# Bonding the Two Universes: Data Protection Considerations in the EU Merger Control
## Can Merger Remedies Be a Way Out?

Master Thesis


**Emine Bilsin**

ANR: 662286

Tilburg Law School
Tilburg Institute for Law, Technology and Society
LL.M. Law and Technology

Supervisor: Dr. Thomas Tombal
Second Reader: Dr. Inge Graef


June 2022

## ACKNOWLEDGEMENTS

*I would like to thank my supervisor, Dr. Inge Graef, for her guidance and feedback which were influential in shaping my thesis. Her way of teaching and expertise truly inspired my academic journey at Tilburg.*

*I am extremely grateful to my supervisor, Dr. Thomas Tombal for his continuous assistance, counselling, and invaluable insights and comments. It is his excellent communication and kind help that have made my thesis writing process went through smoothly.*

*I would like to express my sincere gratitude to Jean Monnet Scholarship Program and the European Commission for funding my study at Tilburg University. I am truly grateful to have been awarded such a prestigious and generous scholarship.*

*My special appreciation goes out to my life partner, Ertugrul, a great lawyer and husband, for his unfailing support, encouragement, travelling back and forth between the two countries, and especially fruitful academic discussions.*

*My loving mother, my father, my siblings, Ayse, Vakkas, Elif, Busra, thank you for always being there for me.*

# Table of Contents

# 1 INTRODUCTION

## 1.1 Background and Problem Statement

The rapid advancement of technology has led companies to attach more and more value to data and has shaped individuals' behaviours accordingly. People are increasingly spending more time online, and data that they share has now become a tool for transforming the technology companies' strategies. With the rise of Web 2.0, the current technologies ease the way for companies to collect, store, process, and merge personal data at a fast pace, in great volumes and wide range, which in turn could bring tremendous value for those companies owing to their controversial, top-secret algorithms. One might refer to arguably positive outcomes of such a data-driven ecosystem for consumer welfare (*e.g.* assisting consumers to more efficiently spend their time through personalised and to-the-point services or enhancing their choices of and accessibility to a variety of products/services as well as the improved innovation and product/service quality).[1] That being said, the negative effects of the aggregated personal data that are enlarged in consequence of the ever-increasing acquisition trends, particularly on the users' data protection and privacy rights, should not be ignored.[2] Accordingly, the accurate legislation tools to address those issues and proper ways to balance the costs of both intervention and non-intervention are still questionable.

In that regard, following the growing awareness and significance of data protection and privacy in today's data-driven economy, the rights and obligations stipulated in the data protection legislation have gained prominence. The collection and use of the enormous amount of data have been considered a data protection law issue.[3] Upon the enactment of the General Data Protection Regulation ("GDPR") in 2018, personal data has been granted a high standard level of protection throughout the European Union ("EU").[4] Nevertheless, excessive collection and use of data in the digital markets have also attracted the scrutiny of competition authorities in their analyses.[5] The proliferation of technology and the use of the internet brought numerous users to digital companies who build their business models depending heavily on the collection and use of individuals' data. This has made the boundaries of data protection and competition law closely intertwined. On the one hand, data-related practices may give rise to significant competition issues regarding the

[1] Competition & Markets Authority (hereinafter "CMA"), 'The Commercial Use of Consumer Data, Report on the CMA's Call for Information' (2015) 50-61.
[2] Anca D. Chirita, 'The Rise of Big Data and the Loss of Privacy' M. Bakhoum et al. (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer 2018) 153. See also European Data Protection Board, 'Statement of the EDPB on the data protection impacts of economic concentration' (27 August 2018) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_en.pdf> accessed 19 June 2022.
[3] Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' Joint Report, 10 May 2016, 3.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (hereinafter "the GDPR").
[5] Autorité de la Concurrence and Bundeskartellamt (n 3) 11.

functioning of digital markets and undermine the competitive process.[6] On the other hand, the growing use of data by technology companies might create detriments for the users' rights to data protection and privacy.[7] This is more evident, particularly in high-profile data-driven mergers through which a merging entity could access large user data sets[8] and gain considerable market power vis-à-vis its end-users and competitors.[9] User data play a central role in big technology takeovers, and increased data concentration through mergers is becoming more widespread, so is the need for legal protection of the individuals' data privacy rights. This triggers the debate regarding whether the traditional merger analysis should include data protection and privacy-related considerations to ensure an accurate competition analysis from the user side.[10] In this regard, the relevance of "data protection" and "privacy"[11] in merger reviews has been discussed in two instances.

The first instance refers to integrating data protection and privacy as a relevant factor for the substantive competition analysis.[12] Competition law focuses on the consumer welfare standard, which is determined according to price, quality, choice, and innovation.[13] In multi-sided markets, users often benefit from online services for "free" in return for their data, and companies monetize this data through, for instance, targeted advertising.[14] Given that data takes the place of price in digital markets, privacy conditions offered for a service might take priority over price as a competition parameter. In this regard, data privacy conditions could be a matter of quality (or

[6] Inge Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' in Martin Moore and Damian Tambini (eds), *Digital Dominance, The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 71-72; Damien Geradin and Monika Kuschewsky, 'Competition Law and Personal Data, Preliminary Thoughts on a Complex Issue' (2013) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088 > accessed 19 June 2022.

[7] Katharina Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16 European Competition Journal 628.

[8] Inge Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 World Competition: Law and Economics Review 473, 491-492.

[9] Organisation for Economic Cooperation and Development (hereinafter "OECD"), 'Big Data: Bringing Competition Policy to the Digital Era' 27 October 2016 (DAF/COMP(2016)14) 5.

[10] Viktoria HSE Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in an Era of Big Data' (2020) 57 Common Market Law Review 161; Francisco Costa-Cabral and Orla Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' (2017) 54 Common Market Law Review 11; Beatriz Kira, Vikram Sinha, Sharmadha Srinivasan, 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (2021) 00 Industrial and Corporate Change 1.

[11] Although the terms 'data protection' and 'privacy' may often be used interchangeably, it must be noted that they are different in context and not synonyms within the EU legal framework. See Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.

[12] Lynskey and Costa-Cabral call this an "internal constraint" that data protection law exercises on competition law: Francisco Costa-Cabral and Orla Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (2015) 25 LSE Working Papers. This will be examined in depth in Section 3.2.

[13] Commission Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/7, para 5 (hereinafter "the Guidance Paper").

[14] Ariel Ezrachi and Maurice E. Stucke, *Virtual Competition the Promise and Perils of Algorithm-Driven Economy* (Harvard University Press 2016) 30.

choice) of a product/service on which businesses may compete,[15] as also acknowledged by the European Commission ("Commission") in several merger decisions.[16]

Standalone privacy concerns that are not part of substantive competition analysis constitute the second instance. As the big technology companies increasingly collect data about the habit, behaviour, and opinion of a vast number of people, concerns about the loss of privacy have become prevalent. Some policymakers are vocal that the data protection and privacy concerns *as such* should be considered by competition authorities in their merger analysis.[17] Yet, the Commission and the Court of Justice of the European Union ("Court") have refused to integrate pure data protection and privacy concerns as a discrete consideration into competition analysis.[18]

All in all, if one takes a price-based approach, data protection and privacy concerns would be overlooked in reviewing a data-driven merger, which may have detrimental effects on consumers.[19] Indeed, many of the high-profile data-driven mergers involving the combination of a large scale of personal user data were unconditionally approved by the Commission despite their potential harm to competition in the markets and long-term harm to consumers' privacy.[20] There is a clear need for a more vigilant competition approach and cooperation between the competition and data protection authorities, given the growing -often blurred-[21] intersection between the two fields. This is even more relevant in the context of merger analysis under the European Union

[15] Orla Lynskey, 'Considering Data Protection in Merger Control Proceedings' (2018) (OECD Non-Price Effects of Mergers DAF/COMP/WD(2018)70) 4; OECD 'Quality Considerations in Digital Zero-Price Markets' 9 October 2018 (DAF/COMP(2018)14) 7-8; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 Antitrust Law Journal 121, 133.

[16] *Facebook/WhatsApp* (Case COMP/M.7217) Commission Decision [2014]; *Microsoft/LinkedIn* (Case COMP/M.8124) Commission Decision [2016] OJ C388; *Google/Fitbit* (Case COMP/M.9660) Commission Decision [2020] OJ C194.

[17] European Data Protection Supervisory (hereinafter "EDPS"), 'Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014) 26. For a comment on the Opinion, see Francisco Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (2016) 23 Maastricht Journal of European and Comparative Law 495. European Data Protection Supervisory, 'Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (2016). This will be further examined in Section 3.3.

[18] Case C-238/05 *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios* [2006] ECR I-11125 para. 63; *Google/DoubleClick* (Case COMP/M.4731) Commission Decision [2008] OJ C184/9 para. 368; *Facebook/WhatsApp* (n 16) para. 164; Commission, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (6 December 2016) IP/16/4284 <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284> accessed 19 June 2022; *Google/Fitbit* (n 16) para. 452, footnotes 299-300.

[19] OECD, 'Big Data: Bringing Competition Policy to the Digital Era' (n 9) 17.

[20] Anca D Chirita, 'Data-Driven Mergers under EU Competition Law' in J Linarelli & O Akseli (eds) *In the Future of Commercial Law: Ways Forward for Harmonisation* (1st ed, Hart Publishing 2019).

[21] Inge Graef, 'Blurring Boundaries of Consumer Welfare- How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' in M. Bakhoum, B. Conde Gallego, M-O. Mackenrodt, & G. Surblytė-Namavičienė (eds), *Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach* (MPI Studies on Intellectual Property and Competition Law 2018).

Merger Regulation ("EUMR")[22] where forward-looking rules and ex-ante merger remedies of competition law may be useful to address possible data protection and privacy-related concerns before their adverse effects occur.[23]

## 1.2 Research Question and Sub-questions

Against this background, this research seeks to answer the question: *To what extent should competition authorities integrate data protection and privacy-related considerations into their merger assessments under the EU Competition Law, and how should merger remedies be designed to promote such integration?* The main question will be answered through the following sub-questions:

- *How do data protection and privacy considerations fit in current merger assessments?*
- *What are the arguments advanced to call for the inclusion of data protection and privacy considerations in merger assessments, and what are the possible implications and challenges of such inclusion?*
- *How should merger remedies be designed to promote the integration of data protection and privacy considerations into merger assessments?*

## 1.3 Literature Review

The last few years have witnessed the emergence of several policy reports, including the analysis of the interplay between data protection and competition law in the digital economy.[24] Concerning the first instance mentioned above, there is a growing call in the literature for integrating data protection considerations into substantive competition analysis[25] as data-driven mergers have

[22] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) [2004] OJ L 24/1 (hereinafter "the EUMR").

[23] Graef, 'Blurring Boundaries of Consumer Welfare- How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 141.

[24] Jacques Crémer, Yves-Alexandre de Montjoye, and Heike Schweitzer, *Competition Policy for the Digital Era* (Final Report, European Commission 2019); Jason Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (March 2019); OECD, 'Consumer Data Rights and Competition' 29 April 2020 (DAF/COMP(2020)1); Autorité de la Concurrence and Bundeskartellamt (n 3); EDPS 2014 (n 17); EDPS 2016 (n 17).

[25] Wolfgang Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 639 Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil; Maurice E. Stucke and Allen P. Grunes, *Big Data and Competition Policy* (Oxford University Press 2016); Ariel Ezrachi and Viktoria HSE Robertson, 'Competition, Market Power and Third-Party Tracking' (2019) 11 Oxford Legal Studies Research Paper; Autorité de la Concurrence and Bundeskartellamt (n 3); Graef, 'Blurring Boundaries of Consumer Welfare- How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21); Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12); Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10). On the other side of the Atlantic, it is suggested to define a privacy-based relevant product market to integrate privacy analysis into competition law, see Pamela Harbour and Tara Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (2010) 76 Antitrust Law Journal 769.

become more prevalent.[26] It is seemingly much more agreed that data privacy can be relevant to merger analysis as a non-price parameter of competition, particularly when the product/services are offered for free in exchange of users' data.[27] Indeed, the Commission in *Facebook/WhatsApp* has acknowledged that privacy could be a competition parameter as it is "becoming increasingly valued" by users.[28] The challenge here lies in establishing privacy competition and measuring a privacy degradation that could potentially lead to anti-competitive effects as neither of these decisions entails a comprehensive examination of privacy as a competition parameter.[29] There is still room for development in the Commission's analysis vis-à-vis nascent data and privacy-related theories of competition harm.[30] In *Microsoft/LinkedIn*, the Commission proceeded from a premise that data protection rules can act as a limit that would prevent the merged entity from engaging in anticompetitive conduct.[31] Yet, in *Google/Fitbit*, it progressively implied that such imposition of data protection rules on the merged entity did not mean that there was no competition risk for data combination.[32]

Regarding the second instance, the proponents of such integration argue that competition authorities should factor "pure" data privacy harms into their merger reviews and block or

[26] For a comprehensive analysis of the Commission's data-driven merger cases, see Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) and Massimiliano Kadar and Mateusz Bogdan, 'Big Data' and EU Merger Control – A Case Review' (2017) 8(8) Journal of European Competition Law & Practice 479.

[27] Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 4; EPDS 2016 (n 17) 13; Elias Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (2018) 13 EUI Working Papers; Maria C. Wasastjerna, 'The Implications of Big Data and Privacy on Competition Analysis in Merger Control and The Controversial Competition-Data Protection Interface' (2019) 30(3) European Business Law Review 337; Samson Esayas, 'Data Privacy in European Merger Control: Critical Analysis of Commission Decisions Regarding Privacy as a Non-Price Competition' (2019) 40(4) European Competition Law Review 166. See for the Commission's decisions: *Facebook/WhatsApp* (n 16); *Microsoft/LinkedIn* (n 16); *Google/Fitbit* (n 16). For the US view see Ohlhausen and Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (n 15) 133; Allen Grunes and Maurice Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (2015) (April) the Antitrust Source American Bar Association, 4. For a critique of this concept, see Geoffrey A Manne and R Ben Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (2015) 2 CPI Antitrust Chronicle, 3-5.

[28] *Facebook/WhatsApp* (n 16) para 87.

[29] Stucke and Grunes, *Big Data and Competition Policy* (n 25) 117; Costa-Cabral and Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' (n 10) 37-38; Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15); Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 19; for the US view: Darren Tucker, 'The Proper Role of Privacy in Merger Review' (2015) 2 CPI Antitrust Chronicle.

[30] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27); Graef, 'When Data Evolves Into Market Power-Data Concentration and Data Abuse under Competition Law' (n 6) 84-85; Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) 42; Stucke and Grunes, *Big Data and Competition Policy* (n 25) 103. For a more detailed analysis of this point, see Section 3.2.2.

[31] *Microsoft/LinkedIn* (n 16) para. 255. Inge Graef, Damian Clifford, and Peggy Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (2018) 8(3) International Data Privacy Law 200, 215.

[32] *Google/Fitbit* (n 16) para. 412. For a more detailed analysis of this point, see Section 3.2.3.

condition mergers that impair users' data protection and privacy rights.[33] Conversely, many scholars refuse competition intervention in pure data protection and privacy concerns because protecting privacy interests is not the objective of merger control, and data protection rules already apply to merged entities.[34]

Some commentators have suggested using competition remedies to tackle new forms of privacy-related consumer exploitation by big digital conglomerates and promote privacy interest in the abuse of dominance and merger review cases.[35] The *Google/Fitbit* decision may be a source of inspiration for further inclusion and promotion of privacy interests in competition assessments through novel merger remedies: such as data silo remedy according to which Google will store Fitbit users' health data separately from any other Google data used for advertising.[36]

A considerable amount of data-driven merger decisions has been piling up over the last decade. Albeit demonstrating some improvements, the Commission's decisions have yet to provide a satisfying approach vis-à-vis potential privacy-related consumer harms stemming from data-centric mergers. There is a gap in the competition enforcement regarding how authorities should address such concerns. Thus, a growing commentary on the interplay between data protection and competition law in the merger control context has emerged. There is little said on the potential use of merger remedies to safeguard data protection and privacy interests that a data-driven merger may otherwise impair. What remains unexplored, however, is a comprehensive study on the possible illustrations of such remedies (*i.e.* how these remedies can be designed). This Thesis aims to contribute to the current debate on the scope of integrating data protection and privacy

[33] EDPS 2014 (n 17); Costa-Cabral and Lynskey, 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12); C. Kuner, F.H. Cate, C. Millard, D.J.B. Svantesson and O. Lynskey 'When Two Worlds Collide: the Interface between Competition Law and Data Protection' (2014) 4 International Data Privacy Law 247; Orla Lynskey, 'At the Crossroads of Data Protection and Competition law: Time to Take Stock' (2018) 8(3) International Data Privacy Law 179; Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20).

[34] Paul Gilbert and Richard Pepper, 'Privacy Considerations In European Merger Control: A Square Peg For A Round Hole' (2015) 5 CPI Antitrust Chronicle, 4; Justus Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision' (2019) CPI Antitrust Chronicle; Guiseppe Colangelo and Mariateresa Maggiolino 'Data Protection in Attention Markets: Protecting Privacy Through Competition?' (2017) 8(6) Journal of European Competition Law & Practice 363; Richard Craig, 'Big Data and Competition – Merger Control Is Not the Only Remedy for Data Protection Issues' (2014) Lexology <https://www.lexology.com/library/detail.aspx?g=0bd8c8f7-2869-4ed8-8606-a11559cbdf41> accessed 19 June 2022. For the US view, see Daniel Sokol and Roisin Comerford, 'Antitrust and Regulating Big Data' (2016) 23 George Mason Law Review 1129, 1156-1158; Ohlhausen and Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (n 15); Manne and Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (n 27). This will be further discussed in Section 3.3.1.

[35] Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer Law International 2016); Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21); Marco Botta and Klaus Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (2019) 10(8) Journal of European Competition Law & Practice 465; EDPS 2014 (n 17) 32. This will be examined in depth in Section 4.3.

[36] *Google/Fitbit* (n 16), see also European Commission - Press release, 'Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions' (IP/20/2484, 17 Dec 2020). <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484> accessed 19 June 2022.

considerations into merger analysis from a novel angle, namely merger remedies, by providing examples of remedies that could be used to address data protection and privacy considerations stemming from a data-driven merger in light of the recent *Google/Fitbit* decision.

### 1.4 Methodology and Structure

A doctrinal research methodology was conducted throughout the research which contributed to the analysis of the legal framework and the Commission's decision-making practice. Academic literature on competition and data protection was reviewed to understand the intersection between data protection and privacy in merger reviews. The main research question was answered through the sub-questions, which were addressed in three main chapters, respectively. The research methods explained above were conducted in three chapters based on various sources. Primary sources include relevant regulations and statutory provisions of the EU, decisions of the Commission and national competition authorities, and judgments of the Court of Justice of the European Union. Secondary sources include reports and guidelines of the EU institutions and national authorities.

The second Chapter will analyse how the Commission's decision-making approaches data protection and privacy considerations in merger review. Prime examples of data-driven mergers will be presented. The third Chapter will concern the arguments for integrating data protection and privacy considerations into merger assessment. It will discuss the possible implications and challenges of such integration. The assessment will include the Commission's decisions, case-law, scholars' perspectives, and opinions of authoritative policymakers. The fourth Chapter will develop a three-fold proposal for designing merger remedies to address data protection and privacy-related consumer harm and promote data privacy interests. The EU merger regulation framework, academic works, and relevant merger cases will be examined.

# 2 HOW DO DATA PROTECTION AND PRIVACY FIT IN CURRENT MERGER ASSESSMENTS?

## 2.1 Introduction

In light of the Commission's decisions, this Chapter aims to answer: *How do data protection and privacy considerations fit in current merger assessments?* Following a brief introduction on the intersection between data protection and competition law, the Chapter will scrutinize certain high-profile mergers involving major tech companies.

## 2.2 Setting the Scene: How Do Data Protection and Competition Law Intersect?

Data, including personal data,[37] place itself in the centre of global digital economies and, for some, replace "oil" as the new driver of economic prosperity.[38] Privacy today goes well beyond the "right to be let alone",[39] and it has gained a commercial character: it is even labelled as an asset traded in digital markets.[40] From the competition law perspective, the accumulation of personal data that is of large amount and high quality is considered a key competitive differentiator in the digital economy.[41]

The relationship between competition law and personal data is characterized by manifoldness and complexity.[42] Data protection rules can be relevant to competition law in several instances as they

[37] Article 4(1) of the GDPR defines personal data as "any information relating to an identified or identifiable natural person" and explains that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". As is seen from the definition, a broad notion of personal data is preferred 'so as to include all information which may be linked to an individual' see Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' WP 136 01248/07/EN, 4 . For instance, Article 29 Working Party considers IP addresses and cookies as personal data relating to an identifiable person, see *Ibid* 16-17 and Article 29 Data Protection Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' WP 148 00737/EN, 8-9.

[38] Meglena Kuneva, 'Keynote Speech: Roundtable on Online Data collection, Targeting and Profiling' (Brussels, 31 March 2009 SPEECH/09/156); Kiran Bhageshpur, 'Data is the New Oil – And That's a Good Thing' (Forbes 15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=29d894307304> accessed 19 June 2022.

[39] As defined by Warren and Brandeis in their seminal article: Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193.

[40] Ohlhaussen and Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (n 15) 38. It has been reportedly claimed by Facebook (now Meta) CEO Mark Zuckerberg that "privacy is no longer a social norm" see Bobbie Johnson, 'Privacy No Longer a Social Norm, Says Facebook Founder' (The Guardian 10 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy > accessed 19 June 2022.

[41] Geradin and Kuschewsky, 'Competition Law and Personal Data, Preliminary Thoughts on a Complex Issue' (n 6) 2.

[42] *Ibid* 15.

function in the same "regulatory continuum with a large area of overlap".[43] In light of the growing acquisition trend in digital industries, their boundaries have become intensely tangled in the context of merger control.[44] Indeed, the number of M&A transactions by the major technology companies has risen significantly over the last decade.[45] This number is expected to increase considering the calls for reform in the merger notification threshold to better catch tech mergers that could not normally be caught by the relevant notification threshold.[46]

Competition and data protection law can be distinguished in their scope, enforcement capabilities, and methods, nevertheless, they share certain common features.[47] The EU data protection legislation aims at protecting individuals: "in particular their right to the protection of personal data".[48] Notwithstanding the judicial and scholarly debate[49], the EU Commission preferred consumer welfare standard as an enforcement priority in competition assessment, which is determined not only according to price but also to quality, choice or innovation.[50] The latter set of parameters is also a relevant factor for the protection afforded by the data protection legislation. Indeed, stimulating privacy-friendly services and greater consumer control over their data, as aimed by data protection law, may also be promoted through competition rules in the form of increased privacy quality, better innovation and wider consumer choice in relation to privacy.

[43] Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10) 3.

[44] For a comprehensive analysis of the Commission's data-driven merger cases, see Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) and Kadar and Bogdan, 'Big Data' and EU Merger Control – A Case Review' (n 26).

[45] Geoffrey Parker, Georgios Petropoulos and Marshall Van Alstyne, 'Platform Mergers and Antitrust' (2021) 30(5) Industrial and Corporate Change 1307, 1311-1316. The authors point out that from 1988 to 2020, Google, Amazon, Facebook, Apple and Microsoft have made 855 M&A transactions in total. Moreover, Furman et al indicates that in the last 10 years five largest companies made over 400 acquisitions globally, see Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 12.

[46] Marc Bourreau and Alexandre de Streel, 'Big Tech Acquisitions, Competition & Innovation Effects and EU Merger Control' (2020) CERRE Issue Paper 15; OECD, *Start-ups, Killer Acquisitions and Merger Control* (2020) 43-46.

[47] For an analysis of competition and data protection legislation framework see EDPS 2014 (n 17) 11-22.

[48] The GDPR Article 1; Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 37) 4.

[49] Although it had been defined as one of the goals of the competition law, consumer welfare had not been prioritized by the Court vis-à-vis other goals of competition law such as the interest of competitors and structure of the market: see Case C-501/06 *GlaxoSmithKline Services Ltd v Commission* [2009] ECR I-09291 para. 63; Case C-8/08 *T-Mobile Netherlands and Others* [2009] ECR I-04529 paras. 31, 36, 38-39; see further Pinar Akman, ''Consumer Welfare' and Article 82EC: Practice and Rhetoric' (2008) 08-25 CCP Working Paper; A. Jorge Padilla and Christian Ahlborn, 'From Fairness to Welfare: Implications for the Assessment of Unilateral Conduct under EC Competition Law' in C. D. Ehlermann and M. Marquis (eds), *A Reformed Approach to Article 82 EC* (Oxford, Hart, 2008) 102. Yet, the consumer welfare goal has gradually emerged as the underlying objective of competition law in the Court's recent case-law, see, for instance, Case C-209/10 *Post Danmark A/S v Konkurrencerådet* [2012] ECR I-0000; Case T-286/09 *Intel Corp v Commission* [2014] 5 CMLR 9. For a good overview on the evolution of the Court's approach in this regard, see Anne C. Witt, 'The European Court of Justice and the More Economic Approach to EU Competition Law – Is the Tide Turning?' (2019) 64(2) Antitrust Bulletin 172.

[50] The Guidance Paper (n 13) para. 5, Ariel Ezrachi 'The Goals of EU Competition Law and the Digital Economy' (2018) BEUC Discussion Paper 4 <https://www.beuc.eu/publications/beuc-x-2018-071_goals_of_eu_competition_law_and_digital_economy.pdf> accessed 19 June 2022. According to the author, amongst other goals, the EU competition law centrally aims at consumer welfare goal.

Furthermore, competition and data protection law pursue a common objective: promoting European market integration.[51] Accordingly, they converged at the level of their goals: promoting consumer welfare and market integration,[52] although their means to achieve those vary.[53]

Albeit shielded by the EU data protection rules, intense personal data activities and data concentration resulting from big tech acquisitions may have far-reaching impacts on the consumers welfare in so much that it requires intervention by other regulators, particularly competition authorities.[54] Besides involving privacy-intrusive activities, these data-centric mergers may give the merged entity a competitive advantage that cannot be matched by its competitors or eliminate potential competition over privacy, a competition parameter in the market,[55] and thus warrant the Commission's scrutiny.

## 2.3 The Current State of Play

### 2.3.1 Early Decisions of the Court and the Commission

The Court for the first time assessed the relationship between competition and data protection in a preliminary ruling concerning agreements on the establishment of a register for the exchange of customer solvency information between competing financial institutions.[56] In *Asnef-Equifax*, the Court ruled that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection".[57] That said, it cannot be inferred from the decision that the Court completely excluded data protection from the sphere of competition law.[58] In fact, concerning the expression "as such" it can be asserted that the Court has left the room open for considering data protection and privacy to the extent that they are relevant to substantive competition analysis.[59] The Commission seemed to follow the Court's stance in *Asnef-Equifax* in its merger decisions from 2008 and onwards, namely, refusing to consider pure data protection and privacy considerations

[51] For competition law, see Ezrachi 'The Goals of EU Competition Law and the Digital Economy' (n 50) 16-17; the Guidance Paper (n 13) paras. 1, 6, 7; the EUMR Recitals 2-6. For data protection law, see the GDPR Recitals 7 and 13; Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The EU General Data Protection Regulation: A New Global Standard for Information Privacy' 6-7 <https://bartvandersloot.com/onewebmedia/SSRN-id3162987.pdf> accessed 19 June 2022.
[52] EDPS 2014 (n 17) 11; Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 21-22.
[53] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 131.
[54] Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25).
[55] Eleanora Ocello, Cristina Sjödin, Anatoly Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (2015) 1 Competition Merger Brief, 5.
[56] *Asnef-Equifax* (n 18).
[57] *Ibid* para. 63.
[58] Marco Botta and Klaus Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) 64(3) Antitrust Bulletin 428, 436.
[59] Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 334.

as a standalone issue in competition analysis while examining such considerations so far as they constitute a part of substantive competition analysis.[60]

For its part, the Commission reviewed the *Google/DoubleClick* merger involving the combination of two large complementary datasets, including personal data. The Commission considered that the combination of search data (by Google) and users' web surfing behaviour (by DoubleClick) would not give a competitive advantage to the merged entity because these data were already available to Google's competitors.[61] As to the merger's likely effect on users' privacy, the Commission deferred any privacy concerns to the sphere of data protection law.[62] [63]

### 2.3.2 The Facebook/WhatsApp Merger

The *Facebook/WhatsApp* merger case resulted with a highly contested decision in 2014. Despite the magnitude of the transaction, as it involved the combination of the significant amount of user data held by the world-famous digital platforms and novel issues in the context of mergers in the technology sector,[64] the merger was unconditionally approved without opening an in-depth investigation by a relatively short -36 page-long- decision.

The decision constituted an important step in the Commission's analysis of privacy considerations, particularly as it articulated privacy as a non-price parameter of competition. Regarding the horizontal overlap in the market for consumer communication services, the Commission noted that consumer communication apps compete based on their functionalities, which also include privacy

[60] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 144.

[61] *Google/DoubleClick* (n 18) para. 359-366. One of the challenging aspects of the assessment of horizontal theories of harm resulting from data combination was that in *Google/DoubleClick* and in the subsequent merger cases mentioned below (Sections 2.3.2, 2.3.3, 2.3.4), the merging parties did not sell their data to third parties as a commercial product (as was the case in *TomTom/Tele Atlas* (Case COMP/M.4854) Commission Decision [2008] OJ C237/8 and *Thomson Corporation/Reuters Group* (Case COMP/M.4726) Commission Decision [2008] OJ C212/5). The data they hold was rather used as an input in providing services.

[62] *Google/DoubleClick* (n 18) para. 368: "irrespective of the approval of the merger, the new entity is obliged in its day to day business to respect the fundamental rights recognised by all relevant instruments to its users, namely but not limited to privacy and data protection".

[63] From *Google/DoubleClick* in 2008 and until *Facebook/WhatsApp* in 2014, the Commission analysed a number of data-driven mergers, including *TomTom/Tele Atlas* (n 61); *Thomson/Reuters* (n 61); *Microsoft/Yahoo! Search Business* (Case COMP/M.5727) Commission Decision [2010] OJ L24/1; *Microsoft/Skype* (Case COMP/M.6281) Commission Decision [2011] OJ C341/02; *Telefónica UK/Vodafone UK/Everything Everywhere/JV* (Case COMP/M.6314) Commission Decision [2012]; *IMS Health/Cegedim Business* (Case COMP/M.7337) Commission Decision [2014]; *Publicis/Omnicom* (Case COMP/M.7023) Commission Decision [2014] OJ C84/1. See Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) and Kadar and Bogdan, 'Big Data' and EU Merger Control – A Case Review' (n 26).

[64] These novel issues in particular related to market for consumer communications apps can be exemplified as the market definition, relevance of market shares, network effects, and importance of user data in the competition assessment, see Ocello, Sjödin, and Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (n 55) 1.

and security, as they are "becoming increasingly valued" by users.[65] When assessing the closeness of competition in the market for consumer communication services, the Commission pointed out the different levels of privacy protection offered by Facebook and WhatsApp: "contrary to WhatsApp, Facebook Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities".[66] Yet, the Commission did not consider whether they compete based on their different level of privacy policies, rather, it noted that the two apps were, to some extent, complementary due to significant overlap between their networks and substantial degree of multi-homing by users.[67] Thus, it was concluded that Facebook and WhatsApp were not close competitors in the consumer communication services market.[68] The ambiguity in the Commission's assessment regarding the lack of privacy competition was exacerbated by the statement that after the announcement of WhatsApp's acquisition by Facebook, many users switched to different messaging platforms due to privacy concerns, particularly Telegram, which offers a higher level of privacy protection.[69] Moreover, as Stucke and Grunes rightly indicate, although many WhatsApp users were already using Facebook's social network platform and could have easily used integrated Facebook Messenger, they "opted for a texting app that afforded them significantly greater privacy protection than Facebook Messenger".[70] Hence, despite the findings implying the existence of privacy competition in the consumer communication market, the Commission did not analyse the merger's effect on such competition, that is to say, whether the merger could stifle competition on privacy by removing a competitive constraint exerted by WhatsApp on Facebook's privacy conditions, and by allowing Facebook to deteriorate post-merger the level of privacy protection offered by WhatsApp.

A possible data-related theory of harm examined was that post-merger, the merged entity could start to collect data from WhatsApp users who are also Facebook users to improve targeted advertising on Facebook's social network in a way that competitors fail to respond. Regarding such concern, the Commission was convinced by Facebook's statement that there were major

[65] *Facebook/WhatsApp* (n 16) paras. 86-87.
[66] *Facebook/WhatsApp* (n 16) para. 102.
[67] Multi-homing means that users install and use more than one consumer communications app simultaneously, see *Facebook/WhatsApp* (n 16) paras. 104-105.
[68] Interestingly, the existence of different privacy policies was one of the Commission's reasons in deciding that they were not competitors, see *Facebook/WhatsApp* (n 16) paras. 102 and 107 and Stucke and Grunes, *Big Data and Competition Policy* (n 25) 131. Stucke and Grunes argue that this may stem from the Commission's reliance on traditional competition theory that "dissimilar products compete less fiercely". Yet, they contend that it may be that the firms compete with each other by differentiating themselves from their rivals. See *Ibid* 129-134.
[69] *Facebook/WhatsApp* (n 16) footnote 79. There are other statements in the decision indicating a competition on the level of privacy protection offered in the relevant markets: "the need to retract WhatsApp's current plan to introduce […] may reduce Facebook's incentive to introduce ads on WhatsApp, since abandoning end-to-end encryption could create dissatisfaction among the increasing number of users who significantly value privacy and security"; "privacy concerns also seem to have prompted a high number of German users to switch from WhatsApp to Threema in the 24 hours following the announcement of Facebook's acquisition of WhatsApp." at para. 174.
[70] Stucke and Grunes, *Big Data and Competition Policy* (n 25) 132.

technical obstacles to integrating the users' Facebook and WhatsApp profiles.[71] The Commission further noted that even if the merged entity were to start using WhatsApp user data, this would not strengthen Facebook's position in the market for online advertising as post-merger, there would remain a sufficient number of alternative providers of online advertising services and a large amount of Internet user data valuable for advertising purposes that were not within Facebook's exclusive control.[72]

Regarding the standalone privacy concerns, the Commission reaffirmed its approach, and held that "any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules".[73]

### 2.3.3 The Microsoft/LinkedIn Merger

In 2016, the Commission approved the acquisition of LinkedIn by Microsoft, involving the combination of datasets of the two significant tech companies controlling large-scale user data, subject to remedies.

The Commission made clear that privacy can be taken into account in merger assessment to the extent that "a significant number of" consumers see it as an important parameter, while maintaining its stance that privacy concerns as such fall outside the scope of merger review.[74] The Commission stated that privacy was an important competition parameter and driver of consumer choice in the market for professional social network (PSN) services.[75] For instance, Xing, a competing PSN, was considered to offer a higher degree of privacy protection to its users than LinkedIn. Should Microsoft's possible foreclosing strategy conduce to the marginalization of Xing, consumer choice as to the level of privacy protection will be restricted.[76]

As to the competition concerns in online advertising stemming from the combination of merging parties' data, essentially consisting of personal data, the Commission found that the merger did

[71] *Facebook/WhatsApp* (n 16) para. 185. This statement has led to a fine of 110 million Euro imposed on Facebook for providing incorrect or misleading information during the merger investigation, as it turned out that it was technically possible to automatically match Facebook and WhatsApp user identities at the time of the merger. That said, this finding did not affect the outcome of the decision authorizing the *Facebook/WhatsApp* merger because of the 'even if' assessment made in para. 187-189: Commission, 'Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover' (18 May 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369> accessed 19 June 2022.
[72] *Facebook/WhatsApp* (n 16) para. 187-189.
[73] *Facebook/WhatsApp* (n 16) para. 164.
[74] Eleanora Ocello and Cristina Sjödin, 'Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets' (2017) 1 Competition Merger Brief, 5. See also Commission, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (n 18).
[75] *Microsoft/LinkedIn* (n 16) para. 350, footnote 330.
[76] *Microsoft/LinkedIn* (n 16) para. 438; Ocello and Sjödin, 'Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets' (n 74) 5.

not give rise to any concern based on two statements. First, the Commission referred to relevant national data protection laws and (then) future GDPR rules limiting Microsoft's ability to access and process user data within the combined datasets.[77] Hence, data protection rules were integrated into the Commission's substantive competition analysis as a limit that could prevent competition concerns from arising.[78]

Secondly, the Commission noted two horizontal theories of harm under the assumption that the combination of datasets is allowed by the relevant data protection legislation: (i) post-merger, data combination may strengthen the merged entity's market power in a *hypothetical market for the supply of data* or increase barriers to entry/expansion for rivals; (ii) even if there is no intention or technical possibility to combine datasets, the merger may eliminate potential competition between the parties based on the data they controlled.[79] Reference to the hypothetical market for data is considered an evolution in the Commission's approach because defining a market for data would allow the Commission to draw a more accurate picture of the impact of data combination-related competition concerns.[80] Yet, these concerns were dismissed since, first, merging parties' data are not made available to third parties as a product for advertising purposes; second, there will continue to be a large amount of user data valuable for advertising, which is not within Microsoft's exclusive control; and third, the parties are small market players in online advertising.[81]

### 2.3.4 The Google/Fitbit Merger

In 2020, the Commission cleared the acquisition of Fitbit, producer of wearable devices, by Google, major digital conglomerate, subject to long-lasting behavioural commitments. At the time of the merger, both parties held control over valuable data on users' online behaviour and health conditions.

---

[77] Thus, Microsoft committed to preserving effective choice in the market for PSN services. *Microsoft/LinkedIn* (n 16) para. 176-178. In addition to these horizontal non-coordinated effects in the market for online advertising, the Commission also referred to applicable data protection rules as a limit on the merged entity's ability to process their combined datasets in the context of possible non-coordinated vertical effects related to (i) the ability to foreclose competing providers of customer relationship management software solutions by refusing access to full LinkedIn data and (ii) the input foreclosure in the sense that Microsoft could restrict access to full LinkedIn data for the purposes of machine learning in competing productivity software solutions, see *Microsoft/LinkedIn* (n 16) para. 254-255 and 375, respectively. In these two instances, the Commission concluded that the transaction would not raise serious doubts as to its compatibility with the internal market.

[78] Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 215.

[79] *Microsoft/LinkedIn* (n 16) para. 179. This framework of assessment of the two data combination related theories of harm has been later followed by the Commission in the *Verizon/Yahoo* merger decision, see *Verizon/Yahoo* (Case COMP/M.8180) Commission Decision [2016].

[80] Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (n 8) 489-501; Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 77-78; Harbour and Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (n 25) 773. See also *infra* footnotes n 121, 173 and 174. It must be noted, though, that the Commission did not clarify its reasoning for defining a hypothetical market for data.

[81] *Microsoft/LinkedIn* (n 16) para. 180.

The Commission examined a data-related horizontal theory of harm, albeit "*not in a traditional sense*",[82] that post-merger, Google could exploit Fitbit users' data to increase its market power in the online advertising market. The Commission initially referred to the GDPR rules as regulatory limits that could prevent illegal data combination.[83] However, it was made clear that the fact that there were such limits and Google will have to comply with these rules did not remove data-related competition concerns: "these regulations do not eliminate the risks that the Parties' control on such data could render the expansion or entry by rival firms more difficult if not impossible".[84] As a result, the Commission found that combining the merging parties' dataset and data collection capabilities could give rise to anti-competitive effects by strengthening Google's dominant position in the supply of online search advertising markets.[85] This could be considered a step further from the Commission's approach in *Microsoft/LinkedIn*, where such regulatory limits were deemed sufficient to evaporate data-related competition concerns since the Commission in *Google/Fitbit* seemed not to be convinced with the ability of data protection legislation to prevent anti-competitive data combination.

Another progressive step in *Google/Fitbit* is that the Commission did not base its reasoning regarding the possible competition effects of data combination on its -highly questionable- premise[86] that datasets controlled by online platforms are substitutable in general.[87] Instead, the Commission concluded that the nature of data (*i.e.* health data) in the relevant case was of very high quality and valuable[88] and that there was no dataset comparable to those offered by Fitbit that Google's competitors could rely on since none of Fitbit's competitors made its data available for advertising.[89]

[82] Since both parties were not active in the same market *Google/Fitbit* (n 16) para. 399.
[83] *Google/Fitbit* (n 16) para. 403-410. In a similar vein, the Commission in the *Apple/Shazam* merger indicated that there were certain regulatory limits on the merged entity to prevent the unlawful data combination: *Apple/Shazam* (Case COMP/M.8788) Commission Decision [2018] OJ C106/16, recitals 225-235.
[84] *Google/Fitbit* (n 16) para. 412.
[85] *Google/Fitbit* (n 16) para. 427-468.
[86] *i.e.* large amount of user data valuable for advertising which are not within the merged entity's exclusive control will remain available to competitors. See, for instance, *Google/DoubleClick* (n 18), *Facebook/WhatsApp* (n 16), *Microsoft/LinkedIn* (n 16), *Verizon/Yahoo* (n 79).
[87] Graef argues that this premise could be due to the fact that the Commission did not define a market for data in the *Google/DoubleClick* and *Facebook/WhatsApp* cases: Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 75.
[88] *Google/Fitbit* (n 16) para. 430-433. For instance, the Commission refused certain market participants' request that the Ads Commitment should also include data other than health and fitness data, in particular payment and account data. In order to substantiate its reasoning, the Commission alluded to the importance of Fitbit's health and fitness data for Google's services compared to non-health data by stating that "data other than health and fitness data are already largely available to Google for millions of users thanks to the multiple activities carried out by the different Google services and entities. […] Moreover, it appears that rivals can also have access to these types of data, including from significantly larger user bases than Fitbit": see *Google/Fitbit* (n 16) para. 968.
[89] *Google/Fitbit* (n 16) para. 457.

The remedies provided make the *Google/Fitbit* decision particularly seminal for this Thesis. In response to the concern that data combination would increase Google's market power by strengthening its ability to exploit data for advertising purposes, the Commission accepted a data silo remedy according to which Google has to keep Fitbit health and fitness data separately and will not use them for advertising purposes for the duration of ten years.[90] The remedy requires a technical separation whereby Google has to implement a "data protection system" to ensure the separation of the accessed data.[91] As part of this commitment, Google will provide users with the choice to grant or deny the use of any health and fitness data stored in their Google or Fitbit Account by other Google services, like Google Search, Maps, Google Assistant or YouTube.[92] The competition-oriented data silo remedy carries "incidental" privacy benefits in the sense that it would also remedy (although it is not aimed at) data protection concerns arising from the use of personal data across the merged entity's businesses beyond the purpose for which it was initially collected.[93] Moreover, under the Web API Access Commitment, Google committed to maintaining access for API users to supported measured body data, subject to user consent and to compliance with the "Privacy and Security Requirements" including the GDPR's data protection principles.[94] These remedies will be further examined in Chapter 4.

Finally, echoing its previous approach, the Commission dismissed standalone privacy concerns raised by several stakeholders, who indicated that the merger would negatively affect users' ability to track how their health data is used and users would be harmed by reduced privacy.[95] It simply stated that these concerns were "not within the remit of merger control".[96]

---

[90] *Google/Fitbit* (n 16) p. 227, Commitments to the European Commission, Section A.1.1 - A.1.2. The period of ten years can be extended by up to another ten years by the Commission, if necessary.

[91] *Google/Fitbit* (n 16) p. 228, Commitments to the European Commission, Section A.1.3.d. The idea of mandating a firewall between the merging entities' databases has been previously put forward by Former US Federal Trade Commissioner Pamela Jones Harbour in her dissenting statement in the FTC's *Google/Doubleclick* decision, see Pamela Jones Harbour, 'Dissenting Statement of Commissioner Pamela Jones Harbour: In the Matter of Google/DoubleClick FTC 2007 No. 071-0170' (2007) <https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf> accessed 19 June 2022.

[92] *Google/Fitbit* (n 16) p. 229, Commitments to the European Commission, Section A.1.5.

[93] Erika Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (2021) 40 Temple University Legal Studies Research Paper, 143.

[94] *Google/Fitbit* (n 16) p. 229, 242-243, Commitments to the European Commission, Sections A.2 and F.

[95] Marc Bourreau et al, 'Google/Fitbit will monetise health data and harm consumers' (CEPR Policy Insight No 107 Submission to the European Commission September 2020) <https://cepr.org/sites/default/files/policy_insights/PolicyInsight107.pdf>; European Data Protection Board, 'Statement on Privacy Implications of Mergers, adopted on 19 February 2020' <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf> accessed 19 June 2022.

[96] *Google/Fitbit* (n 16) para. 452, footnotes 299-300; Commission, 'Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions' (17 December 2020) IP/20/2484 <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484> accessed 19 June 2022.

## 2.4 Interim Conclusion

Starting with the *Google/DoubleClick* decision, one can see the ever-increasing relevance of data and privacy in the substantive analysis of data-centric mergers. In the Commission's view, data protection and privacy could be a relevant factor in the merger analysis as a (i) non-price parameter of competition, and (ii) limit preventing competition concerns from arising. On the contrary, the Commission has refrained from incorporating pure data protection and privacy interests as a discrete consideration in competition analysis by echoing the Court's stance in *Asnef-Equifax*. Lastly, the remedies provided in *Google/Fitbit* seem to be inspiring for the possible inclusion of such interests.

# 3 THE INCLUSION OF DATA PROTECTION AND PRIVACY IN MERGER ASSESSMENTS

## 3.1 Introduction

This Chapter will scrutinize the instances where data protection and privacy could be included in merger assessment through the lens of the arguments and concepts developed in the literature and the Commission's decisions. Thus, the Chapter seeks to answer: *What are the arguments advanced to call for the inclusion of data protection and privacy considerations in merger assessments and what are the possible implications and challenges of such inclusion?*

## 3.2 Integrating Data Protection and Privacy as Part of Substantive Competition Analysis

The question of whether the risk of accumulation of personal data and loss of privacy should be considered in merger assessments has been the subject of long-lasting debate in the digital economy. Indeed, data concentration resulting from a merger constitutes one of the many other fields where competition and data protection law closely intersect,[97] and where competition enforcers face a "regulatory dilemma" in deciding under which legal field they should assess novel data and privacy-related concerns arising in digital markets.[98] The Autorité de la Concurrence and Bundeskartellamt point out this intersection and express that "the fact that some specific legal instruments serve to resolve sensitive issues on personal data does not entail that competition law is irrelevant to personal data".[99]

Thus far, the Commission has addressed potential competition theories of harm resulting from data concentration in reviewing certain data-rich mergers. This Section will first explore the role of personal data in merger analysis and data-related competition theories of harm developed through merger decisions. It will then examine two instances where data protection and privacy could be included in the substantive competition analysis.

[97] Geradin and Kuschewsky, 'Competition Law and Personal Data, Preliminary Thoughts on a Complex Issue' (n 6) 12; Kadar and Bogdan, 'Big Data' and EU Merger Control – A Case Review' (n 26).
[98] Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 429. The authors exemplify this regulatory dilemma with the Facebook investigations by the two national competition authorities. In 2019, the German Bundeskartellamt sanctioned Facebook due to the exploitative abuse of dominance behaviour under competition law, whereas the Italian Competition Authority investigated Facebook's similar behaviour and decided to sanction Facebook under consumer law.
[99] Autorité de la Concurrence and Bundeskartellamt (n 3) 23.

### 3.2.1 The Growing Role of Personal Data in Merger Analysis

Access to large datasets has increasingly been the primary driver of mergers in data-related markets.[100] Such data-rich mergers may entail particular data-related competition concerns depending on the role of data. Personal data can occupy two roles in digital markets: an ancillary role as an input or a traded commodity.[101] When personal data serves as an input for the provision of digital products/services, a possible exclusionary/anti-competitive foreclosure theory of harm might be that accumulation of data may constitute a barrier to entry or expansion in the market and give the merged entity a competitive advantage if data combination precludes competitors from replicating or acquiring the relevant data necessary to compete.[102] Even if the combination of the merging parties' data troves would not be possible, two firms may compete pre-merger to purchase and sell data, and the merger may eliminate this competition.[103] In the latter theory, personal data is considered a traded commodity.[104] The Commission has already evaluated the first theory of harm in a number of data-focused mergers,[105] and both have been framed by the Commission in *Microsoft/LinkedIn* as a relevant basis for assessing data-related competition concerns for future merger analysis.[106]

Some scholars argue that access to personal datasets cannot act as a barrier to entry or a source of market power due to data's non-rivalrous nature, its broad availability, its dispersed ownership, a significant degree of multi-homing by users, and diminishing returns, and thus there is no need for a competition intervention.[107] It is nonetheless important to note that data access can be made

[100] Stucke and Grunes, *Big Data and Competition Policy* (n 25) 3; Autorité de la Concurrence and Bundeskartellamt (n 3) 16.
[101] Costa-Cabral and Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12) 11-12; EDPS 2016 (n 17) 6.
[102] Costa-Cabral, Orla Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12) 11; Autorité de la Concurrence and Bundeskartellamt (n 3) 16; Elena Argentesi, Paolo Buccirossi, Emilio Calvano, Tomaso Duso, Alessia Marrazzo and Salvatore Nava, 'Merger Policy in Digital Markets: an Ex-Post Assessment' (2020) 17(1) Journal of Competition Law & Economics 95, 112-114. Bourreau et al, 'Google/Fitbit will monetise health data and harm consumers' (n 95) 4. Data accumulation may also facilitate the creation of "data-opolies" see Maurice E. Stucke 'Should We Be Concerned About Data-Opolies?' (2018) 2 Georgetown Law Technology Review 275.
[103] Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 78-79; Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 26-27.
[104] Costa-Cabral and Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12) 11.
[105] See, for instance, *Google/DoubleClick* (n 18), *Facebook/WhatsApp* (n 16), *Microsoft/LinkedIn* (n 16); *Google/Fitbit* (n 16); *Microsoft/Yahoo! Search Business* (n 63), *Thomson/Reuters* (n 61); *Telefónica UK/Vodafone UK/Everything Everywhere/JV* (n 63); *Publicis/Omnicom* (n 63); *Microsoft/Skype* (n 63).
[106] This theory of harm framework has later been followed by the Commission in the *Verizon/Yahoo* merger. See Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 82, Ocello and Sjödin, 'Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets' (n 74) 1-3 and *Verizon/Yahoo* (n 79).
[107] Gilbert and Pepper 'Privacy Considerations In European Merger Control: A Square Peg For A Round Hole' (n 34) 6-7, noting that the data combination may be a competition concern only in the most exceptional cases. For the US view see: Sokol and Comerford 'Antitrust and Regulating Big Data' (n 34) 1135-1140: Multi-homing means that users

exclusive,[108] direct network effects and certain limitations may reduce the users' ability to multi-home,[109] and available evidence on the diminishing returns is 'somewhat mixed'.[110] Moreover, not all datasets held by digital platforms are substitutable for each other; unique datasets may be needed to operate a specific online platform.[111] The Furman Report rightly notes that "consumer behavioural data held by the current incumbents, therefore, act as far more of a barrier to entry and expansion for potential rivals than it ever did when they were starting out".[112] Hence, such a general statement (*i.e.* access to personal data cannot act as a barrier to entry) cannot always hold true as the value and relevance of data are highly context-dependent, and the assessment of whether data combination would confer the merged entity a competitive advantage or raise the entry barrier depends on the factual circumstances of the case due to which a case-by-case reading is required.[113] As the decisions, statements, and reports of the competition authorities have developed; it is much more agreed that the accumulation of personal data at the hands of a single firm may, in some circumstances, create entry barriers/market power that warrants the application of competition law.[114]

---

use multiple online providers for several different services or even for the same service, and thus share its data with multiple providers (at 1135); Darren S Tucker and Hill Wellford, 'Big Mistakes Regarding Big Data' (2014) (Dec.) the Antitrust Source American Bar Association: Non-rivalrous nature of data refers that collection and use of data by one firm does not exclude collection and use of the identical data by others (at 3). For an overview of these concepts, in particular diminishing returns, from an economic perspective, see Andres V. Lerner, 'The Role of "Big Data" in Online Platform Competition' (2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780> accessed 19 June 2022: the author explains diminishing returns to scale that data collection can be valuable up to a certain point after which the returns from having additional data start to diminish.

[108] Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 23, 34-35-36. According to the Report, data can be made excludable through contract, technical barriers or regulation so that data owners cannot share it with others. The CMA states that simultaneous use of data can be prevented through licenses or other controls, see CMA, 'The Commercial Use of Consumer Data' (n 1) 94. See also, Stucke and Grunes, *Big Data and Competition Policy* (n 25) 46: the authors rightly question if personal data is freely-available, why companies are looking for a way to preclude other firms from getting access to data.

[109] Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 23, 34-35-36. Limitations on multi-homing may include: loss of personal data, loss of reputation, anti-competitive terms imposed by platforms, technical barriers, tying of services, and consumer inertia. In a similar vein, Deutscher notes that direct network effects constitute consumer lock-in and status quo bias which ultimately prevent them from multi-homing, see Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 18.

[110] Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 23, 34-35-36.

[111] For a good overview of the substitutability of different types of data, see Graef 'Market Definition and Market Power in Data: The Case of Online Platforms' (n 8), 495-501.

[112] Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 39.

[113] Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 88. See further, Daniel L. Rubinfeld and Michal Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339; Nils-Peter Schepp and Achim Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (2016) 7(2) Journal of European Competition Law & Practice 120.

[114] See, *Google/Fitbit* (n 16); Autorité de la Concurrence and Bundeskartellamt (n 3), CMA 'The Commercial Use of Consumer Data' (n 1), Crémer et al., *Competition Policy for the Digital Era* (n 24) 108-109; Furman et al., *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 33-41. For a good overview of the Commission's decisional practice evolution in this regard, see Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 72. For a similar view in the literature, see Marc Bourreau, Alexandre de Streel, and Inge Graef, 'Big Data and Competition Policy: Market Power, Personalized Pricing and Advertising' (2017) CERRE Policy Report; Stucke and Grunes, *Big Data and Competition Policy* (n 25);

As indicated, the Commission did consider data-related exclusionary concerns in some merger cases. However, until *Google/Fitbit*, it had never been convinced that these concerns would likely materialize due to either contractual constraints[115] or statutory limitations imposed on the merged entity by the relevant data protection legislation[116] and wide availability of data which are not within the merged entity's exclusive control.[117] Some authors rightly question the credibility of the Commission's reasoning on the so-called wide availability of data held by third parties post-merger[118] "without analysing the substitutability of the particular type of data affected in more detail".[119] Accordingly, to better address data-related competition concerns, competition analysis should assess: (i) the value of data in question in terms of economies of scale and scope, its level of transience, and diminishing returns; and (ii) actual and potential availability of substitutable data (whether data can be obtained from third parties, *e.g.* data brokers, or directly from users, respectively).[120] Moreover, defining an additional market for data is suggested for conducting a more comprehensive analysis.[121] In *Microsoft/LinkedIn* (later in *Verizon/Yahoo*), the Commission took a progressive step by referring to a hypothetical market for data, yet, one had to wait for the *Google/Fitbit* decision to see a relatively well-rounded analysis of the circumstances in which data combination might confer a significant competitive advantage to the merged entity.[122] The

Schepp and Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (n 113); Rubinfeld and Gal, 'Access Barriers to Big Data' (n 113).

[115] See, for instance, *Google/DoubleClick* (n 18); *Telefónica UK/Vodafone UK/Everything Everywhere/JV* (n 63).

[116] See, for instance, *Microsoft/LinkedIn* (n 16).

[117]See, for instance, *Google/DoubleClick* (n 18); *Facebook/WhatsApp* (n 16); *Microsoft/LinkedIn* (n 16), *Telefónica UK/Vodafone UK/Everything Everywhere/JV* (n 63).

[118] As repeatedly stated by the Commission: "a large amount of internet user data that valuable for advertising purposes that is not within the merging parties' exclusive control", see, for instance, *Google/DoubleClick* (n 18), *Facebook/WhatsApp* (n 16), *Microsoft/LinkedIn* (n 16), *Verizon/Yahoo* (n 79).

[119] Inge Graef, Thomas Tombal and Alexandre Streel, 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' (2019) 024 TILEC Discussion Paper, 10. See also Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 6-7; Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) 35-40.

[120] Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 86-87, citing Bourreau, De Streel and Graef, 'Big Data and Competition Policy: Market Power, Personalized Pricing and Advertising' (n 114) 7-8; Graef 'Market Definition and Market Power in Data: The Case of Online Platforms' (n 8), 503-504, including an overview of the actual substitutability of data at 495-501.

[121] Graef, *Ibid*. See also Konstantina Bania, 'The Role of Consumer Data in the Enforcement of EU Competition Law' (2018) 14(1) European Competition Journal 38, 42-55; Harbour and Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (n 25) 773.

[122] In particular, the Commission analysed these circumstances in view of (i) the relevance of Fitbit data for online advertising, (ii) Google's position in the market, (iii) data combination's impact, (iv) barriers to entry/expansion, (v) absence of countervailing buyer power and (vi) efficiencies, see *Google/Fitbit* (n 16) para. 430-467. It must be noted, though, that improvement in the Commission's analysis mentioned herein only refers to the assessment of data-related competition concerns in the market for online advertisement. The Commission found no concerns regarding the merger's impact on competition in the market for general search services (because Fitbit data is less relevant) and digital healthcare services (as there are alternative data providers available), see *Google/Fitbit* (n 16) para. 469-496. For the latter market, the Commission's reasoning regarding the substitutability of the remaining data has been criticized, see, for instance, Jay Modrall, 'Google/Fitbit: The EU Commission Misses A Step' (Kluwer Competition

Commission in *Google/Fitbit* took into consideration the value and relevance of the data in question for online advertising services,[123] and examined the actual and potential availability of substitutable data, as a result of which it concluded that there was no dataset comparable to those offered by Fitbit that the competing advertisers could rely on.[124]

That said, although the evolution of the Commission's assessment of the exclusionary data-related competition concerns should be welcomed, it still lacks the evaluation of potential direct privacy-reducing consumer harm caused by data concentration.[125] To be more precise, in the context of multisided platforms, exclusionary theories[126] focus on the role of personal data as a source of market power and anti-competitive foreclosure, and analyse whether the accumulation of data could harm rivals and customers on the paying side of the platform. Such theories only deal with indirect (end-)consumer harm that occurs when the market power gained/strengthened through data accumulation allows the merged entity to charge higher prices on the paying side of the platform (*e.g.* for advertising services), which will be then passed on to consumer prices (*e.g.* for the advertised products/services).[127] In contrast, these theories do not analyse to what extent accumulation of personal data may have direct exploitative effects on consumers on the free side of platforms, for instance, in the form of degraded privacy protection. It seems that this "blind-spot" in the Commission's approach to data-driven mergers could be cured through a privacy-related theory of harm, namely privacy-as-competition-parameter, articulated by the competition scholars and, to a certain extent, by the Commission.[128]

---

Law Blog June 17, 2021) <http://competitionlawblog.kluwercompetitionlaw.com/2021/06/17/google-fitbit-the-eu-commission-misses-a-step/> accessed 19 June 2022.

[123] *Google/Fitbit* (n 16) para. 430-434. See *supra* footnote 88.

[124] *Google/Fitbit* (n 16) para. 457. This is because, while "Fitbit is just one of many sources of health and wellness data, […] none of Google's competitors in online advertising has access to a database or data collection capabilities equivalent to those of Fitbit and it is not likely that they would acquire such assets without incurring into significant costs and in timely manner. In fact, no competitor of Fitbit seems to make its data available for advertising purposes".

[125] Nick Economides and Ioannis Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: a Competition Law Perspective' (2019) 5 CLES Research Paper Series, 31-32; Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 10; Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) 40, 42, 43; Kadar and Bogdan, 'Big Data' and EU Merger Control – A Case Review' (n 26) 486, noting that 'the Commission is primarily concerned by horizontal overlaps or by vertical (input) foreclosure theories'.

[126] For a description of the concepts of exclusionary and exploitative abuses see Robert O'Donoghue and A. Jorge Padilla, *The Law and Economics of Article 102 TFEU* (3rd ed., Hart Publishing 2020) 262, 294-302.

[127] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 10, citing Nathan Newman, 'Search, Antitrust, and the Economics of the Control of User Data' (2014) 30(3) Yale Journal on Regulation 401, 441. Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 346. For instance, in *Google/Fitbit*, the Commission examined whether the combination of Fitbit's health data with Google's data would increase barriers to entry/expansion in the online advertising market which would likely raise advertising prices, without looking into possible privacy-reducing theories of consumer harm. See *Google/Fitbit* (n 16) Section 9.3.3.

[128] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 1-2, 9-13; Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) 40, 42, 43.

### 3.2.2 Towards a Workable Theory of Consumer Harm: Privacy as a Competition Parameter

According to the EU competition policy, undertakings compete to offer consumers lower prices, high-quality and improved products/service with a wide range of choices.[129] Although the price has traditionally been the central focus in assessing the competitiveness of a given market, the value of other competitive parameters important to consumers is widely acknowledged.[130] Indeed, the Court in *Post Danmark I* stated that "[c]ompetition on the merits may, by definition, lead to the departure from the market or the marginalization of competitors that are less efficient and so less attractive to consumers from the point of view of, among other things, price, choice, quality or innovation".[131] With the expansion of digital markets where the products/services are often supposedly offered for free, the traditional price-based approach to consumer welfare may prove to be dysfunctional, and instead, quality may come to the forefront as an important parameter of competition.[132]

The privacy-as-competition-parameter concept has been widely accepted throughout the competition and data protection interface discussion.[133] The Commission, in theory, articulated the quality of the privacy policy offered to users as a competitive parameter on which undertakings

[129] Commission Guidelines on the Assessment of Horizontal Mergers under the Council Regulation on the Control of Concentrations Between Undertakings [2004] OJ C31/05, para. 8 (hereinafter "the Horizontal Merger Guidelines"); Commission Guidelines on the application of Article 81(3) of the Treaty [2004] OJ C101/97, para. 16; the Guidance Paper (n 13) para. 5.

[130] Ariel Ezrachi and Maurice Stucke, 'The Curious Case of Competition and Quality' (2014) 256 University of Tennessee Legal Studies Research Paper Series; Ioannis Lianos, 'Some Reflections on the Question of the Goals of EU Competition Law' (2013) 3 CLES Working Paper Series. The growing importance of non-price competition parameters can be clearly seen in the Commission's relatively recent merger decision. In the *Dow/DuPont* merger, the Commission analysed the transaction's effect on innovation, as a non-price parameter, and found that the merger could significantly reduce innovation competition in pesticide markets, due to which it required a divestment commitment, see *Dow/DuPont* (Case COMP/M.7932) Commission Decision [2017] OJ C353/9.

[131] *Post Danmark A/S v Konkurrencerådet* (n 49) para. 22.

[132] Ezrachi 'The Goals of EU Competition Law and the Digital Economy' (n 50); *Microsoft/Skype* (n 63) para. 81; *Microsoft/Yahoo! Search Business* (n 63) paras. 101, 119. See also Michal Gal and Daniel L Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' (2016) 80(3) Antitrust Law Journal 521, 532; Stucke and Grunes, *Big Data and Competition Policy* (n 25) 116. For the references to the quality dimension in the Horizontal Merger Guidelines (n 129), see para. 36 (about decreasing quality) and para. 65 (about deteriorating quality).

[133] OECD, 'Consumer Data Rights and Competition' (n 24) 25; Economides and Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: a Competition Law Perspective' (n 125) 31; Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24); EPDS 2014 (n 17); CMA 'The Commercial Use of Consumer Data' (n 1); Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 4; Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (n 8); Margrethe Vestager, European Commissioner for Competition, Competition in a Big Data World, Address Before the DLD 16 Conference (January 17, 2016) recognizing privacy as a non-price dimension of competition. For the US view: Grunes and Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (n 27). OECD defines the concept of privacy quality as a competition parameter as "the control that consumers have over whether and how much of their data is collected (the range of data and its frequency); how it is used, both by the collecting entity and any third parties that are granted access to it; and how it is safeguarded from unauthorized or inappropriate uses". See OECD 'Quality Considerations in Digital Zero-Price Markets' (n 15) 7.

may engage in competition[134] so long as it constitutes "an important parameter in the eyes of (a significant number of) customers" or "a key parameter of competition".[135] This concept integrates data protection and privacy into competition law assessment as the competitive implications of privacy following a merger are inherently related to the substantive competition analysis. Therefore, incorporating privacy in this way does not contradict the Commission's tendency not to factor pure privacy interests in competition analysis.

The privacy-as-competition-parameter theory of harm might include: (i) a decrease in privacy quality post-merger by way of either directly degrading the level of privacy afforded or increasing the intensity of collection and use of personal data without counterbalancing the product/service benefits,[136] or (ii) a decrease in the merged entity's incentive to compete to offer high levels of privacy or invest in privacy-friendly products/services.[137] This concept suggests that privacy quality degradation could reduce consumer welfare in the same way as price increase could.[138]

These theories might apply even if the merging parties are not deemed close competitors, for instance, when the merger removes a "maverick"[139] that disrupts the market by developing or

[134] See *Facebook/WhatsApp* (n 16) and *Microsoft/LinkedIn* (n 16), see *supra* Sections 2.3.2 and 2.3.3. Although acknowledged in theory, privacy has so far not appeared as a significant parameter on which firms engage in competition in the Commission's decisional practice.

[135] Ocello and Sjödin, 'Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets' (n 74) 5, and Ocello, Sjödin, and Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (n 55) 6, respectively.

[136] Ocello, Sjödin, and Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (n 55); Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 4; Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (n 93) 83. For the US view, see Grunes and Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (n 27) 4. Indeed, the collection of a massive amount of personal data is considered as charging an excessive price, see OECD 'Consumer Data Rights and Competition' (n 24) 29; OECD 'Big Data: Bringing Competition Policy to the Digital Era' (n 9) 48. See also *infra* footnote 167.

[137] Gilbert and Pepper 'Privacy Considerations In European Merger Control: A Square Peg For A Round Hole' (n 34); Harbour and Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (n 25) 794; Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (n 7) 632.

[138] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 16; Autorité de la Concurrence and Bundeskartellamt (n 3) 24-25; Ocello, Sjödin, and Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (n 55) 6, noting that "a web-site that, post-merger, would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its 'free' product could be seen as either increasing its price or degrading the quality of its product"; Grunes and Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (n 27) 36; Newman, 'Search, Antitrust, and the Economics of the Control of User Data' (n 127) 442-443.

[139] Maverick is defined as a "firm that has a history of preventing or disrupting coordination, for example by failing to follow price increases by its competitors, or has characteristics that gives it an incentive to favour different strategic choices than its coordinating competitors would prefer". See the Horizontal Merger Guidelines (n 129) para. 42. For an analysis of the concept of maverick firm in the EU merger control, see Joseph Bromfield and Matthew Olczak, 'The Role of the Maverick Firm Concept in European Commission Merger Decisions' (2018) 14(2) Journal of Competition Law and Economics 179.

offering an innovative privacy-enhancing product.[140] Although the Commission noted in *Facebook/WhatsApp* that the parties were not close competitors,[141] WhatsApp could have been considered a maverick exerting competitive pressure on Facebook Messenger and other texting apps that prioritize behavioural advertising over users' privacy needs by offering a higher level of privacy protection to its users (through its no-ads and privacy-focused business model).[142] Indeed, when the merger was notified, WhatsApp had grown into a leading online texting app within less than five years from its launch, thanks to, in part, its "top-grade privacy protection".[143] Some scholars rightly contend that the merger diminished competition over the quality of privacy policies[144] and decreased user choice by removing a privacy-friendly app from the market.[145] While the Commission recognized the privacy-as-competition-parameter theory in *Facebook/WhatsApp*, it shied away from thoroughly exploring any privacy-quality degradation theory of harm. A slightly improved approach was taken in *Microsoft/LinkedIn*, where it held that combining personal user data could generate foreclosure effects, leading to the marginalization of existing competitors offering a higher degree of privacy protection than LinkedIn, and thus, the merger would restrict consumer choice in relation to privacy.[146] In addition to the product quality dimension, as endorsed in *Microsoft/LinkedIn*, privacy can be framed as an important element of consumer choice.[147]

---

[140] Gilbert and Pepper 'Privacy Considerations In European Merger Control: A Square Peg For A Round Hole' (n 34) 5, suggesting that "the removal of an important maverick that has developed innovative data-protection and control systems could potentially raise competition issues by reducing innovation in data privacy, even if the merging parties were not otherwise close competitors". See also Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 4.

[141] *Facebook/WhatsApp* (n 16) para. 107.

[142] Stucke and Grunes, *Big Data and Competition Policy* (n 25) 133. The Commission also indicated that WhatsApp did not store messages and did not collect any user data for the purposes of online advertising, see *Facebook/WhatsApp* (n 16) paras. 102 and 166.

[143] Maurice E. Stucke 'The Relationship Between Privacy and Antitrust' (2022) Notre Dame Law Review (Forthcoming), 3, citing the First Amended Complaint for Injunctive and Other Equitable Relief, FTC v Facebook Inc. No. 1:20-cv-03590 (DDC filed August 19, 2021), para. 114.

[144] As "WhatsApp represented a moat to prevent inroads from rival, privacy-focused texting apps" see Stucke and Grunes, *Big Data and Competition Policy* (n 25) 83. Although Facebook did not introduce advertising on WhatsApp, it gradually reduced the level of privacy protection offered by WhatsApp post-merger through privacy policy updates in 2016 and 2021. In 2016, WhatsApp updated its privacy policy to share certain user data, including users' phone numbers with Facebook, which allowed Facebook to further intensify its tracking and targeted advertisement activities. Later in January 2021, WhatsApp announced its new privacy policy which states that WhatsApp may share user data such as phone numbers, IP addresses, and payments made through the app with Facebook and its businesses. But this time without an opt-out option; the 2021 update involved a take-it-or-leave-it condition, that is to say, unless people accept the update they will not be able to continue using WhatsApp's messaging functions as of February 8, 2021. See <https://www.whatsapp.com/legal/privacy-policy/revisions/20160825?lang=et> and <https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page > accessed 19 June 2022.

[145] Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 6.

[146] *Microsoft/LinkedIn* (n 16) para. 350.

[147] *Microsoft/LinkedIn* (n 16) para. 350, footnote 330. See also, Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 12. For the references to the consumer choice, see the Horizontal Merger Guidelines (n 129) para. 8.

### i. Challenges of Resorting to the Privacy-as-Competition-Parameter Theory

That said, two challenges have generally been voiced against the privacy-as-competition-parameter theory. Firstly, it is argued that firms, in practice, do not (or rarely) compete based on their privacy quality.[148] One argument for the absence of privacy competition lies in the so-called privacy paradox; that is, while consumers often claim that they care about the protection of their privacy and data, these reported preferences do not correspond to their actual behaviours.[149] As such, consumers may be willing to pay less or none as a trade-off for disclosing more personal information to digital companies.[150] Yet, there exists no one-fits-all approach given that product/service characteristics in, and specific circumstances of, each market differ, so does the level to which consumers value privacy quality of a product/service compared to any trade-offs they possibly receive by agreeing on a lower privacy quality.[151] It may be observed that consumers are often not as adamant in demanding more privacy-friendly products/services as they are in choosing lower-priced products/services. This could stem from the numerous hurdles consumers face during their privacy-sensitive decision-making process: consumers often do not know how tech firms use their data due to these firms' untransparent data processing activities and lack of intelligibility of declarations of consent (*e.g.* privacy policies are often too long or complicated which makes it harder to understand for an average user).[152] Even if they do know, they generally have limited control over the use of their data vis-à-vis these tech giants because of their lack of bargaining power and oft-used take-it-or-leave-it conditions according to which users have to

[148] Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 433; OECD 'Quality Considerations in Digital Zero-Price Markets' (n 15) 7; Colangelo and Maggiolino 'Data Protection in Attention Markets: Protecting Privacy Through Competition?' (n 44) 368; Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 13) 7.

[149] Colangelo and Maggiolino 'Data Protection in Attention Markets: Protecting Privacy Through Competition?' (n 34) 368; Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 7; Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25) 6-7; Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 432. For an overview of privacy paradox see Spyros Kokolakis, 'Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon' (2017) 64 Computers & Security 122.

[150] On the monetary value of privacy see Alessandro Acquisti, Liad Wagman, Curtis Taylor, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442.

[151] Indeed, Kerber explains that privacy preferences are highly 'context-specific' and 'heterogenous', see Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25) 7.

[152] Botta and Wiedemann examines privacy paradox through the role of consent, and suggest that the root cause of this phenomenon does not relate to users' unwillingness or laziness to act to protect their data and privacy, but it rather lies on the lack of users' ability to make an informed choice because of the firms' untransparent data processing activities and the lack of intelligibility of declarations of consent, see Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 432. See further, CMA 'The Commercial Use of Consumer Data' (n 1) 100-101, citing the Demos and Ofcom studies, respectively reporting that participants "[…] knew and understood much less about how data were collected and used" and "[…] had only vague ideas about what happened to their personal data online", see Jamie Bartlett, *The Data Dialogue* (Demos September 2012) and Ofcom, 'Being Online: an Investigation of People's Habits and Attitudes' Ipsos MORI, June 2013.

either consent to the dictated terms or quit the service.[153] Moreover, public opinion regarding privacy and data protection is progressively changing towards a more privacy-consciousness stage.[154] Moncuit argues that tech companies may create a "Schumpeterian wave" by entering the market using privacy protection as a competitive asset vis-à-vis existing players, and consumers may suddenly surge towards new tech firms offering more privacy-focused services.[155] Hence, a case-by-case approach is required to deliver a reliable competition analysis that better reflects actual consumer preferences regarding the desired privacy quality in a given market and thus the merger's effects on privacy as a competition parameter.

A second underlying argument for the lack of privacy competition is that the accumulation of market power has already worsened privacy protection in the market. As Stucke and Grunes note, "the reason why market forces have not yielded the privacy protections that individuals desire is the absence of meaningful competition".[156] Indeed, in many digital markets, direct network effects fuel market concentration and dominance, which thus leaves users with no or only a limited choice for the use of a given product/service.[157] Thus, it is safe to claim that digital markets as such are not able to satisfy users' privacy preferences properly.

---

[153] Bart Custers, et al, 'Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10(4) SCRIPTed 435, 456-57; Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (2018) 34(2) Computer Law & Security Review 289; Damian Clifford, Inge Graef, and Peggy Valcke, 'Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2017) CiTiP Working Paper 3, 35.

[154] OECD 'Quality Considerations in Digital Zero-Price Markets' (n 15) 7, referring to the launch of privacy-focused services like the anonymous web search service DuckDuckGo; Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (n 93) 88; Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 25-26. For instance, after the announcement of WhatsApp's privacy policy change in 2021, 25 million new users reportedly joined Telegram (offering a more privacy-friendly service) within 72 hours, and Signal (another privacy-focused alternative) has become one of the most downloaded apps, see <https://t.me/durov/147> and <https://www.theverge.com/2021/1/12/22226792/whatsapp-privacy-policy-response-signal-telegram-controversy-clarification> accessed 19 June 2022, respectively. Likewise, following the 2021 update, many Turkish users switched over to Telegram, Signal and BiP (a Turkish online messaging application) in an effort to use more privacy-focused options, see < https://www.trtworld.com/life/turkish-whatsapp-users-quit-app-as-demand-spikes-for-other-options-43133> accessed 19 June 2022. Due to growing public outcry, the Turkish Competition Authority has promptly responded, and only 3 days after the announcement, it has opened an in-depth investigation towards Facebook over the said privacy update under Article 6 of the national competition act concerning the abuse of dominant position, see <https://www.ic4r.net/2021/02/02/turkish-competition-board-tcb-has-launched-an-investigation-against-facebook-for-its-recent-implementation-concerning-data-sharing-preferences/ > accessed 19 June 2022.

[155] Aymeric de Moncuit, 'In Which Ways Should Privacy Concerns Serve as an Element of the Competition Assessment' (2018) <https://ec.europa.eu/competition/information/digitisation_2018/contributions/aymeric_de_moncuit.pdf> accessed 19 June 2022, 2 and 10.

[156] Stucke and Grunes, *Big Data and Competition Policy* (n 25) 51, cited from Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 7. Likewise, the Furman Report indicates that "[…] misuse of consumer data and harm to privacy is arguably an indicator of low quality caused by a lack of competition": see Furman et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 43.

[157] Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 432; Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25) 7 and 9. The CMA notes that the lack of privacy

A third argument might be explained by the competition enforcers' premise that the existence of data protection legislation "is, in itself, sufficient to ensure that markets involving personal data accurately reflect consumer data privacy preferences".[158] It is nonetheless important to note that the GDPR's concept of consent, as an indicator of consumers' privacy preferences, may have flaws, especially in digital markets shaped by strong network effects, given that users' ability to make an informed choice is often undermined by the incumbent firms' untransparent disclosure activities and lack of salient and understandable privacy policies.[159] As Lynskey puts forward, this "erroneous" premise may lead to a general finding of lack of privacy competition and thus to more market concentration since the transaction would not be subjected to further analysis on whether the parties actually compete on this basis.[160] Thus, weak competition in the digital markets in a way fuels the degradation of users' privacy rights, and a vicious cycle ensues. From an economic perspective, a well-functioning competitive market would be capable of providing more privacy options, which could also satisfy consumers' demand for better privacy protection and ultimately foster privacy competition.[161]

The second challenge is a technical one. Even if one can establish privacy competition, measuring consumer harm resulting from privacy quality degradation is still difficult to perform.[162] New economic methods are being developed to quantify quality degradation, such as the SSNDQ test (small but significant non-transitory decrease in quality), which posits that the impact of the quality decrease can be measured in a similar way to price increase and examines to what extent a firm could profitably degrade (privacy) quality offered to the detriment of users.[163] However, it is still

competition shows that digital markets fail to deliver what consumers want regarding privacy, see CMA 'The Commercial Use of Consumer Data' (n 1) 95.

[158] Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 3.

[159] Bart Custers, et al, 'Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law' (n 153) 456-57; Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 433.

[160] Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 3.

[161] Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25) 9. For an economic study on the competition and privacy, see Ramon Casadesus Masanell and Andres Hervas Drane. 'Competing with Privacy' (2015) 61(1) Management Science 229: the authors conclude that competition drives the provision of services with a low level of disclosure when consumers' willingness to pay is high, and it also ensures that services with a high level of disclosure subsidize consumers when their willingness to pay is low.

[162] For a comprehensive contribution on quality measurement in competition analysis see OECD, 'The Role and Measurement of Quality in Competition Analysis' 28 October 2013 (DAF/COMP(2013)17) <https://www.oecd.org/competition/Quality-in-competition-analysis-2013.pdf > accessed 19 June 2022, and Ezrachi and Stucke, 'The Curious Case of Competition and Quality' (n 129); Stucke and Grunes, *Big Data and Competition Policy* (n 25) 115-122 . For a good overview of quality as a dimension of competition in digital markets see OECD, 'Quality Considerations in Digital Zero-Price Markets' (n 15). See also Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27).

[163] This test originally derives from the SSNIP test (small but significant non-transitory increase in price), that is traditionally used by competition authorities to define relevant markets and assess market power. OECD, 'The Role and Measurement of Quality in Competition Analysis' (n 162) 9; Gal and Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' (n 132) 551-552; Stucke and Grunes, *Big Data and Competition Policy* (n 25) 118-122; Crémer et al, *Competition Policy for the Digital Era* (n 24) 50. Elsewhere, this test is also called as SSNDPP – small but significant non-transitory decrease in privacy protection – see, for instance, Stucke

unclear how this test can be applied to concrete cases.[164] Indeed, competition law's economic-oriented methods alone might be of little use in measuring the actual consumer harm arising from privacy degradation. In this regard, the defects of quantitative methods can be remedied by applying qualitative methods that could be developed with the help of EU data protection rules as normative guidance, which will be explored in Section 3.3.2 below.

### ii. Practical Implications of Integrating the Privacy-as-Competition-Parameter Theory

The extension of the consumer harm theories beyond traditional price parameter carries at least, two practical implications. First, integrating the privacy-as-competition-parameter into the analysis of data-driven mergers (typically involving multisided platforms) would nudge the Commission to focus on "a more immediate form of consumer harm on the free user side of online platforms" in the form of exploitative behaviours, in addition to its current attention on examining indirect consumer harm stemming from data combination-originated foreclosure on the paying side.[165] Indeed, by having access to a larger consumer database, the merged entity may be able to exploit its market power to the detriment of consumers by way of, for instance, price or quality-based discrimination on the basis of their online behaviour,[166] or lower privacy protection by

'Should We Be Concerned About Data-Opolies?' (n 102) 287. For a different economic quantitative method for measuring the consumer harm arising from the quality degradation, see Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27), the author develops a 'privacy calculus' model based on a study of willingness-to-pay for privacy in monetary terms in the form of conjoint analysis.

[164] Crémer et al, *Competition Policy for the Digital Era* (n 24) 50; Stucke and Grunes, *Big Data and Competition Policy* (n 25) 117; OECD, 'The Role and Measurement of Quality in Competition Analysis' (n 162) 9, noting that in practice SSNDQ test "is unworkable, […], given the inherent difficulties of measuring quality alongside the existing complications of the applying the SSNIP test itself within real market situations". As an example, SSNDQ test is applied in Qihoo 360 v TenCent case by the Supreme People's Court of China, see David S Evans and Vanessa Y Zhang 'Qihoo 360 v Tencent: First Antirust Decision by the Supreme Court' (2014) Competition Policy International 1, <https://www.competitionpolicyinternational.com/qihoo-360-v-tencent-first-antitrust-decision-by-the-supreme-court/> accessed 19 June 2022.

[165] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 16-18. For an overview of different types of privacy-related exploitative theories of harm in the context of abuse of dominance analysis, see Economides and Lianos 'Restrictions on Privacy and Exploitation in the Digital Economy: a Competition Law Perspective' (n 125) 35-72. It must be noted that the focus on exploitative conducts does not imply that exclusionary behaviours could not cause privacy harm.

[166] CMA 'The Commercial Use of Consumer Data' (n 1) 91-93: on the quality-based discrimination, the Report notes that "[…] the collection of consumer data may enable firms to make judgments about the lowest level of quality needed by consumers/groups of similar consumers. This may enable a firm to engage in quality discrimination where quality differences are not reflected in the prices of goods and services". Quality-based discrimination can be done by either "restricting the products that are displayed to consumers" or "varying the order in which products are listed on their website to display relatively poorer or better quality products first depending on the information they collect about consumers". See further, Wolfie Christl, 'How Companies Use Personal Data Against People: Automated Disadvantage. Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information' (2017) Working Paper by Cracked Labs 28; Alessandro Acquisti, 'The Economics of Personal Data and the Economics of Privacy' (2010) OECD Privacy Guidelines Background Paper 3, 17; Christopher Townley, Eric

harvesting too much data from them.[167] A similar theory of harm has been articulated by the Bundeskartellamt in its investigation against Facebook.[168] The Bundeskartellamt found that Facebook's data use conditions were in violation of data protection rules and thus constituted an exploitative abuse in the market for social networks. Yet, the Commission developed a theory of consumer harm based on the exclusionary effects of data combination, namely whether the competitors would have access to a similar dataset post-merger necessary to compete with the merged entity, but did not further consider how data combination could subsequently allow the merged entity to exploit consumers.[169] This approach correlates with the Commission's general reluctance to challenge exploitative abuses involving direct consumer harm (vis-à-vis exclusionary abuses) which may stem from the "belief in the self-correcting nature of the market that may mitigate harmful effects of exploitative behaviour by dominant firms in the longer term".[170] Disclosure of even more consumer data might alter the balance of power between the consumers and incumbents in favour of the latter, which would then further exacerbate its market power.[171] Due to this, and unprecedented scale of data activities, one could claim that the self-correcting nature of the market has vanished into thin air. Thus, the need for developing a more privacy-focused consumer exploitation theory of harm could be satisfied by the privacy-as-competition-

Morrison and Karen Yeung, 'Big Data and Personalized Price Discrimination in EU Competition Law' (2017) 38 King's College Research Paper Series, 1-2.

[167] Literature suggests that lowering the level of privacy protection could constitute an exploitative abuse, see Ezrachi and Robertson, 'Competition, Market Power and Third-Party Tracking' (n 25) 8-9; Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (n 7). For the US view, see Stucke 'Should We Be Concerned About Data-Opolies?' (n 102) 286-287, defining the excessive data collection as the equivalent of charging an excessive price: "A data-opolist, to the extent its business model depends on harvesting and exploiting personal data, has the incentive to reduce its privacy protection below competitive levels and collect personal data above competitive levels". For the same analogy, see Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in an Era of Big Data' (n 10) 172-178; Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 137.

[168] Yet, the Bundeskartellamt did not opt for framing privacy conditions as quality, rather it considered privacy conditions for using a product or service as 'trading conditions' and found that such conditions constituted an exploitative abuse ('exploitative business terms'), see Press Release Bundeskartellamt 'Bundeskartellamt prohibits Facebook from combining user data from different sources' 7 February 2019 <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html >. For the official English version of the decision: Bundeskartellamt Decision B6-22/16, 6 February 2019 <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5> accessed 19 June 2022. For an opposing view on the Bundeskartellamt's reasoning, see Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision' (n 34) 4-5, claiming that increased user data collection benefits a large number of users rather than exploiting them.

[169] Economides and Lianos 'Restrictions on Privacy and Exploitation in the Digital Economy: a Competition Law Perspective' (n 125) 31-35; Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) 40, 42. In this regard, Lynskey and Costa-Cabral referred to the Court's approach in the Tetra Laval decision, and rightly noted that '[…] it is not the sole role of the Commission under the EUMR to prevent the creation and strengthening of a dominant position; the Commission must also consider the incentives for the abuse of such position post-merger.' Costa-Cabral and Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12) 27, citing Case C-12/03 *Commission of the European Communities v Tetra Laval* [2005] ECR I-987, para. 74.

[170] Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 211-212. Indeed, the Commission's Guidance Paper (n 13) provides enforcement guidance concerning the exclusionary conduct by dominant firms, and does not address exploitative conducts.

[171] Acquisti, 'The Economics of Personal Data and the Economics of Privacy' (n 166) 17.

parameter concept. Furthermore, privacy-as-competition-parameter theory of harm could also complement the analysis of unilateral effects on price in a given horizontal merger, by involving the assessment of whether the elimination of a competitive constraint on privacy as a result of the merger would increase the merged entity's ability and incentive to degrade the level of privacy protection.[172] Overall, such privacy-related consumer harm theory would lead to a complete picture of the merger's potential effect, including "direct" consumer harm, on each "key" competition parameter and all sides of online platforms.

Secondly, integrating privacy-as-competition-parameter may go hand in hand with defining a market for data. Given the multi-sided nature of many online platforms, the conventional market definition approach focusing solely on the paying side may be the reason for not adequately addressing potential harms occurring on the (free) user side. Several scholars have thus suggested that the definition of a potential market for data in addition to the existing relevant markets would significantly contribute to delivering reliable and complete analysis of competition concerns arising on both sides of the multisided platforms as a result of a data-driven merger.[173] This is because, although digital markets are not often shaped by supply and demand for data in the formal sense, tech firms do compete over the acquisition of data valuable for improving their ability to deliver high quality and more relevant services (*e.g.* better-tailored ads) as well as for developing new products/services, and defining a market for data would better capture not only current data usages but also prospective data activities in digital markets.[174] Hence, the definition of a market for data could allow the Commission to scrutinize privacy-related consumer harms, in particular, it helps the Commission to predict the potential exploitative concerns stemming from the aggressive use of accumulated consumer data.[175]

[172] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 16-17.

[173] Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (n 8) 489-501, noting that under the EU competition rules definition of market for data can only be performed to the extent that data is commercially traded (at 490); Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 79-81; Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 77-78; Konstantina Bania, 'The Role of Consumer Data in the Enforcement of EU Competition Law' (n 121) 42-55. Likewise, in the US, Harbour and Koslov propose defining a market for data to give an accurate picture of market reality: "Internet-based firms often derive great value from user data, far beyond the initial purposes for which the data initially might have been shared or collected, and this value often has important competitive consequences. In contrast, product market definitions based only on a snapshot of current data usage may not accurately capture this aspect of competition, especially in markets that exhibit network effects based on aggregations of data". See Harbour and Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (n 25) 773.

[174] Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 77-78. Harbour and Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (n 25) 773.

[175] Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 15-16.

### 3.2.3 The Evolution in the Role Attributed to Data Protection Rules

In the Commission's practice, a second instance where data protection rules are integrated into substantive competition analysis is as a statutory limitation on the merged entity's ability to engage in anti-competitive conduct.[176] Albeit a favourable improvement given the expanding intersection between data protection and competition law, the Commission's reasoning on the assumed role for data protection rules as a limit has certain flaws. From a logical perspective, the legality of conduct under data protection law (or any legal field) does not guarantee compliance with competition rules.[177] Thus, the existence of data protection legislation cannot (and should not) preclude the enforcement of competition rules especially given the complexity of digital markets and multi-layered market problems posed by emerging technologies. Moreover, the reference to the GDPR rules as a limit preventing potential competition concerns from arising posits that such rules are complied with and effectively enforced. The Commission in *Microsoft/LinkedIn* seems to put "too much faith" in the (then) newly adopted GDPR regime, which might not be as effective as one would assume "in addressing the existing loopholes regarding data".[178] Indeed, there has been a continued debate on the dissuasiveness and enforceability of the EU data protection legislation, which may negatively affect the effective operation of such rules.[179] Graef points out a "bottleneck" in the enforcement of data protection rules vis-à-vis big tech firms, which is that the lead supervisory authority of many big tech firms is often either Irish or Luxembourg data

[176] Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 215-217. Jörg Hoffmann and Germán Johansen, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-05, 40-48: the Authors refer to this functionality of the applicable data protection regime as 'normative factual remedies' that could render personal data-related competition concerns unnecessary. See *Microsoft/LinkedIn* (n 16), *Verizon/Yahoo* (n 79), *Google/Fitbit* (n 16); See also *Sanofi/Google/DMI JV* (Case COMP/M.7813) Commission Decision [2016] OJ C112/1, para. 69: the Commission stated that the transaction parties would "lack the ability to lock-in patients by limiting or preventing the portability of their data given that, according to the draft General Data Protection Regulation (GDPR) users will have the right to ask for the data portability of their personal data".

[177] Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 437; Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 19. This logic is also supported by the Court's case law. For instance, in *Deutsche Telekom,* the Court stated that the legality of the conduct in question under the relevant telecom regulation could not diminish the undertaking's responsibility to comply with the legal rules on abuse of a dominant position, see, Case C-280/08 P *Deutsche Telekom AG v European Commission* [2010] ECR I-09555 para. 80-85. Likewise, in *Astra Zeneca,* the Court held that "[…] the illegality of abusive conduct under Article 82 EC is unrelated to its compliance or non-compliance with other legal rules and, in the majority of cases, abuse of dominant positions consist of behaviour which is otherwise lawful under branches of law other than competition law." Case C-457/10 P *AstraZeneca AB and AstraZeneca plc v. European Commission* [2012] ECLI:EU:C:2012:770, para. 132.

[178] Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20) 30-31. See also Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 216; Hoffmann and Johannsen, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (n 176) 48.

[179] Sebastian J. Golla, 'Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR' (2017) JIPITEC. For an overview of the enforcement challenges regarding the EU data protection rules, see David Wright, 'Enforcing Privacy' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International Publishing 2016) 25-33.

protection authorities, and these authorities lack the necessary resources to adequately address the wide-scale cases that these tech firms involved in.[180]

The *Google/Fitbit* decision marks an evolution in the Commission's treatment of data protection rules as a limit towards a nuanced view. The Commission was not convinced that Google's compliance with the GDPR could evaporate the risks that Google's control of aggregated data would raise barriers to entry/expansion in the market. This reflects a realisation on the Commission's side that competition concerns should be assessed on their own. It must be borne in mind that the Commission is entrusted with the ultimate authority to decide in which instances data protection law cannot provide an effective solution to the data-related competition concerns, and thus competition intervention is warranted.[181] In *Google/Fitbit*, the Commission seems to opt for a "cautious approach" -some competition scholars have called for-[182] when assessing the ability of data protection rules to prevent firms from engaging in anti-competitive conduct and eliminate competition concerns stemming from data concentration.

## 3.3 Integrating Data Protection and Privacy into Merger Assessment Beyond Substantive Competition Analysis

### 3.3.1 A Normative Discussion: Integration of Data Protection and Privacy Concerns as a Standalone Issue

Differently from the integration of data protection and privacy as part of substantive competition analysis, one can raise a more far-reaching question of competition policy, namely, whether pure data protection and privacy concerns should take part in competition analysis as a standalone issue. This is more of a normative discussion on whether an economic-oriented policy should factor non-efficiency interests like the protection of consumers' data and privacy as a discrete consideration,[183] which has been constantly answered in the negative by the Commission, as

[180] Inge Graef, 'The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation' (2020) (Nov.) CPI Antitrust Chronicle, 7; citing the Commission Communication, 'Data Protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation" COM(2020) 264 Final, June 24, 2020, 5-6. See further, Billy Hawkes, 'The Irish DPA and its Approach to Data Protection' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International Publishing 2016); Wright, 'Enforcing Privacy' (n 179) 43.

[181] Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 436.

[182] See, Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 218; Hoffmann and Johannsen, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (n 176) 48.

[183] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 146; Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10) 13-19.

discussed above.[184] Privacy advocates[185] and policymakers[186] have been vocal about expanding the normative scope of competition enforcement so as to incorporate non-economic concerns like data protection violations. The idea is that the expansion of the digital economy has revealed that data protection rules alone are insufficient to overcome potential privacy harms and there is a need for a holistic approach from different regulatory perspectives, including competition law.[187] Competition scholars overwhelmingly refused this "controversial" attempt to use competition law to resolve data protection and privacy problems because non-economic interests fall outside the scope and goal of competition law and competition authorities lack the legal competence and necessary expertise to address these problems.[188] Likewise, the Author shares the view that competition enforcement should not be entrusted with the obligation to consider pure data protection and privacy concerns without a nexus to any form of economic efficiency-related competition concern, as it may pave the way for competition enforcement to end up examining any public policy concern that is somehow related to a merger (*e.g.* environmental considerations, public security, employment etc.) and thereby to deviate from its primary goal, that is to ensure effective competition in the market.[189]

[184] See decisions in *supra* Section 2.3. See also Margrethe Vestager, European Commissioner for Competition, Competition in a Big Data World, Address Before the DLD 16 Conference (January 17, 2016) stating that "I do not think we need to look to competition enforcement to fix privacy problems."

[185] Some of them argue that as a broader public policy objective, the Commission has a positive duty to promote the effective application of the fundamental rights provided by the EU Charter of Fundamental Rights, including the rights to privacy and data protection, when exercising its competences, see Costa-Cabral and Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (n 12); Kuner, Cate, Millard, Svantesson and Lynskey 'When Two Worlds Collide: the Interface between Competition Law and Data Protection' (n 33). Articles 7 and 8 of the Charter of Fundamental Rights of the European Union set out the rights to privacy and data protection, respectively. Pursuant to Article 51 of the Charter, the EU institutions "[…] shall therefore respect these rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties", see Charter of Fundamental Rights of the European Union [2016] OJ C 202/389.

[186] The EDPS advances its position based on the consumer welfare standard as one of the main goals of the EU competition law, and suggests developing "a concept of consumer harm, particularly through violation of rights to data protection, for competition enforcement in digital sectors of the economy." EDPS 2014 (n 17) 32. For the consumer welfare standard as a competition goal. See *supra* footnotes 49 and 50.

[187] Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25); Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10).

[188] Craig, 'Big Data and Competition – Merger Control Is Not the Only Remedy for Data Protection Issues' (n 34); Gilbert and Pepper 'Privacy Considerations In European Merger Control: A Square Peg For A Round Hole' (n 34); Colangelo and Maggiolino 'Data Protection in Attention Markets: Protecting Privacy Through Competition?' (n 34); Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision' (n 34); Hoffmann and Johannsen, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (n 176) 34-40.

[189] The Thesis does not attempt to examine this normative discussion in detail. It rather aims at providing a brief explanation on the current state of play.

### 3.3.2 Data Protection as a Normative Tool for the Competition Assessment

Having zoomed in on the relationship between competition and data protection law, one could see that their interaction works on two sides: both regimes can equally complement each other.[190] In the context of mergers, the EU data protection rules can provide normative guidance for the "qualitative" assessment of the effects of privacy-based competition.

In that respect, it is considered that data protection rules can serve as an element of legal context for determining anti-competitive conducts.[191] Accordingly, violation of the data protection rules by, for instance, harvesting too much data from individuals, may imply exploitative conduct in the realm of competition law. Caution should be devoted here not to simultaneously qualify any potential violation of data protection rules as competition law violations.[192] This approach, however, entails a challenge in the context of the forward-looking merger assessment as it may be challenging to predict ex-ante that the merged entity will degrade privacy.[193] Notwithstanding, by deriving inspiration from the *Tetra Laval* case,[194] the Commission should scrutinise the possible post-merger privacy conditions to assess whether the merger incentivises or makes it possible for the merged entity to engage in abusive conduct.[195]

---

[190] Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 200.

[191] Many commentators based this approach on the Court's statement in *Allianz Hungária*, where it held that the impairment of domestic law provisions could be taken into consideration when examining whether the conduct in question led to restriction of competition by object. See Case C-32/11 *Allianz Hungária Biztositó and Others* [2013] ECLI:EU:C:2013:160, para. 46-47. See Autorité de la Concurrence and Bundeskartellamt (n 3) 23; EDPS 2014 (n 17) 3; Moncuit, 'In Which Ways Should Privacy Concerns Serve as an Element of the Competition Assessment' (n 155) 7; Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 32; Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 359. The Bundeskartellamt's Facebook case also suggests using data protection rules as a normative benchmark for determining whether a dominant firm's exploitative behaviour constitutes abusive conduct. In this case, the Bundeskartellamt cooperated with data protection authorities in examining the matters intersecting with data protection rules, see Press Release Bundeskartellamt 'Bundeskartellamt prohibits Facebook from combining user data from different sources' (n 168) and the official English version of the decision: Bundeskartellamt Decision B6-22/16 (n 168).

[192] Torsten Körber, 'Is Knowledge (Market) Power? On the Relationship between Data Protection, "Data Power" and Competition Law' (2018) 27, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112232> accessed 19 June 2022.

[193] This is indeed what the Commission did in *Facebook/WhatsApp*, by refusing such prediction and referring to the EU data protection rules under which the merged entity would be obliged to refrain such practices post-merger. *Facebook/WhatsApp* (n 16) para. 164, cited from Deutscher, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (n 27) 19. See also Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 37.

[194] *Tetra Laval* (n 169) para. 74. The Court held that the Commission should examine the merger's effect on the likelihood of engaging in abusive conduct, in particular 'both of the incentives to adopt such conduct and the factors liable to reduce, or even eliminate, those incentives'.

[195] Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 37-38.

The competition enforcers can also draw some insights from the substantive principles of the EU data protection legislation in "measuring" privacy deterioration.[196] To that end, commentators suggested the application of a qualitative test grounded on the core EU data protection principles.[197] Such principles provided in Article 5(1) of the GDPR, also called "data quality requirements"[198] cover the lawful, fair, and transparent processing of personal data, purpose limitation, data minimization, accuracy, storage limitation, and data security. To illustrate, the quality of the merged entity's post-merger privacy policy (predicted based on its past data-related behaviours), which hypothetically requires users to disclose too much data and/or allows the entity to use these data across its entire ecosystem beyond what is necessary to fulfil the initial purpose (*e.g.* for advertising), might be deemed to be degraded given data minimization and/or purpose limitation principles. The test may involve cooperation between competition and data protection authorities to measure the possible impact of a merger on users' privacy as a dimension of quality, as also proposed by the EDPS as part of its "Digital Clearing House" initiative.[199] This is one of the circumstances where positive synergies in the interface between data protection and competition law could be achieved.

### 3.3.3 Scope for Collaboration Between Authorities

Notwithstanding the tendency not to factor pure data protection interests as a discrete consideration in competition analysis, one cannot simply ignore the ever-expanding intersection between the two fields. Indeed, a growing body of literature and institutional reports call for cooperation between competition and data protection enforcers to yield potential synergies in the intersecting areas.[200] Fundamentally, the EU competition and data protection law converge at the level of their goals to

[196] Linking with the previous paragraph, the decrease in privacy protection as a result of a merger might not necessarily violate the EU data protection rules. In this case, data protection rules can still be used as a normative tool for the 'measurement' of privacy deterioration that raises competition concerns.

[197] Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 8; see also Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10) 37; Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 138-139.

[198] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 129.

[199] Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15) 8. For more information on Digital Clearinghouse, see <https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en> accessed 19 June 2022.

[200] Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25); Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31); Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21); Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10); Lynskey, 'Considering Data Protection in Merger Control Proceedings' (n 15); Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58); Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10); Chirita, 'Data-Driven Mergers under EU Competition Law' (n 20); Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (n 93); EDPS 2014 (n 17); EDPS 2016 (n 17); Autorité de la Concurrence and Bundeskartellamt (n 3); OECD, 'Consumer Data Rights and Competition' (n 24) 49-51.

promote consumer welfare and market integration,[201] and ensure "fairness".[202] The notion of fairness could be used as an instrument to facilitate more substantive alignments of data protection and competition rules and their coherent enforcement.[203] Moreover, data protection enforcement is often said to fall short of addressing intrusive data activities by digital conglomerates, which also cause serious market failures, particularly given their increasing takeover trend driven by a desire to access more data. It has been suggested that developing a holistic and integrated approach to merging the rules of competition and data protection is necessary to solve such market failures and promote individuals' privacy in the digital economy.[204] It must be borne in mind that competition law cannot always satisfy specific privacy concerns (as it does not aim to do so) vis-à-vis the shortcomings of data protection enforcement. It is, therefore, more desirable to complement competition enforcement with robust data protection enforcement, and they should be applied in parallel.[205] In this regard, institutions and regulators should rely on a more proactive approach and constantly collaborate if a data privacy-related consumer harm risk arises at the intersection of competition and data protection. Such cooperation would reduce the risk of uncertainty and conflicting outcomes that may stem from the parallel application of the two and further strengthen their coherent enforcement.[206] In this line, the EDPS's Digital Clearing House, a voluntary network of enforcement authorities aiming to ensure greater dialogue for the effective and coherent enforcement of rules protecting individuals, seems promising.[207] As will be discussed in Chapter 4, the scope for cooperation and proactive approach to stimulate higher levels of privacy protection and ensure undistorted competition is of significance, especially in the context of merger remedies whenever a merger raises economic efficiency-oriented competition concerns.[208]

[201] See *supra* Section 2.2.

[202] For an analysis of the notion of fairness and its relevance to the EU competition and data protection law, see Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31). See further, Harri Kalimo and Klaudia Majcher, 'The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace' (2017) 2 European Law Review.

[203] Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31).

[204] Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (n 25); Costa-Cabral and Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (n 10); Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10).

[205] Graef, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' (n 6) 94; Botta and Wiedemann, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (n 58) 444-445; OECD, 'Quality Considerations in Digital Zero-Price Markets' (n 15) 31. As rightly noted, "their relationship is mutually reinforcing", see Information Commissioner's Office ("ICO") & CMA, 'Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO' (May 19, 2021), 30.

[206] Botta and Wiedemann, *Ibid*.

[207] EDPS 2016 (n 17); see *supra* footnote 199.

[208] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 146.

## 3.4 Interim Conclusion

As articulated by the Commission and literature, data privacy considerations can be included in merger assessments as part of substantive competition analysis as a (i) non-price competition parameter, and (ii) limit preventing competition concerns from arising. Integrating privacy as a competition parameter into competition analysis carries at least two potential implications: (i) it allows competition enforcers to focus on more direct harm to consumers in the form of exploitation of the accumulated data by the merged entity, and (ii) supports defining a relevant market for data. Yet, it also faces challenges due to the debate on the lack of privacy competition and difficulties in measuring privacy degradation. Regarding the use of data protection rules as a limit, it is seen that the Commission has opted for a more cautious approach when assessing the -ostensible- ability of such rules to limit anti-competitive effects of mergers.

In contrast, data protection and privacy interests as a discrete concern beyond substantive competition assessment are predominantly excluded from the sphere of competition law. Nevertheless, the literature calls for (i) competition and data protection authorities to collaborate and join forces against the harmful activities of big tech firms, and (ii) using data protection rules as normative guidance in the assessment of novel data and privacy-related competition harms.

# 4 DESIGNING A WAY OUT: MERGER REMEDIES

## 4.1 Introduction

Having identified the instances where data protection could be relevant to merger assessments, one might question the potential for including data protection and privacy in merger remedies to promote their effectiveness that would otherwise be put in jeopardy by the consummation of a data-driven merger. This Chapter thus seeks to answer: *How should merger remedies be designed to promote the integration of data protection and privacy considerations into merger assessments?*

The Chapter will first scrutinize the merger remedies' framework in EU Competition Law to determine whether there is a scope for the Commission to include data protection and privacy in remedies as a condition for merger approval. Further, it will develop a three-fold proposal for designing merger remedies involving data protection and privacy interests.

## 4.2 The EU Legal Framework for Merger Remedies

Merger remedies aim at reconstructing competition in the market following a concentration in a fine-tuned manner to reap some of the benefits associated with the concentration while keeping the market competitive.[209] Under the EUMR, the Commission may take three positions in reviewing a concentration: to allow,[210] to prohibit,[211] or to clear the transaction subject to modifications.[212] When a proposed concentration raises concerns in that it may significantly impede effective competition, the merging parties may offer commitments (remedies) to address specific competition concerns raised by the Commission and thereby obtain clearance.[213] Remedies can be proposed in either Phase I or Phase II, or (informally) even before the notification of the concentration.[214] Although an immaterial categorization,[215] the commitments may take the form of structural remedies (*i.e.* involving permanent one-off change like divestiture) or behavioural remedies (*i.e.* mix of remedies requiring ongoing implementation and remedies sharing similarities with one-off structural ones: *e.g.* commitments to behave in a particular manner, obligations to provide access to critical assets, license key technology, establish a firewall, etc.).[216]

[209] Ariel Ezrachi, 'Behavioral Remedies in EC Merger Control - Scope and Limitations' (2006) 29(3) World Competition 459.
[210] The EUMR Articles 6(1) and 8(1).
[211] The EUMR Article 8(3).
[212] The EUMR Articles 6(1)(b), 6(2) and 8(2).
[213] European Commission, Commission Notice on Remedies Acceptable under Council Regulation (EC) No 139/2004 and under Commission Regulation (EC) No 802/2004, 2008/C 267/01, (hereinafter "the Commission Notice on Remedies") para. 18.
[214] The EUMR Articles 6(2) and 8(2), and the Commission Notice on Remedies, *Ibid,* para. 78, respectively.
[215] Case T-102/96 *Gencor v Commission* [1999] ECR II-753, para. 319.
[216] Ezrachi, 'Behavioral Remedies in EC Merger Control - Scope and Limitations' (n 209) 460.

Regarding the nature of acceptable commitments, the EUMR only provides that commitments should be proportionate to the competition concern and be capable of eliminating it.[217] The scope of this proportionality principle needs to be clarified. In this regard, one should distinguish between remedies imposed unilaterally by the Commission in prohibition decisions (coercive remedies) and remedies offered by the undertakings themselves in commitment decisions (voluntary remedies).[218] The Court in *Alrosa* stated that the proportionality principle applies to both coercive and voluntary remedies, yet the extent to which it applies differs depending on whether it relates to the former or the latter.[219] Accordingly, remedies in prohibition decisions must be proportionate to the competition concern, whereas the commitments voluntarily offered by the undertakings can go beyond what is required to address the competition concerns to maintain the market structure in the future. Within the merger context, as it is for the merging parties to propose commitments to convince the Commission that the transaction would be compatible with the internal market,[220] the Court's approach should also apply to commitments offered during a merger review.[221] Indeed, the "weaker nexus" between the merger remedies and the competition concerns raised might be explained because the merger remedies are voluntary and consensual in nature, negotiated between the parties and the Commission.[222] Considering that the Commission has broad discretion in assessing the adequacy of the commitments offered by the parties and the final say in accepting them,[223] it could, as part of the remedy negotiations, demand measures that not only focus on eliminating efficiency-oriented competition concerns but also address data protection and privacy interests harmed by the concentration. This makes it possible for the Commission to apply the remedies provided in Section 4.3.2 with a view to promoting the effectiveness of data protection and privacy whenever a merger raises competition concerns.

[217] The EUMR Recital 30.

[218] Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 343-344; Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (n 17) 511. For a critical assessment of coercive and voluntary remedies dichotomy, see Ioannis Lianos, 'Competition Law Remedies in Europe' in Lianos and Geradin (eds) *Handbook on Competition Law – Enforcement and Procedure* (Edward Elgar Publishing 2018), 438-454.

[219] Case C-441/07 P *European Commission v Alrosa Company Ltd.* [2010] ECR I-6012, para. 38-48.

[220] The Commission Notice on Remedies (n 213) paras. 2 and 19. It is nevertheless argued that the commitments are often either dictated or influenced by the Commission, see Hoffmann and Johannsen, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (n 176) 50 (and footnotes 140-141).

[221] Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (n 17) 511, footnote 153; Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 343, 344 and 353.

[222] Lianos, 'Competition Law Remedies in Europe' (n 218) 370.

[223] Case T-158/00 *Arbeitsgemeinschaft der öffenthlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland (ARD) v Commission* [2003] ECR II-3825, para. 328. Indeed, judicial review of the Commission's remedial discretion in merger cases is rather limited, see Lianos, 'Competition Law Remedies in Europe' (n 218) 422-425. The General Court also admitted that 'the Commission may have exercised a certain influence on the terms of the commitments proposed by the parties' Case T-282/02 *Cementbouw Handel & Industry v. Commission* [2006] ECR II-331, para. 314.

## 4.3 The Proposal for Designing Merger Remedies Involving Data Protection and Privacy Interests

Building upon the above considerations and deriving inspiration from Graef's work[224] and the *Google/Fitbit* decision, this Section suggests that there is room for the Commission to apply merger remedies promoting data protection and privacy interests and discusses how to do design such remedies, through a three-fold Proposal.

### 4.3.1 First Phase: Establishing the Merger-Specific Competition Concern

The determinant factor in testing the merger's compatibility under the EUMR is whether the transaction would significantly impede effective competition, particularly due to the creation or strengthening of a dominant position.[225] Accordingly, if a notified merger does not lead to a significant impediment to effective competition, the Commission has no power but to clear the merger and leave non-efficiency interests untethered to competition aside. This is in line with the inherent logic of competition law: "[t]he application of competition law is thus only triggered in the presence of actual, proven competition problems".[226] Thus, per the first phase, one shall establish that the merger raise competition concerns in that it could significantly impede effective competition so that the Commission could impose remedies and thereby factor non-efficiency interests such as data protection therein. As explained in Section 4.2, the competition concern identified may not necessarily cover specific data protection concerns to be addressed through novel remedies proposed below due to the weaker nexus between the remedy and the concern factored therein.

This phase is also of significant use in deciding which type of remedies involving data protection interests should be applied. In particular, if the merger raises privacy-related competition harm (*e.g.* privacy quality degradation post-merger), having a well-structured theory of harm would help to pinpoint exactly where the privacy harm occurs and how the remedies should address it.

### 4.3.2 Second Phase: Designing Remedies that also Further Data Protection and Privacy Interests

As part of the second phase, the design of a remedy addressing efficiency concerns arising from a data-driven merger shall be made in a way to also promote data protection and privacy interests that would be harmed following the consummation of the merger. That said, designing ex-ante remedies satisfying such concerns is a difficult task to undertake. The need for a case-specific

[224] Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35); Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21).
[225] The EUMR Articles 2(2) and 3.
[226] Graef, Clifford and Valcke, 'Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law' (n 31) 210.

approach[227] becomes even more apparent given the high dynamics and lack of predictability of digital markets. Keeping this in mind, this Section suggests (non-exhaustive) general and example-based remedies that could be tailored according to the specific context of each merger (*i.e.* in which particular way the merger may adversely affect consumers' privacy).

### i. Remedies Involving Data Use Restrictions

The first option vis-à-vis the combination of the merging parties' datasets might be a remedy restricting the use of parties' data across different businesses of the merged entity for incompatible purposes.[228] Such remedy may require maintaining the data held by the merging parties separately post-merger or creating a firewall between them.[229] This type of remedy is expected to become prevalent following the *Google/Fitbit* decision, where the Commission accepted a data silo remedy requiring the creation of a silo for storage of Fitbit health data separately and prohibiting Google from using such data for advertising purposes. It must be noted that the data silo remedy in *Google/Fitbit* has been put forward for the sole purpose of eliminating the merger's adverse effect on competition stemming from the data combination.[230] On the other hand, since these datasets mostly also include personal data, keeping the merging entities' data in a silo would also prevent users' data from being combined and used across different businesses of the merged entity. Therefore, a remedy involving data use restrictions post-merger due to efficiency concerns would, at the same time, rectify likely data protection concerns arising from the use of personal data beyond the purpose for which it was initially collected. This would be in line with the GDPR's purpose limitation principle, which limits further processing of personal data other than for the purpose it was specifically collected.[231] This would also comply with the provision restricting data combination in the draft Digital Markets Act, which introduces ex-ante regulatory obligations for "gatekeepers" in digital markets.[232]

---

[227] The Court stressed the need for a case-by-case examination of the commitments offered by the merging parties: *Gencor v Commission* (n 215) para. 320.

[228] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 146; EDPS 2014 (n 17) 32; OECD, 'Consumer Data Rights and Competition' (n 24) 39.

[229] In the US, the remedy of this kind has been proposed by the former FTC Commissioner Pamela Jones Harbour in her dissenting statement in the FTC's *Google/DoubleClick* decision, see 'Dissenting Statement of Commissioner Pamela Jones Harbour: In the Matter of Google/DoubleClick FTC 2007 No. 071-0170' (n 91). In the *Ticketmaster/Live Nation* merger, the FTC and the merging parties agreed to create a firewall between the parties' certain datasets as a condition for merger approval, see Department of Justice, 'Justice Department Requires Ticketmaster Entertainment Inc, to Make Significant Changes to Its Merger with Live Nation Inc.' January 25, 2010, see <https://www.justice.gov/opa/pr/justice-department-requires-ticketmaster-entertainment-inc-make-significant-changes-its> accessed 19 June 2022. Yet, it should be noted that in both cases, the idea behind keeping datasets separately post-merger was solely based on the elimination of the merger's anticompetitive effects.

[230] *i.e.* data-related competition concerns, see *supra* Section 3.2.1.

[231] The GDPR Article 5(1)(b).

[232] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)" COM(2020) 842 Final, 15 December 2020, Article 5(a).

Such remedy may involve "loose" data use restrictions (*e.g.* Fitbit's health data will not be used for Google Ads) or "stricter" data use restrictions (*e.g.* Fitbit's health data will not be combined with any characterization of Google's non-health data not only in advertising but also in health data and insurance markets).[233] Even if the Commission in *Google/Fitbit* deemed the loose restrictions to be sufficient to sweep away data-related foreclosure concerns in online advertising, one may claim that the possibility for Google to exploit users in health data and insurance markets has remained. The Commission should have gone further than restricting the use of data for only a specific business of the merged entity by taking a more holistic approach to likely consumer harms anticipated in the markets other than advertising. As discussed, the Commission could also resort to stricter data use restrictions for the sake of promoting data protection interests as the competition concern was already present.

### ii. Sui Generis Remedies Reinforcing Compliance with the GDPR

Secondly, in a more general manner, where the merger involves firms holding sets of personal data, it may be desirable to implement a remedy reinforcing the merging entities' data protection law obligations. The idea behind this remedy is to provide consumers greater control over the use of their data, which could potentially cure many of the exploitative consumer harms.[234] One may claim that the undertakings are already obliged to comply with the EU data protection law, so there is no point in integrating such rules into competition remedies. Yet, as mentioned, consumers often face hurdles when performing control over their data due to, in particular, the imbalance between their privacy rights and the firms' disclosure activities, and the GDPR often suffers from the lack of proper enforcement by data protection authorities. It may be helpful to apply the GDPR obligations as a mandatory minimum in merger remedies and exceed this threshold to strengthen them when necessary.[235] In this way, stronger data protection obligations could be imposed on firms with market power, thereby cementing the asymmetric enforcement of the data protection rules. Contrary to what the Commission assumed, data protection rules could not exert forceful limitations to prevent competition problems from occurring.[236] Hence, such a remedy might prove to be an efficient tool from at least two perspectives: (i) fostering the existing data protection law obligations through well-enforced competition remedies, and (ii) safeguarding effective competition vis-à-vis exclusionary and exploitative harms arising from the data concentration instead of referring to data protection rules that could supposedly prevent such harms.

---

[233] During the Phase II analysis of the *Google/Fitbit* transaction before the Commission, a group of commentators called for the need for more extensive remedies (in addition to data silo remedy in relation to the online advertisement market) including data use restrictions (i) preventing the combination of health data with any characterization of Google's non-health data in health data and insurance markets, and (ii) requiring that Google can only use Fitbit data for health data and insurance applications: see Bourreau et al, 'Google/Fitbit will monetise health data and harm consumers' (n 95) 9.

[234] *i.e.* privacy-related exploitative theories of consumer harm, see *supra* Section 3.2.2.

[235] Botta and Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (n 35) 475.

[236] See *supra* Section 3.2.3.

There may be various illustrations of this type of remedy, particularly centring around consent. To exemplify, a remedy may mandate an obligation to obtain opt-in,[237] specific and informed[238] consent from users for transferring their data between the merged entities' businesses following the merger or later processing them across these businesses.[239] It might be accompanied by the obligation to provide information about the processing and use of their personal data periodically. This raises transparency and users' awareness of what is happening with their data and nudges them to take action. One should also make sure that service use is not made conditional on giving consent.[240] One step further, a remedy may include a "double opt-in" requirement whenever the merged entity post-merger wishes to process personal user data in a manner that goes beyond the legitimate expectation of a regular user.[241] To further strengthen the consent, a periodic reminder (*e.g.* monthly or annually) asking users to renew their consent could be deployed.[242] The *Google/Fitbit* decision demonstrates the use of a consent-reminder remedy requiring Google to provide users with "an effective choice to grant or deny the use of health and wellness data" by other Google services.[243]

Further examples may include a remedy mandating that the merged entity provides more privacy options so users can craft their privacy preferences for a given service per how much they value their privacy. For instance, users could be offered an option to pay a fee for a service in return for

[237] According to the GDPR, data subjects must always be actively opt-in - "by a clear affirmative action" - to give their consent. Thus, silence, pre-ticked boxes, or inactivity do not constitute valid consent. See the GDPR Article 4(11) and Recital 32.

[238] The GDPR Article 4(11). Accordingly, consent must be freely given, specific, informed, and unambiguous. For an analysis of these criteria, see 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) A Commentary* (Oxford University Press 2020), 181-185.

[239] A similar remedy was applied by the Colombian competition authority in the context of the review of a joint venture between the three largest banks of Colombia. As a condition for approving the proposed transaction, the joint venture was required to comply with the relevant data protection obligations and to obtain consent from customers prior to transferring their personal data from their banks to the joint venture. Cited from Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (n 93) 140-141 and OECD, 'Merger Control in Dynamic Markets – Contribution from Colombia' 6 December 2019 (DAF/COMP/GF/WD(2019)21), 2-3.

[240] This is referred to as the 'take-it-or-leave-it' choices, which undermines the 'freely' given nature of valid consent. See the GDPR Articles 4(11) and 7(4), and Frederik J Zuiderveen Borgesius, Sanne Kruikemeier, Sophie C Boerman and Natali Helberger, 'Tracking Walls, Take-it-or-leave-it Choices, the GDPR and the ePrivacy Regulation' (2018) 3(3) European Data Protection Law Review 353. The take-it-or-leave-it choices are also relevant to competition law in the sense that "limited 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", which results in providing more personal data to platforms than users would have wanted under competitive market conditions: see CMA, 'Online Platforms and Digital Advertising Market Study' 1 July 2020, 8. See also Bundeskartellamt Decision B6-22/16 (n 168) 185-187.

[241] Botta and Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (n 35) 476. According to the authors, a double opt-in method could be that "users have to actively change their privacy preferences (step 1), and then they have to confirm the new settings by clicking on a link that has been sent via e-mail".

[242] Bourreau et al, 'Google/Fitbit will monetise health data and harm consumers' (n 95) 9; Botta and Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (n 35) 476.

[243] As a data silo remedy only prevents usage of Fitbit's health and wellness data for advertising (and not for any other Google services, like Google Maps, Google Assistant, YouTube, etc.).

reduced collection and retention of personal data.[244] This would not only reinforce the GDPR's primary goal to enhance individuals' control over their data but also foster privacy competition in the market by increasing user choice concerning privacy. Notwithstanding, from a moral perspective, pricing privacy may be questionable as it may allow rich people to buy more privacy while poor cannot.[245]

The solutions applied within the scope of data protection enforcement can be a source of inspiration for designing novel merger remedies. An example would be the "compare and forget" method implemented by the Dutch data protection authority in its investigation into WhatsApp.[246] Accordingly, WhatsApp was only granted short-term and read-only access to its users' contact lists to help them identify which of their contacts were already using WhatsApp. After identification, WhatsApp had to delete the contact information immediately. In the context of data-driven mergers, this method could help eliminate the foreclosure effect stemming from the combination of datasets (*i.e.* by limiting the merged firm's ability to access more data via its enlarged datasets and to gain a competitive advantage vis-à-vis existing rivals and by levelling the field for newcomers to be able to compete). It could also limit the potential excessive data retention and collection, in line with the data minimization principle,[247] thereby preventing long-term consumer privacy harm.

It goes without saying that remedies of this kind should be applied without prejudice to the enforcement of the GDPR. In practice, the design, monitoring, and implementation of these GDPR-reminder remedies can be carried out in collaboration between the competition and data protection authorities, as will be discussed in Section 4.3.3. This would help to alleviate any confusion regarding the enforcement of such remedies (*e.g.* risk of double punishment in breach of *ne bis in idem*) and allow the data protection authorities to provide guidance and expertise to competition authorities as the latter are neither well-equipped nor experienced to deal with data protection concepts and problems.

[244] EDPS 2014 (n 17) 32. It must be noted though that the opposite (*i.e.* offering a service for free or a reduced fee in return for much more excessive data disclosure activities) can only be implemented to the extent that it is allowed by the existing data protection rules.
[245] Malgieri and Custers, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (n 153) 12.
[246] EDPS *Ibid*; Dutch Data Protection Authority, 'Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc.: Report on the definitive findings' (English Translation) January 2013, 30, see <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-whatsapp-dutchdpa-final-findings-en.pdf> accessed 19 June 2022.
[247] The GDPR Article 5(1)(b); Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (n 17) 510.

### iii. Data Portability Remedy

Having both competition and data protection law dimensions,[248] data portability might be a rather promising concept to use in the context of merger remedies. In the simplest term, data portability allows users to move their data from one firm to another. From the data protection law perspective, it aims at strengthening individuals' control over their data;[249] whereas regarding the competition law, it helps to neutralize consumer lock-in effects fuelled by switching costs and strong network effects in online platforms by facilitating their switch to competing platforms, thereby promoting effective competition.[250] A merger remedy requiring data portability might also prevent the merged entity from engaging in consumer exploitation post-merger in the form of excessive data collection or retention.[251]

The Commission in *Microsoft/LinkedIn* and *Google/Sanofi* referred to the GDPR's data portability right that could limit the merged entity's invasive data activities and consumer lock-in.[252] As discussed, the Commission should not rely on the GDPR's (insufficient) ability to prevent competition concerns,[253] instead, it should proactively step in by mandating the data portability as a condition for merger approval if necessary.[254] Besides, where a merger raises particular data protection concerns that could be cured by data portability (even if such concern does not also amount to an efficiency-related competition concern), it would still be possible and desirable to guarantee the right's effective implementation through well-enforced competition remedies. Moreover, a merger remedy mandating data portability might go further than what is provided under Article 20 of the GDPR, which only covers the portability of "personal" data "provided" by the data subjects. Considering the big data debate and the ability of tech giants to harvest data through various techniques without recourse to the very owner of data,[255] inferred or derived data by these firms may also be of significant value and a potential source of concern.[256] Thus, one could widen the scope of the merger remedy mandating data portability to any type of data,

[248] Inge Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union' (2015) 39 Telecommunications Policy 502. See further, Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42(6) European Law Review 793. The right to data portability is provided under Article 20 of the GDPR which states that 'The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided […]' and '[…] the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible'.
[249] The GDPR Recital 68.
[250] Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union' (n 248) 507; EDPS 2014 (n 17) 32.
[251] Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (n 17) 511.
[252] *Microsoft/LinkedIn* (n 16) para. 178; *Sanofi/Google/DMI JV* (n 176) paras. 67-69.
[253] See *supra* Section 3.2.3.
[254] Graef, 'The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation' (n 180) 7.
[255] Autorité de la Concurrence and Bundeskartellamt (n 3) 6-7.
[256] Graef, 'The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation' (n 180) 7.

whether it be provided, inferred, derived, or even non-personal data. Notwithstanding, particular care should be devoted here not to upset the merging parties' incentive to collect data that may bring along efficiencies, so a case-by-case analysis is required to create a balance in determining the type of the data subject to portability. Furthermore, as part of a merger remedy, the Commission may require the merged entity to develop an IT system fostering technical "interoperability" between platforms to transfer data in a structured, commonly used, and machine-readable format.[257]

### iv. Tensions with the Data Access Remedy

Data access remedies, including compelled access to data, duplicating the relevant datasets, and divestiture of data to a third party, might be an effective tool in eliminating the anti-competitive effects of data concentration in the form of foreclosing rivals from data access.[258] This was the case in *Thomson/Reuters*, where the merging parties were required to sell copies of their databases, including personal information.[259] Nevertheless, if the datasets to be shared involve personal data, an efficiency-oriented data access remedy may generate "tensions" with data protection law in the sense that disclosing personal data to third parties requires a lawful basis per Article 6 of the GDPR and has to comply with the GDPR's data protection principles.[260] Thus, such remedies should be designed "in a way that aligns with data protection law"[261] by clearly demonstrating a lawful basis for disclosure and requiring compliance with the data protection principles.

It may be that the imposition of a merger remedy requiring disclosure of personal data is considered a legal obligation or such remedy is necessary for the purposes of the data controller's legitimate interests per Article 6(1)(c) and (f) of the GDPR, thus putting the data processing on a lawful

[257] This is because, per the GDPR, users can request from the data controller to transfer their data directly to another controller only if it is technically feasible. Thus, there is no legal obligation for the controllers to set up such a system. The GDPR Recital 68 only states that "Data controllers should be encouraged to develop interoperable formats that enable data portability". Nevertheless, it should be noted that competition remedies may only impose individual interoperability requirement for a given case. In order for interoperability to work, other undertakings would still need to implement a similar interconnection technology. See Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union' (n 248) 510. See also the 'Data Transfer Project' contributed by some of the big tech companies like Apple, Facebook, Google, Microsoft, Twitter in an effort to create common framework with open-source code that can allow user-initiated direct data portability between the two platforms, <https://datatransferproject.dev> accessed 19 June 2022.

[258] Schepp and Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (n 113) 123; Hoffmann and Johannsen, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (n 176) 56-62 (analysing the data sharing remedy in the context of both exclusive -*i.e.* unique and indispensable for specific services- and non-exclusive data); Crémer et al., *Competition Policy for the Digital Era* (n 24) 99.

[259] *Thomson/Reuters* (n 61).

[260] Graef, Tombal and Streel, 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' (n 119) 26-30. As the authors point out, demonstrating a lawful basis for data access remedy is expected both from the undertaking sharing the data and the undertaking receiving the data. See also ICO & CMA, 'Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO' (n 203) 23-24; Autorité de la Concurrence and Bundeskartellamt (n 3) 18.

[261] ICO & CMA, *Ibid* 23. See also, Furman et al., *Unlocking digital competition, Report of the Digital Competition Expert Panel* (n 24) 74.

footing.[262] What is more desirable to better accommodate data protection interests and empower individuals to control their data is to require obtaining consent -as a lawful basis- from the individuals whose data is at stake as part of a data access remedy. The Autorité de la Concurrence's *GDF Suez* case might serve as an example.[263] The interim remedy imposed on GDF Suez, a dominant gas company, involved a duty to share its customers' personal information with rivals. The Autorité de la Concurrence implemented a system allowing the customers to opt-out of disclosing their information to other companies.[264] As the GDPR has strengthened the consent by requiring individuals to explicitly opt-in for processing,[265] future remedies of this kind should require opt-in consent before disclosing personal data to rivals. Nevertheless, it should be noted that considering the significant number of customers opting out from data transfer in *GDF Suez*, it may be that there would be even lesser numbers of data subjects who actively opt-in to give their consent to data transfer. [266] In this case, opt-in consent requirement may defeat the purpose of compelled data access remedy, significantly decrease its efficiency and may not be applied. Still, another lawful basis (*e.g.* Article 6(1)(c)/(f)) should be demonstrated.

Irrespective of the type of lawful basis, these remedies should still be accompanied by safeguards in line with the GDPR's principles.[267] For instance, personal data subject to disclosure must be strictly limited to what is necessary to fulfil the purpose according to the data minimisation principle, and processed in a manner compatible with the initial purpose per the purpose limitation principle. Moreover, the individuals whose data is subject to disclosure must be informed about the further processing based on a new purpose.[268]

A successful example of designing data access remedies in a way to eliminate tensions with data protection law is found in *Google/Fitbit*. Under the Web API access remedy, providing access to supported measured body data for API users must be subject to user consent as required under the GDPR and API users must comply with the "Privacy and Security Requirements".[269] The latter

[262] Graef, Tombal and Streel, 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' (119) 28.
[263] Autorité de la Concurrence, Decision No.17-D-06 (GDF Suez) 21 March 2017, <https://www.autoritedelaconcurrence.fr/fr/decision/relative-des-pratiques-mises-en-oeuvre-dans-le-secteur-de-la-fourniture-de-gaz-naturel> accessed 19 June 2022.
[264] At the time when this decision was taken, the GDPR had not yet entered into force. Thus, an opt-out remedy might have been seen as appropriate back then, see Graef, Tombal and Streel, 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' (119) 28.
[265] The GDPR has introduced a new criterion for consent: consent must be given by a clear affirmative action or by a statement. This requires a deliberate action by the user to actively opt-in. See the GDPR Article 4(11) and Recital 32. See also *supra* footnote 237.
[266] Vikas Kathuria and Jure Globocnik, 'Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy' (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-04, 28-29.
[267] As set out in Article 5 of the GDPR. See Graef, Tombal and Streel, 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' (119) 11-12, 30; also EDPS 2014 (n 17) 32.
[268] As per Articles 12, 13 and 14 of the GDPR.
[269] *Google/Fitbit* (n 16) p. 229, Commitments to the European Commission, Section A.2.

requirements are rather extensive and provide a higher degree of data protection for those whose data is at stake. Accordingly, access must be minimal and proportionate to what is necessary and limited to a specific purpose; users must be adequately informed about their data being accessed prior to such access; users' express and informed consent must be obtained, and the parties requesting access must comply with data security requirements in handling data.[270] Hence, the Web API access remedy sets out the lawful basis for data sharing (*i.e.* consent) and requires compliance with many of the GDPR's data protection principles (*e.g.* lawful, fair, and transparent processing, data minimisation, purpose limitation, data security).

### 4.3.3 Third Phase: Collaborating with the Data Protection Authorities in the Design and Implementation of the Merger Remedies

As per the third phase, the Commission shall maintain a productive collaboration with the data protection authorities in designing, supervising, and implementing the remedies. In the face of the growing relevance of data protection in competition analysis, commentators and institutions have already been vocal about drafting competition remedies in cooperation and consultation with the data protection authorities.[271] Having a high degree and particular expertise in the field, data protection authorities may inform the design of remedies to minimize their likely adverse impacts on data protection and privacy and shed light on issues that are new to competition enforcers. Examples would be the *GDF Suez* and the Bundeskartellamt's *Facebook* cases,[272] where competition authorities consulted data protection authorities. Noteworthy developments at the national level include the UK Digital Regulation Cooperation Forum[273] and the Dutch Digital Cooperation Platform[274] which aim to ensure greater cooperation and facilitate the exchange of knowledge and expertise between the regulators, including competition and data protection authorities.

---

[270] *Google/Fitbit* (n 16) pp. 242-243, Commitments to the European Commission, Section F.

[271] OECD, 'Executive Summary of the Discussion on Quality Considerations in the Zero-Price Economy – Annex to the Summary Record of the 130th Meeting of the Competition Committee Held on 27-28 November 2018' (DAF/COMP/M(2018)/ANN9/FINAL) 5; EDPS 2016 (n 17) 15; OECD, 'Consumer Data Rights and Competition' (n 24) 40; Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (n 35) 354; Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 146-148; Botta and Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (35) 473; Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (n 93) 143-144. Kira, Sinha and Srinivasan 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (n 10) 17, noting that the establishment of digital or data science units in certain jurisdictions like Australia and the UK might be better equipped for ensuring the implementation of such remedies.

[272] See *supra* footnotes 263 and 168, respectively.

[273] For more information, see Competition and Markets Authority, Information Commissioner's Office, Office of Communications, and Financial Conduct Authority, 'The Digital Regulation Cooperation Forum' (10 March 2021) <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum> accessed 19 June 2022.

[274] For more information, see the Dutch Data Protection Authority, Media Authority, Authority for the Financial Markets, and Authority for Consumers and Markets, 'The Digital Regulation Cooperation Platform (SDT)' (13 October 2021) <https://autoriteitpersoonsgegevens.nl/en/news/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation> accessed 19 June 2022.

Almost all the behavioural remedies provided in the previous section require effective implementation and monitoring mechanisms to ensure that their effect does not decrease over time,[275] as they are prone to circumvention. Without strong implementation and monitoring, behavioural commitments would be nothing but empty promises. Hence, involving data protection authorities further in the implementation of remedies brings along innumerable benefits: it would save the Commission from spending time and incurring costs for monitoring and ensuring compliance with and deterrence of the remedies adopted as the firms would be aware that there are now two authorities watching them on this matter. It would also provide data protection authorities with the "ex-ante" means to proactively monitor firms' compliance with data protection rules and intervene to take pre-emptive measures even before any infringement has occurred.[276] Moreover, as the EU data protection rules are implemented at the national level, it would cure the diverging levels of protection offered throughout the EU by enabling authorities to take unified actions.[277] Eventually, coherent enforcement of the EU data protection legislation would enhance legal certainty surrounding those rules for consumers and companies operating in the EU.

The ways of collaboration vary. Regarding the data silo remedy, the *Google/Fitbit* decision may be a source of inspiration, where Google was required to implement a data protection system to ensure technical separation of the datasets.[278] The relevant data protection authority may be put in charge of establishing and later auditing this technical separation system as it would probably already have more experience with technical restrictions for keeping data separate as part of its compliance mechanism.

The data protection authority can also help the Commission and parties in selecting an independent monitoring trustee(s) and, later on, closely work with the Commission on the matters regarding the monitoring trustee's tasks (*e.g.* evaluation of the periodic reports written by the trustee to assess whether the commitments are being complied with).[279] As a progressive move, the *Google/Fitbit* decision provided that the trustee may share its reports with the Data Protection Commission, in this case, the Irish data protection authority.[280]

[275] The Commission Notice on Remedies (n 213) paras. 13 and 130.
[276] Graef, 'Blurring Boundaries of Consumer Welfare How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' (n 21) 146-149.
[277] *Ibid*.
[278] *Google/Fitbit* (n 16) p. 228, Commitments to the European Commission, Section A.1.3.(d).
[279] For the role and tasks of the monitoring trustee, see the Commission Notice on Remedies (n 213) paras. 117-120. The monitoring trustee is appointed by the merging parties, which will be later subject to the Commission's approval. The Commission has discretion in approving the trustee and assessing whether the proposed candidate is a suitable fit for carrying out the relevant tasks; see the Commission Notice on Remedies (n 213) paras. 124-125.
[280] *Google/Fitbit* (n 16) p. 233, Commitments to the European Commission, Section B.3.26.

One step further, the Commission could nominate a data protection authority as a (one of the) monitoring trustee(s), whom the merging parties would later appoint.[281] It should be noted that there is already scope for the data protection authorities to act as a *de facto* monitoring agent according to the new data protection principle introduced by the GDPR: that of accountability.[282] This means that firms must demonstrate their compliance with the data protection rules when requested. When a merger remedy involving data protection-related commitments is put in place, the relevant data protection authority could extend the merged entity's accountability obligation to demonstrate its compliance with these commitments, as their content would already inherently fall within the scope of the GDPR.

## 4.4 Interim Conclusion

This Chapter proposes that there is room for the Commission to incorporate data protection and privacy interests into merger remedies. The Proposal is threefold: (i) efficiency-oriented competition concerns shall be determined, (ii) remedies addressing such concerns shall be carefully designed in a way that also furthers data protection and privacy interests, and (iii) active collaboration with data protection authorities shall be maintained in designing, implementing, and monitoring such remedies. Regarding the second phase, the Chapter discusses how to design such remedies by taking into account the GDPR and its data protection principles, and provides examples of novel merger remedies.

[281] This might be possible on the basis of the monitoring trustee mandate entered into by the parties and the trustee. To exemplify, the commitment package in Google/Fitbit included a provision allowing the Commission to nominate a monitoring trustee if all the proposed monitoring trustees are rejected by the Commission, see *Google/Fitbit* (n 16) p. 232, Commitments to the European Commission, Section B.1.22.
[282] The GDPR Article 5(2).

# 5 CONCLUSION

This Thesis aims to dig more deeply into the possible inclusion of data protection and privacy in the competition assessment of a merger by bringing a novel angle to the debate through the discussion of merger remedies. It intends to answer: *To what extent should competition authorities integrate data protection and privacy-related considerations into their merger assessments under the EU Competition Law, and how should merger remedies be designed to promote such integration?*

The research first examines: *How do data protection and privacy considerations fit in current merger assessments?* As data-driven mergers expand in the last decade, data and privacy have become increasingly relevant for the substantive analysis of mergers. In parallel, the Commission's assessment of privacy and data-related competition concerns has progressed. In contrast, the Commission has refrained from incorporating pure data protection and privacy interests as a discrete consideration in competition analysis. Furthermore, it is considered that the remedies adopted in *Google/Fitbit* seem to be inspiring for this Thesis' proposal.

Subsequently, it seeks to answer: *What are the arguments advanced to call for the inclusion of data protection and privacy considerations in merger assessments, and what are the possible implications and challenges of such inclusion?* A distinction is made between integrating data protection and privacy (i) as part of substantive competition analysis and (ii) beyond substantive competition analysis as a standalone issue.

It is considered that from the perspective of the Commission and competition literature, data protection and privacy can be integrated into substantive competition analysis: (i) as a non-price parameter of competition and (ii) as a limit preventing anti-competitive effects from arising. Regarding the first point, the privacy-as-competition-parameter concept has been widely acknowledged by the commentators and, to a certain extent, the Commission. Nevertheless, the debate on the so-called lack of privacy competition and the measurement of privacy degradation pose certain challenges that may stand against establishing a robust theory of consumer harm based on the privacy dimension of competition. These difficulties could be overcome by conducting a detailed investigation of the actual consumer preferences regarding the desired privacy options based on the specific characteristics of a given market and products/services offered therein, and by using data protection rules as normative guidance in gauging the privacy quality, in addition to economic-oriented competition tools. The integration of privacy into competition assessment as a dimension of competition significantly contributes to delivering a complete analysis of a data-driven merger's effect on the market, including direct harm to consumers following the potential exploitation of the accumulated data by the merged entity, and supports defining a relevant market for data. Overall, the privacy and data-related competition theories of harm are still nascent, and there is room for development. On the second point, one could see that the Commission has

implicitly departed from its reliance on the ostensible ability of data protection rules to address data-related competition concerns and that it has desirably started to treat the ability of such rules more cautiously.

Given the ever-growing role of data in the digital economy bringing the boundaries of competition and data protection much closer, it is now time to leave aside the debate over which field of law should take the lead to provide the most effective solution to the problems of the digital markets. Rather, one should focus on the intersecting areas where potential synergies could be achieved. In the context of the greater inclusion of data protection and privacy beyond substantive competition assessment, there is indeed scope for (i) competition and data protection authorities to collaborate and join forces against the harmful activities of big tech firms and (ii) using data protection rules as normative guidance in the assessment of data-related competition theories of harm and merger's impact on users' privacy as a dimension of competition.

The research lastly analyses: *How should merger remedies be designed to promote the integration of data protection and privacy considerations into merger assessments?* After examining the EU legal framework for merger remedies, it is concluded that there is a scope for the Commission to include data protection and privacy in remedies as a condition for merger approval. Thus, the Thesis suggests a three-fold Proposal.

In this regard, one shall first establish that the merger raise competition concerns in that it could significantly impede effective competition so that the Commission could impose remedies and thereby factor non-efficiency interests such as data protection therein. The second phase provides a list of possible remedies addressing data protection and privacy considerations that may stem from a data-driven merger. Per the third phase, it is suggested that the Commission shall maintain a productive collaboration with the data protection authorities in designing, supervising, and implementing the remedies. The data protection authorities' expertise shall inform and enlighten the latter steps.

Hence, the Proposal suggests that when a data-driven merger raises competition concerns, the Commission may and should incorporate protection and privacy into merger remedies to protect and promote the effectiveness of these rights that would otherwise be jeopardised due to the merger. As mentioned, this has already been discussed -although in a limited scope- in the literature. As for the ways of doing this, the research provides examples of novel merger remedies, which have been unexplored in the literature, and thus, make the Proposal different from the others. The Proposal contributes to the existing literature by illustrating possible novel merger remedies in which data protection interests can be promoted (*e.g.* remedies involving data use restrictions, reinforcing compliance with the GDPR, and data portability) and ways to eliminate potential tensions between a competition-oriented merger remedy and data protection law.

For this research, the Proposal means the enlargement of areas of intersection between competition and data protection law, which is to be welcomed. It also means better protection for individuals' privacy, which society has craved for so long in the digital age. Considering their common goals, strengths and weaknesses in identifying and addressing data-driven mergers' effect on the market and individuals' life, it is concluded that data protection and competition law can work in synergy and perfectly complement each other. The Proposal creates one of the occasions where positive synergies and benefits can be achieved through collaboration between the authorities and more proactive competition enforcement.

The research limits itself to analysing data-driven mergers where no efficiency defence for the accumulation of data is discussed. Regarding the competition and data protection interface in the context of mergers, it remains to be studied for the future how competition authorities should strike a balance between data-driven efficiency defences and users' data protection and privacy rights. Caution should be devoted here not to create an efficiency offence. Yet, given the increasing erosion of privacy in the internet age, stakes are higher than ever if competition policy prioritises economic efficiency vis-à-vis the fundamental right to data protection. It remains to be seen how competition enforcers would tread the thin line between such interests.

# Bibliography

**Primary Sources**

**TABLE OF CASES**

**European Court of Justice**

C-12/03 Commission of the European Communities v Tetra Laval [2005] ECR I-987

C-238/05 Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios [2006] ECR I-11125

C-8/08 T-Mobile Netherlands and Others [2009] ECR I-04529

C-501/06 GlaxoSmithKline Services Ltd v Commission [2009] ECR I-09291

C-280/08 P Deutsche Telekom AG v European Commission [2010] ECR I-09555

C-441/07 P European Commission v Alrosa Company Ltd. [2010] ECR I-6012

C-209/10 Post Danmark A/S v Konkurrencerådet [2012] ECR I-0000

C-457/10 P AstraZeneca AB and AstraZeneca plc v. European Commission [2012] ECLI:EU:C:2012:770

C-32/11 Allianz Hungária Biztositó and Others [2013] ECLI:EU:C:2013:160

**General Court**

T-102/96 Gencor v Commission [1999] ECR II-753

T-158/00 Arbeitsgemeinschaft der öffenthlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland (ARD) v Commission [2003] ECR II-3825

T-282/02 Cementbouw Handel & Industry v. Commission [2006] ECR II-331

T-286/09 Intel Corp v Commission [2014] 5 CMLR 9

**European Commission**

COMP/M.4726 Thomson Corporation/Reuters Group Commission Decision [2008] OJ C212/5

COMP/M.4731 Google/DoubleClick Commission Decision [2008] OJ C184/9

COMP/M.4854 TomTom/Tele Atlas Commission Decision [2008] OJ C237/8

COMP/M.5727 Microsoft/Yahoo! Search Business Commission Decision [2010] OJ L24/1

COMP/M.6281 Microsoft/Skype Commission Decision [2011] OJ C341/02

COMP/M.6314 Telefónica UK/Vodafone UK/Everything Everywhere/JV Commission Decision [2012]

COMP/M.7023 Publicis/Omnicom Commission Decision [2014] OJ C84/1

COMP/M.7217 Facebook/WhatsApp Commission Decision [2014]

COMP/M.7337 IMS Health/Cegedim Business Commission Decision [2014]

COMP/M.7813 Sanofi/Google/DMI JV Commission Decision [2016] OJ C112/1

COMP/M.8124 Microsoft/LinkedIn Commission Decision [2016] OJ C388

COMP/M.8180 Verizon/Yahoo Commission Decision [2016]

COMP/M.7932 Dow/DuPont Commission Decision [2017] OJ C353/9

COMP/M.8788 Apple/Shazam Commission Decision [2018] OJ C106/16

COMP/M.9660 Google/Fitbit Commission Decision [2020] OJ C194

**National Case Law**

Pamela Jones Harbour, 'Dissenting Statement of Commissioner Pamela Jones Harbour: In the Matter of Google/DoubleClick FTC 2007 No. 071-0170' (2007) <https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf > accessed 19 June 2022

Autorité de la Concurrence, Decision No.17-D-06 (GDF Suez) 21 March 2017, <https://www.autoritedelaconcurrence.fr/fr/decision/relative-des-pratiques-mises-en-oeuvre-dans-le-secteur-de-la-fourniture-de-gaz-naturel> accessed 19 June 2022

Bundeskartellamt, Decision B6-22/16, 6 February 2019, <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5> accessed 19 June 2022

## TABLE OF LEGISLATION

**European Union Law**

Charter of Fundamental Rights of the European Union [2016] OJ C 202/389

Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) [2004] OJ L 24/1

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Commission Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/7

Commission Guidelines on the application of Article 81(3) of the Treaty [2004] OJ C101/97

Commission Guidelines on the Assessment of Horizontal Mergers under the Council Regulation on the Control of Concentrations Between Undertakings [2004] OJ C31/05

**Legislative Proposals**

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)" COM(2020) 842 Final, 15 December 2020

**Secondary Sources**

**OFFICIAL MATERIAL**

**European Commission**

Commission, 'Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover' (18 May 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369> accessed 19 June 2022

Commission, Commission Notice on Remedies Acceptable under Council Regulation (EC) No 139/2004 and under Commission Regulation (EC) No 802/2004, 2008/C 267/01

Commission Communication, 'Data Protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation" COM(2020) 264 Final, June 24, 2020

Commission, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (6 December 2016) IP/16/4284 <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284> accessed 19 June 2022

Commission, 'Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions' (17 December 2020) IP/20/2484 <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484> accessed 19 June 2022

Crémer J et al, *Competition Policy for the Digital Era* (Final Report, European Commission 2019)

Kuneva M, 'Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling' (Brussels, 31 March 2009 SPEECH/09/156)

Vestager M, European Commissioner for Competition, Competition in a Big Data World, Address Before the DLD 16 Conference (January 17, 2016)

**Others**

Article 29 Data Protection Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' WP 148 00737/EN

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' WP 136 01248/07/EN

Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' Joint Report, 10 May 2016

Bundeskartellamt 'Bundeskartellamt prohibits Facebook from combining user data from different sources' 7 February 2019 <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 19 June 2022

CMA, 'Online Platforms and Digital Advertising Market Study' 1 July 2020

CMA, 'The Commercial Use of Consumer Data, Report on the CMA's Call for Information' (2015)

Department of Justice, 'Justice Department Requires Ticketmaster Entertainment Inc, to Make Significant Changes to Its Merger with Live Nation Inc.' January 25, 2010, see <https://www.justice.gov/opa/pr/justice-department-requires-ticketmaster-entertainment-inc-make-significant-changes-its> accessed 19 June 2022

Dutch Data Protection Authority, 'Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc.: Report on the definitive findings' (English Translation) January 2013 <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-whatsapp-dutchdpa-final-findings-en.pdf> accessed 19 June 2022

EDPB, 'Statement of the EDPB on the data protection impacts of economic concentration' (27 August 2018) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_en.pdf> accessed 19 June 2022

EDPB, 'Statement on Privacy Implications of Mergers, adopted on 19 February 2020' <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf> accessed 19 June 2022

EDPS, 'Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (2016)

EDPS, 'Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014)

Furman J et al, *Unlocking digital competition, Report of the Digital Competition Expert Panel* (March 2019)

Information Commissioner's Office & CMA, 'Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO' (May 19, 2021)

OECD, 'Big Data: Bringing Competition Policy to the Digital Era' 27 October 2016 (DAF/COMP(2016)14)

OECD, 'Consumer Data Rights and Competition' 29 April 2020 (DAF/COMP(2020)1)

OECD, 'Executive Summary of the Discussion on Quality Considerations in the Zero-Price Economy – Annex to the Summary Record of the 130th Meeting of the Competition Committee Held on 27-28 November 2018' (DAF/COMP/M(2018)/ANN9/FINAL)

OECD, 'Merger Control in Dynamic Markets – Contribution from Colombia' 6 December 2019 (DAF/COMP/GF/WD(2019)21)

OECD 'Quality Considerations in Digital Zero-Price Markets' 9 October 2018 (DAF/COMP(2018)14)

OECD, *Start-ups, Killer Acquisitions and Merger Control* (2020) 43-46

OECD, 'The Role and Measurement of Quality in Competition Analysis' 28 October 2013 (DAF/COMP(2013)17) <https://www.oecd.org/competition/Quality-in-competition-analysis-2013.pdf > accessed 19 June 202

**BOOKS**

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) A Commentary* (Oxford University Press 2020)

Chirita A, 'The Rise of Big Data and the Loss of Privacy' M. Bakhoum et al. (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer 2018)

Chirita A, 'Data-Driven Mergers under EU Competition Law' in J Linarelli & O Akseli (eds) *In the Future of Commercial Law: Ways Forward for Harmonisation* (1st ed, Hart Publishing 2019)

Ezrachi A and Stucke M, *Virtual Competition the Promise and Perils of Algorithm-Driven Economy* (Harvard University Press 2016)

Graef I, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer Law International 2016)

Graef I, 'Blurring Boundaries of Consumer Welfare- How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' in M. Bakhoum, B. Conde Gallego, M-O. Mackenrodt, & G. Surblytė- Namavičienė (eds), *Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach* (MPI Studies on Intellectual Property and Competition Law 2018)

Graef I, 'When Data Evolves Into Market Power- Data Concentration and Data Abuse under Competition Law' in Martin Moore and Damian Tambini (eds), *Digital Dominance, The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018)

Hawkes B, 'The Irish DPA and its Approach to Data Protection' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International Publishing 2016)

Lianos I, 'Competition Law Remedies in Europe' in Lianos and Geradin (eds) *Handbook on Competition Law – Enforcement and Procedure* (Edward Elgar Publishing 2018)

O'Donoghue R and Padilla J, *The Law and Economics of Article 102 TFEU* (3rd ed., Hart Publishing 2020)

Padilla J and Ahlborn C, 'From Fairness to Welfare: Implications for the Assessment of Unilateral Conduct under EC Competition Law' in C. D. Ehlermann and M. Marquis (eds), *A Reformed Approach to Article 82 EC* (Oxford, Hart, 2008)

Stucke M and Grunes A, *Big Data and Competition Policy* (Oxford University Press 2016)

Wright D, 'Enforcing Privacy' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International Publishing 2016)

**ARTICLES**

**<u>Peer-reviewed Journals</u>**

Acquisti A, Wagman L and Taylor C, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442

Argentesi E, Buccirossi P, Calvano E, Duso T, Marrazzo A and Nava S, 'Merger Policy in Digital Markets: an Ex-Post Assessment' (2020) 17(1) Journal of Competition Law & Economics 95

Bania K, 'The Role of Consumer Data in the Enforcement of EU Competition Law' (2018) 14(1) European Competition Journal 38

Botta M and Wiedemann K, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (2019) 10(8) Journal of European Competition Law & Practice 465

Botta M and Wiedemann K, 'The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) 64(3) Antitrust Bulletin 428

Bromfield J and Olczak M, 'The Role of the Maverick Firm Concept in European Commission Merger Decisions' (2018) 14(2) Journal of Competition Law and Economics 179

Casadesus-Masanell R and Hervas-Drane A. 'Competing with Privacy' (2015) 61(1) Management Science 229

Colangelo G and Maggiolino M, 'Data Protection in Attention Markets: Protecting Privacy Through Competition?' (2017) 8(6) Journal of European Competition Law & Practice 363

Costa-Cabral F, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (2016) 23 Maastricht Journal of European and Comparative Law 495

Costa-Cabral F and Lynskey O, 'Family ties: the intersection between data protection and competition in EU Law' (2017) 54 Common Market Law Review 11

Custers B et al, 'Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10(4) SCRIPTed 435

Esayas S, 'Data Privacy in European Merger Control: Critical Analysis of Commission Decisions Regarding Privacy as a Non-Price Competition' (2019) 40(4) European Competition Law Review 166

Ezrachi A, 'Behavioral Remedies in EC Merger Control - Scope and Limitations' (2006) 29(3) World Competition 459

Gal M and Rubinfeld D, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' (2016) 80(3) Antitrust Law Journal 521

Gilbert P and Pepper R, 'Privacy Considerations In European Merger Control: A Square Peg For A Round Hole' (2015) 5 CPI Antitrust Chronicle

Golla S, ‘Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR’ (2017) JIPITEC

Graef I, ‘Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union’ (2015) 39 Telecommunications Policy 502

Graef I, ‘Market Definition and Market Power in Data: The Case of Online Platforms’ (2015) 38 World Competition: Law and Economics Review 473

Graef I, ‘The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation’ (2020) (Nov.) CPI Antitrust Chronicle

Graef I, Damian Clifford, and Peggy Valcke, ‘Fairness and Enforcement Bridging Competition, Data Protection and Consumer Law’ (2018) 8(3) International Data Privacy Law 200

Grunes A and Stucke M, ‘No Mistake About It: The Important Role of Antitrust in the Era of Big Data’ (2015) (April) the Antitrust Source American Bar Association

Harbour P and Koslov T, ‘Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets’ (2010) 76 Antitrust Law Journal 769

Haucap J, ‘Data Protection and Antitrust: New Types of Abuse Cases? An Economist’s View in Light of the German Facebook Decision’ (2019) CPI Antitrust Chronicle

Kadar M and Bogdan M, ‘Big Data’ and EU Merger Control – A Case Review’ (2017) 8(8) Journal of European Competition Law & Practice 479

Kalimo H and Majcher K, ‘The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace’ (2017) 2 European Law Review

Kemp K, ‘Concealed Data Practices and Competition Law: Why Privacy Matters’ (2020) 16 European Competition Journal 628.

Kerber W, ‘Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection’ (2016) 639 Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil;

Kira B, Sinha V and Srinivasan S, ‘Regulating digital ecosystems: bridging the gap between competition policy and data protection’ (2021) 00 Industrial and Corporate Change 1

Kokolakis S, ‘Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon’ (2017) 64 Computers & Security 122

Kokott J and Sobotta C, ‘The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law 222

Körber T, 'Is Knowledge (Market) Power? On the Relationship between Data Protection, "Data Power" and Competition Law' (2018) 303 NZKart (for the English version, see <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112232> accessed 19 June 2022)

Kuner C, Cate F, Millard C, Svantesson D and Lynskey O, 'When Two Worlds Collide: the Interface between Competition Law and Data Protection' (2014) 4 International Data Privacy Law 247

Lynskey O, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42(6) European Law Review 793

Lynskey O, 'At the Crossroads of Data Protection and Competition law: Time to Take Stock' (2018) 8(3) International Data Privacy Law 179

Malgieri G and Custers B, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (2018) 34(2) Computer Law & Security Review 289

Manne G and Sperry R, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (2015) 2 CPI Antitrust Chronicle

Newman N, 'Search, Antitrust, and the Economics of the Control of User Data' (2014) 30(3) Yale Journal on Regulation 401

Ohlhausen M and Okuliar A, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 Antitrust Law Journal 121

Parker G, Petropoulos G and Van Alstyne M, 'Platform Mergers and Antitrust' (2021) 30(5) Industrial and Corporate Change 1307

Robertson V, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in an Era of Big Data' (2020) 57 Common Market Law Review 161;

Rubinfeld D and Gal M, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339

Schepp N and Wambach A, 'On Big Data and Its Relevance for Market Power Assessment' (2016) 7(2) Journal of European Competition Law & Practice 120

Sokol D and Comerford R, 'Antitrust and Regulating Big Data' (2016) 23 George Mason Law Review 1129

Stucke M, 'Should We Be Concerned About Data-Opolies?' (2018) 2 Georgetown Law Technology Review 275

Stucke M, 'The Relationship Between Privacy and Antitrust' (2022) Notre Dame Law Review (Forthcoming)

Tucker D, 'The Proper Role of Privacy in Merger Review' (2015) 2 CPI Antitrust Chronicle

Tucker D and Wellford H, 'Big Mistakes Regarding Big Data' (2014) (Dec.) the Antitrust Source American Bar Association

Warren S and Brandeis L, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193

Wasastjerna M, 'The Implications of Big Data and Privacy on Competition Analysis in Merger Control and The Controversial Competition-Data Protection Interface' (2019) 30(3) European Business Law Review 337

Witt A, 'The European Court of Justice and the More Economic Approach to EU Competition Law – Is the Tide Turning?' (2019) 64(2) Antitrust Bulletin 172

Zuiderveen Borgesius F, Kruikemeier S, Boerman S and Helberger N, 'Tracking Walls, Take-it-or-leave-it Choices, the GDPR and the ePrivacy Regulation' (2018) 3(3) European Data Protection Law Review 353

**Others**

Acquisti A, 'The Economics of Personal Data and the Economics of Privacy' (2010) OECD Privacy Guidelines Background Paper 3

Akman P, ''Consumer Welfare' and Article 82EC: Practice and Rhetoric' (2008) 08-25 CCP Working Paper

Bourreau M, de Streel A, and Graef I, 'Big Data and Competition Policy: Market Power, Personalized Pricing and Advertising' (2017) CERRE Policy Report

Bourreau M and de Streel A, 'Big Tech Acquisitions, Competition & Innovation Effects and EU Merger Control' (2020) CERRE Issue Paper 15

Christl W, 'How Companies Use Personal Data Against People: Automated Disadvantage. Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information' (2017) Working Paper by Cracked Labs 28

Clifford D, Graef I, and Valcke P, 'Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2017) CiTiP Working Paper 3

Costa-Cabral F and Lynskey O, 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (2015) 25 LSE Working Papers

De Moncuit A, 'In Which Ways Should Privacy Concerns Serve as an Element of the Competition Assessment' (2018) <https://ec.europa.eu/competition/information/digitisation_2018/contributions/aymeric_de_moncuit.pdf> accessed 19 June 2022

Deutscher E, 'How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets' (2018) 13 EUI Working Papers

Douglas E, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (2021) 40 Temple University Legal Studies Research Paper

Economides N and Lianos I, 'Restrictions on Privacy and Exploitation in the Digital Economy: a Competition Law Perspective' (2019) 5 CLES Research Paper Series

Ezrachi A, 'The Goals of EU Competition Law and the Digital Economy' (2018) BEUC Discussion Paper 4 <https://www.beuc.eu/publications/beuc-x-2018-071_goals_of_eu_competition_law_and_digital_economy.pdf> accessed 19 June 2022

Ezrachi A and Robertson V, 'Competition, Market Power and Third-Party Tracking' (2019) 11 Oxford Legal Studies Research Paper

Ezrachi A and Stucke M, 'The Curious Case of Competition and Quality' (2014) 256 University of Tennessee Legal Studies Research Paper Series

Geradin D and Kuschewsky M, 'Competition Law and Personal Data, Preliminary Thoughts on a Complex Issue' (2013) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088 > accessed 19 June 2022

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' (2019) 024 TILEC Discussion Paper

Hoffmann J and Johansen G, 'EU Merger Control & Big Data, On Data-Specific Theories of Harm and Remedies' (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-05

Kathuria V and Globocnik J, 'Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy' (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-04

Lerner A, 'The Role of "Big Data" in Online Platform Competition' (2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780> accessed 19 June 2022

Lianos I, 'Some Reflections on the Question of the Goals of EU Competition Law' (2013) 3 CLES Working Paper Series

Lynskey O, 'Considering Data Protection in Merger Control Proceedings' (2018) (OECD Non-Price Effects of Mergers DAF/COMP/WD(2018)70)

Ocello E, Sjödin C and Subočs A, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (2015) 1 Competition Merger Brief

Ocello E and Sjödin C, 'Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets' (2017) 1 Competition Merger Brief

Townley C, Morrison E and Yeung K, 'Big Data and Personalized Price Discrimination in EU Competition Law' (2017) 38 King's College Research Paper Series

Van der Sloot B and Zuiderveen Borgesius F, 'The EU General Data Protection Regulation: A New Global Standard for Information Privacy' 6-7 <https://bartvandersloot.com/onewebmedia/SSRN-id3162987.pdf> accessed 19 June 2022

**WEBSITES AND BLOGS**

Bartlett J, *The Data Dialogue* (Demos September 2012) <https://demos.co.uk/project/the-data-dialogue/> accessed 19 June 2022

Bhageshpur K, 'Data is the New Oil – And That's a Good Thing' (Forbes 15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=29d894307304> accessed 19 June 2022

Bourreau M et al, 'Google/Fitbit will monetise health data and harm consumers' (CEPR Policy Insight No 107 Submission to the European Commission September 2020) <https://cepr.org/sites/default/files/policy_insights/PolicyInsight107.pdf> accessed 19 June 2022

Craig R, 'Big Data and Competition – Merger Control Is Not the Only Remedy for Data Protection Issues' (2014) Lexology <https://www.lexology.com/library/detail.aspx?g=0bd8c8f7-2869-4ed8-8606-a11559cbdf41> accessed 19 June 2022

Competition and Markets Authority, Information Commissioner's Office, Office of Communications, and Financial Conduct Authority, 'The Digital Regulation Cooperation Forum' (10 March 2021) <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum> accessed 19 June 2022

Data Transfer Project <https://datatransferproject.dev> accessed 19 June 2022

Dutch Data Protection Authority, Media Authority, Authority for the Financial Markets, and Authority for Consumers and Markets, 'The Digital Regulation Cooperation Platform (SDT)' (13 October 2021) <https://autoriteitpersoonsgegevens.nl/en/news/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation> accessed 19 June 2022

EDPS, Big Data & Digital Clearinghouse <https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en> accessed 19 June 2022

Eroglu M, 'Turkish Competition Board has launched an investigation against Facebook for its recent implementation concerning data sharing preferences' (Istanbul Center for Regulation) <https://www.ic4r.net/2021/02/02/turkish-competition-board-tcb-has-launched-an-investigation-against-facebook-for-its-recent-implementation-concerning-data-sharing-preferences/ > accessed 19 June 2022

Evans D and Zhang V, 'Qihoo 360 v Tencent: First Antirust Decision by the Supreme Court' (2014) Competition Policy International 1, <https://www.competitionpolicyinternational.com/qihoo-360-v-tencent-first-antitrust-decision-by-the-supreme-court/> accessed 19 June 2022

First Amended Complaint for Injunctive and Other Equitable Relief, FTC v Facebook Inc. No. 1:20-cv-03590-JEB (DDC filed August 19, 2021) <https://www.ftc.gov/system/files/documents/cases/ecf_75-1_ftc_v_facebook_public_redacted_fac.pdf> accessed 19 June 2022

Johnson B, 'Privacy No Longer a Social Norm, Says Facebook Founder' (The Guardian 10 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 19 June 2022

Modrall J, 'Google/Fitbit: The EU Commission Misses A Step' (Kluwer Competition Law Blog June 17, 2021) <http://competitionlawblog.kluwercompetitionlaw.com/2021/06/17/google-fitbit-the-eu-commission-misses-a-step/> accessed 19 June 2022

Ofcom, 'Being Online: an Investigation of People's Habits and Attitudes' Ipsos MORI, June 2013 <https://www.ofcom.org.uk/__data/assets/pdf_file/0014/32063/being-online.pdf> accessed 19 June 2022

Statt N, WhatsApp clarifies it's not giving all your data to Facebook after surge in Signal and Telegram users' (The Verge 12 January 2021) <https://www.theverge.com/2021/1/12/22226792/whatsapp-privacy-policy-response-signal-telegram-controversy-clarification> accessed 19 June 2022

Telegram, Durov's Channel <https://t.me/durov/147> accessed 19 June 2022

TRT World, 'Turkish WhatsApp users quit app as demand spikes for other options' (10 January 2021) < https://www.trtworld.com/life/turkish-whatsapp-users-quit-app-as-demand-spikes-for-other-options-43133> accessed 19 June 2022

WhatsApp Privacy Policy (August 25, 2016) <https://www.whatsapp.com/legal/privacy-policy/revisions/20160825?lang=et> accessed 19 June 2022

WhatsApp Privacy Policy (January 4, 2021) <https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page > accessed 19 June 2022