF WORKING DOCUMENT Better Regulation Guidelines, SWD(2021) 305 final.

Literature

A. Bygrave L and Tosoni L, 'Article 4(11). Consent' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Ackermann T, 'European Competition Law', in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2017).

Ahlborn C and S. Evans D, *The Microsoft Judgment and its Implications for Competition Policy Towards Dominant Firms in Europe* (Antitrust Law Journal, 2008).

Axhamn J, *Databasskydd* (Publit, 2016).

Bania K, *Fitting the Digital Markets Act in the existing legal framework: the myth of the "without prejudice" clause* (European Competition Journal, 2022).

Belloso Moreno N, *The EU Digital Markets Act (DMA): A Summary (2022)*, Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109299>.

Bergemann D and Bonatti A, *Data, Competition, and Digital Platforms* (MIT Sloan Research Paper, 2022).

Bian B, Ma X, Tang H, *The Supply and Demand for Data Privacy: Evidence from Mobile Apps* (2021), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3987541>.

Binns R and Bietti E, *Dissolving Privacy, One Merger at a Time: Competition, Data and Third Party Tracking* (Computer Law & Security Review, 2018).

Buttarelli G, *Competition Rebooted: Enforcement and personal data in digital markets Keynote speech at Joint ERA-EDPS seminar Brussels* (2015).

Cappai M and Colangelo G, *Applying ne bis in idem in the Aftermath of bpost and Nordzucker: The Case of EU Competition Policy in Digital Markets* (a modified version is forthcoming in Common Market Law Review, 2023).

Competition and Markets Authority, *Online platforms and digital advertising Market study final report* (2020).

Condorelli D and Padilla J, *Harnessing Platform Envelopment in the Digital World* (2020), Available on SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504025>.

Condorelli D and Padilla J, *Data-Driven Envelopment with Privacy-Policy Tying* (2021) Available on SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600725>.

Costa-Cabral F and Lynskey O, *Family Ties: The Intersection between Data Protection and Competition in EU Law* (Kluwer Law International, 2017).

Crémer J, de Montjoye Y-A and Schweitzer H, *Competition Policy for the digital era Final report* (Directorate-General for Competition, 2019).

Crémer J, Dinielli D, Heidhues P, Kimmelman G, Monti G, Podszun R, Schnitzer M, Scott Morton F, de Streel A, *Enforcing the Digital Markets Act: Institutional Choices, Compliance, and Antitrust* (Yale Tobin Center for Economic Policy, 2022).

D. Chirita A, *Data-Driven Unfair Competition in Digital Markets* (Durham Law School Research Paper, 2022).

de Terwangne C, ‘Article 5. Principles relating to processing of personal data’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Docksey C, ‘Article 70 Tasks of the Board’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Douglas E, *The New Antitrust/Data Privacy Law Interface* (The Yale Law Journal Forum, 2021).

E. Stucke M, *Should We Be Concerned About Data-opolies?* (University of Tennessee Legal Studies Research Paper, 2018).

EDPB, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR) Adopted on 5 December 2022.

Egan E, *CHARTING A WAY FORWARD: Data Portability and Privacy* (Facebook White Paper, 2019).

Esayas S, *Data Privacy in European Merger Control: Critical Analysis of Commission Decisions Regarding Privacy as a Non-Price Competition* (European Competition Law Review, 2019).

European Commission, *Joaquín Almunia Vice President of the European Commission responsible for Competition Policy, Competition and personal data protection* (2012, SPEECH/12/860).

European Data Protection Supervisor, Preliminary Opinion, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, March 2014.

Ezrachi A and H.S.E. Robertson V, *Competition, Market Power and Third-Party Tracking* (Oxford Legal Studies Research Paper, 2018).

Ezrachi A, *Article 102 TFEU, EU Competition Law: An Analytical Guide to the Leading Cases* (Hart Publishing, 2014).

Gebicka A and Heinemann A, *Social Media & Competition Law* (World Competition, 2014).

Geradin D and Kuschewsky M, *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue* (2013), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088>.

Geradin D, Bania K and Karanikioti T, *The interplay between the Digital Markets Act and the General Data Protection Regulation* (2022), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203907>.

Goldberg S, Johnson G and Shriver S, *Regulating Privacy Online: An Economic Evaluation of the GDPR* (Law & Economics Center at George Mason University Scalia Law School Research Paper Series, 2019).

Graef I, *EU competition law, data protection and online platforms data as essential facility* (Kluwer Law International, 2016) ISBN-13 9789041183248.

Graef I, Tombal T and de Streel A, *Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law* (TILEC Discussion Paper, 2019).

H. Lande R, *The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern* (University of Baltimore School of Law Legal Studies Research Paper, 2008).

Hettne J and Otken Eriksson I, *EU-rättslig metod - Teori och genomslag i svensk rättstillämpning* (2nd Edition, Norstedts Juridik, 2011).

H.S.E. Robertson V, *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data* (Common Market Law Review, 2019).

J. Gerber D, *Competition Law and Antitrust* (Oxford University Press, 2020).

J. Neven D, *Competition economics and antitrust in Europe* (Economic Policy, 2006).

K. Ohlhausen M and Okuliar A, *Competition, Consumer Protection, and the Right (Approach) to Privacy* (Antitrust Law Journal, Forthcoming, 2015).

Kellerbauer M, ‘Article 102 TFEU’, in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press, 2019).

Kerber W and Specht L, *Synergies between Data Protection Law and Competition Law* (2021), Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3977039>.

Klamert M and Schima B, ‘Article 19 TEU’, in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights* (Oxford University Press, 2019).

Kleineman J, ‘Rättsdogmatisk metod’, in Maria Nääv & Mauro Zamboni (eds), *Juridisk metodlära* (2nd Edition, Studentlitteratur, 2018).

Kosta E, ‘Article 7. Conditions for consent’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Kotschy W, ‘Article 6. Lawfulness of processing’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Komninos A, *The Digital Markets Act: How Does it Compare with Competition Law?* (2022) Available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136146>.

Krämer J, Senellart P, de Streel A, *Making data Portability More Effective for The Digital Economy* (Centre on Regulation in Europe, 2020).

Köndgen J, ‘Sources of law’, in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2017).

Larouche P and de Streel A, *Interplay between the New Competition Tool and Sector-Specific Regulation in the EU* (Directorate-General for Competition, 2020).

Law J, *A Dictionary of Business and Management* (5th Edition, Oxford University Press, 2009) ISBN-13: 9780199234899.

Li W et al, *A multimodal psychological, physiological and behavioural dataset for human emotions in driving tasks* (Scientific Data, 2022).

Lynskey O, 'Article 20. Right to data portability' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

M. Douglas E, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* (Temple University Legal Studies Research Paper, 2021).

M. Smits J, *What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research* (Maastricht European Private Law Institute Working Paper, 2015).

Madiega T, *Digital Markets Act* (European Parliamentary Research Service, 2022).

Mandrescu D, *Tying and bundling by online platforms – Distinguishing between lawful expansion strategies and anti-competitive practices* (Computer Law & Security Review, 2020).

Monti G, *The Digital Markets Act – Institutional Design and Suggestions for Improvement* (TILEC Discussion Paper, 2021).

Motta M and Peitz M, *Intervention triggers and underlying theories of harm Expert advice for the Impact Assessment of a New Competition Tool Expert study* (Directorate-General for Competition, 2020).

Nowag J and Groussot X, *From Better Regulation to Better Adjudication? Impact Assessment and the Court of Justice's Review* (Lund University Legal Research Paper Series, 2017).

OECD, *The evolving concept of market power in the digital economy* (2022).

Pereira Avelar F, *Global Framework Agreements: A Response to Urgent Global Labour Concerns* (1st Edition, Lund University, 2021).

Reichel J, 'EU-rättslig metod', in Maria Nääv & Mauro Zamboni (eds), *Juridisk metodlära* (2nd Edition, Studentlitteratur, 2018).

Reyna A, *The Psychology of Privacy - What Can Behavioral Economic Contribute to Competition in Digital Markets?* (International Data Privacy Law, 2018).

Riesenhuber K, ‘Interpreation of EU Secondary Law’, in Karl Riesenhuber (ed), *European Legal Methodology* (Intersentia 2017).

S Gal M and Aviv O, *The Competitive Effects of the GDPR* (Oxford Academic, 2020).

Schweitzer H and Welker R, *A Legal Framework for Access to Data – A Competition Policy Perspective* (German Federal Ministry of Justice and Consumer Protection, 2020).

Tombal T, *GDPR As Shield to a Data Sharing Remedy* (CPDP 2020 and ASCOLA 2020 Conferences, 2020).

Tosoni L, ‘Appendix 1: Data Protection Case Law Chart’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary - Update of Selected Articles* (Oxford University Press, 2021).

Witt A, *Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case* (Jean Monnet Working Paper, 2020).

Witt A, *The Digital Markets Act – Regulating the Wild West* (Common Market Law Review, 2023).

WORLD BANK GROUP, World Development Report 2021: data for better lives.

WORLD ECONOMIC FORUM, *Personal Data: The Emergence of a New Asset Class* (2011).

Zanfir-Fortuna G, ‘Article 13. Information to be provided where personal data are collected from the data subject’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Zanfir-Fortuna G, ‘Article 14. Information to be provided where personal data have not been obtained from the data subject’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Zanfir-Fortuna G, ‘Article 15. Right of access by the data subject’ in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).

Online sources

European Commission, *AT.40670 Google - Adtech and Data-related practices* <https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_AT_40670> (visited 2023-05-16).

European Commission, *Factual summary of the contributions received in the context of the open public consultation on the New Competition Tool* (2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/summary_stakeholder_consultation.pdf> (visited 2023-05-25).

European Commission, *Summary of the contributions of the National Competition Authorities to the impact assessment of the new competition tool* (2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/summary_contributions_NCAs_responses.pdf> (visited 2023-05-25).

LinkedIn, *Top Companies 2022: The 50 best workplaces to grow your career in the U.S.* <https://www.linkedin.com/pulse/top-companies-2022-50-best-workplaces-grow-your-career-us-/> (visited 2023-04-14).

Statista, *The 100 largest companies in the world by market capitalization in 2022* <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/> (visited 2023-04-14).

University of Warwick, *Daniele Condorelli* <https://warwick.ac.uk/fac/soc/economics/staff/dcondorelli/> (visited 2023-05-22).

Cases

European Union

Court of Justice

C-26/62 - *Van Gend en Loos v Administratie der Belastingen*, ECLI:EU:C:1963:1.

C-6/72 - *Europemballage Corporation and Continental Can Company v Commission*, ECLI:EU:C:1973:22.

C-6/73 - *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, ECLI:EU:C:1974:18.

C-155/73 - *Sacchi*, ECLI:EU:C:1974:40.

C-34/74 - *Roquette Frères v French State*, ECLI:EU:C:1974:117.

C-27/76 - *United Brands v Commission*, ECLI:EU:C:1978:22.

C-53/81 - *Levin v Staatssecretaris van Justitie*, ECLI:EU:C:1982:105.

C-322/81 - *Michelin v Commission*, ECLI:EU:C:1983:313.

C-226/84 - *British Leyland v Commission*, ECLI:EU:C:1986:421.

C-30/87 - *Bodson v Pompes funèbres des régions libérées*, ECLI:EU:C:1988:225.

C-215/88 - *Casa Fleischhandel v BALM*, ECLI:EU:C:1989:331.

C-241/91 P - *RTE and ITP v Commission*, ECLI:EU:C:1995:98.

C-333/94 P - *Tetra Pak v Commission*, ECLI:EU:C:1996:436.

C-251/95 - *SABEL v Puma, Rudolf Dassler Sport*, ECLI:EU:C:1997:528.

Opinion of Advocate General Jacobs in C-7/97 - *Bronner*, ECLI:EU:C:1998:264.

C-7/97 - *Bronner*, ECLI:EU:C:1998:569.

C-395/96 P - *Compagnie Maritime Belge Transports and Others v Commission*, ECLI:EU:C:2000:132.

C-238/99 P - *Limburgse Vinyl Maatschappij and Others v Commission*, ECLI:EU:C:2002:582.

C-444/00 - *Mayer Parry Recycling*, ECLI:EU:C:2003:356.

Opinion of Advocate General Stix-Hackl in C-222/02 - *Paul and Others*, ECLI:EU:C:2003:637.

C-204/00 P - *Aalborg Portland and Others v Commission*, ECLI:EU:C:2004:6.

C-418/01 - *IMS Health*, ECLI:EU:C:2004:257.

C-397/01 - *Pfeiffer and Others*, ECLI:EU:C:2004:584.

C-95/04 P - *British Airways v Commission*, ECLI:EU:C:2007:166.

C-404/06 - *Quelle*, ECLI:EU:C:2008:231.

C-468/06 - *Sot. Lélos kai Sia*, ECLI:EU:C:2008:504.

C-202/07 P - *France Télécom v Commission*, ECLI:EU:C:2009:214.

C-52/09 - *TeliaSonera Sverige*, ECLI:EU:C:2011:83.

C-543/09 - *Deutsche Telekom*, ECLI:EU:C:2011:279.

C-468/10 - *ASNEF*, ECLI:EU:C:2011:777.

C-209/10 - *Post Danmark*, ECLI:EU:C:2012:172.

C-457/10 P - *AstraZeneca v Commisson*, ECLI:EU:C:2012:770.

C-32/11 - *Allianz Hungária Biztosító and Others*, ECLI:EU:C:2013:160.

C-280/13 - *Barclays Bank*, ECLI:EU:C:2014:279.

C-131/12 - *Google Spain and Google*, ECLI:EU:C:2014:317.

C-129/14 PPU - *Spasic*, ECLI:EU:C:2014:586.

Opinion of Advocate General Cruz Villalón in C-201/14 - *Bara and Others*, ECLI:EU:C:2015:461.

C-201/14 - *Bara and Others*, ECLI:EU:C:2015:638.

C-23/14 - *Post Danmark*, ECLI:EU:C:2015:651.

C-582/14 - *Breyer*, ECLI:EU:C:2016:779.

C-13/16 - *Rīgas satiksme*, ECLI:EU:C:2017:336.

C-413/14 P - *Intel v Commission*, ECLI:EU:C:2017:632.

C-136/17 - *GC and Others (De-referencing of sensitive data)*, ECLI:EU:C:2019:773.

Opinion of Advocate General Szpunar in C-673/17 - *Planet49*, ECLI:EU:C:2019:246.

C-673/17 - *Planet49*, ECLI:EU:C:2019:801.

Opinion of Advocate General Saugmandsgaard Øe in C-152/19 P - *Deutsche Telekom v Commission*, ECLI:EU:C:2020:678.

C-61/19 - *Orange Romania*, ECLI:EU:C:2020:901.

C-117/20 - *bpost*, ECLI:EU:C:2022:202.

C-151/20 - *Nordzucker and Others*, ECLI:EU:C:2022:203.

C-48/22 P - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:C:2022:207.

Opinion of Advocate General Rantos in C-252/21 - *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2022:704.

C-77/21 - *Digi*, ECLI:EU:C:2022:805.

General Court (Tribunal)

T-504/93 - *Tiercé Ladbroke v Commission*, ECLI:EU:T:1997:84.

T-371/03 - *Le Voci v Council*, ECLI:EU:T:2005:290.

T-322/01 - *Roquette Frères v Commission*, ECLI:EU:T:2006:267.

T-201/04 - *Microsoft v Commission*, ECLI:EU:T:2007:289.

T-301/04 - *Clearstream v Commission*, ECLI:EU:T:2009:317.

T-307/12 - *Mayaleh v Council*, ECLI:EU:T:2014:926.

T-60/06 RENV II - *Italy v Commission*, ECLI:EU:T:2016:233.

T-612/17 - *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763.

European Commission

75/75/EEC: Commission Decision of 19 December 1974 relating to a proceeding under Article 86 of the EEC Treaty (IV/28.851 - General Motors Continental) (Only the Dutch text is authentic).

84/379/EEC: Commission Decision of 2 July 1984 relating to a proceeding under Article 86 of the EEC Treaty (IV/30.615 - BL) (Only the English text is authentic).

2001/463/EC: Commission Decision of 20 April 2001 relating to a proceeding pursuant to Article 82 of the EC Treaty (Case COMP D3/34493 — DSD) (Text with EEA relevance) (notified under document number C(2001) 1106).

COMMISSION DECISION of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft), C(2004)900 final.

Decision of 23 July 2004 (COMP/A.36.568/D3 – Scandlines Sverige AB v Port of Helsingborg).

COMMISSION DECISION of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 – Google/ DoubleClick), C(2008) 927 final.

Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, C(2014) 7239 final.

COMMISSION DECISION of 4.5.2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (TFEU) and Article 54 of the EEA Agreement Case AT.40153 – E-book MFNs and related matters.

COMMISSION DECISION of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)).