The interface between competition law and data privacy law: violation of privacy as an exploitative theory of harm under Article 102 TFEU

By

Arletta Gorecka

Thesis submitted for degree of Doctor of Philosophy

University of Strathclyde

April 2024

Word count: 97830 words

Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree. The copyright of this thesis belongs to the author under the terms of the United Kingdom Copyright Acts as qualified by University of Strathclyde Regulation 3.50.

Due acknowledgment must always be made of the use of any material contained in, or derived from, this thesis.

Signed: Arletta Gorecka

Data: 30/11/2023

Dedication

For my mum and dad who have taught me how to chase my own dreams and never give up. Thank you.

Acknowledgements

My PhD journey has been one of the most exciting periods of my life. Many people have helped me along this process.

I gratefully acknowledge the support I have also received from my supervisors, excellent researchers, and lecturers — Professor Oles Andriychuk and Professor Barry Rodger. Thank you for continuous support. You have helped me to become the researcher and academic I am today. Thank you.

This thesis would not have been possible without the support and love of my parents. I wish to express my thankfulness to mum and dad for helping me to become the person I am. Thank you for embracing my weirdness, listening to my endless monologues about this thesis, and giving me all the necessary advice.

I am raising a toast to thank you all.

Greenfaulds, April 2024
Arletta Gorecka

Table of content

Table of figures

Abstract

The debate on the intersection between competition and privacy constitutes a major challenge and an opportunity to the existing competition law framework. Big Tech firms are powerful in controlling digital behaviour and market forces in an unprecedented way. Most online products and services, including social networks, search engines, and number-independent interpersonal communication services are offered free of charge. In exchange to access online products and services, digital firms collect and process users' data for commercial purposes. The ability of digital firms to collect and process an unprecedented magnitude of personal data has opened new directions for large digital firms to abuse their market position. In fact, it is not to suggest that big data enabled more abuse, but rather that the novelty of challenges introduced by extensive data acquisition has triggered the competition law framework to accommodate the definition of abuse and different components such as market definition. Particularly important is that the market power of Big Tech firms is interlinked with threats to users' privacy through collection and use of personal data, which may fall outside the scope of competition law, while still having an impact on competition in online markets. In fact, the collection of personal data does not immediately constitute a violation of competition laws and can potentially offer a competitive edge. The key aspect that determines a competition law violation is not simply the mishandling of data or infringement of user privacy, but rather the presence of misconduct that actively harms competition. In other words, it is the conduct that goes beyond data misuse and privacy breaches and detriments to competition; at the same time Big Tech is adapting to new reality and more and more often becomes a guardian of privacy, posing thereby a new challenge for competition & data protection enforcers.

This thesis focuses on assessing the extent to which the current framework of EU competition law can incorporate the privacy-related theory of harm. The objective is to assess the significance of protecting individuals' privacy as a fundamental aspect in establishing the exploitative abuse of dominance, under Article 102 of the Treaty on the Functioning of the European Union (TFEU). Specifically, the thesis explores instances where Big Tech firms exploit their dominant position through excessive data collection and/or limiting choice, subsequently harming competition, and direct affecting user well-being. This thesis posits the stance that zero-priced business models of online platforms and the ubiquity of data generation create strong incentives to acquire and process consumer data,

introducing incentives to harm digital consumers' privacy. The thesis aims to assess how the existing EU competition law framework can address and regulate exploitative abuses, particularly concerning protection of individuals' privacy. Notably, this thesis argues that competition law might acknowledge privacy-related harms as forming exploitative theories of harm under Article 102 TFEU. As indicated by the rationale of the *Asnef-Exquitax* case and the CJEU's *Facebook case*, competition law will intervene only in instances where privacy-related harms resulted in the distortion of competition.

The analysis of the Digital Markets Act (DMA), the new EU tool to address large digital platform's conducts and ensure fair and contestable digital markets, remains outside the scope of this thesis, as the DMA is a parallel regime having no strictly legal impact on Article 102 TFEU. This thesis focuses on the assessment of Article 102 TFEU, which is more flexible and can be applied to a broader range of unfair practices. Notably, Article 102 TFEU emphasises on enhanced transparency and predictability, aiming to prevent abuse of dominant position that could undermine healthy competition to the detriment of consumers and other market participants. Although traditional competition law and the DMA can be enforced in parallel, it is unclear whether and to what extent the Commission and the NCAs would continue to sanction digital gatekeepers under Article 102 TFEU.

Abbreviations

AGCM - Italian Consumer Protection Authority

B2C - Business-to-consumer

BEUC - The European Consumer Organisation

BKartA - Bundeskartellamt

Charter - Charter of Fundamental Rights of the European Union

CJEU - Court of Justice of the European Union

CMA - Competition and Markets Authority

Commission - European Commission

DMA - Digital Markets Act

DOJ Antitrust Division - United States Department of Justice Antitrust Division

EDPB - European Data Protection Board

FTC - Federal Trade Commission

GAFAM - Google (Alphabet); Apple; Facebook (Meta); Amazon; and Microsoft

GDPR - General Data Protection Regulation

GWB - German Competition Act

ICO - Information Commissioner's Office

NCA - National Competition Authority

TEU - Treaty on European Union

TFEU - Treaty on the Functioning of the European Union

SSNIP - Small but Significant Non-Transitory Increase in the Price

SSNDQ - Small but Significant Non-Transitory Decrease in the Quality

Chapter 1: Introduction

1.1. Purpose of this thesis

Competition law and data protection are strong forces shaping the digital economy. The influence of large digital service and product providers has blurred the divide between privacy and competition law regulation. Digital services and products, introduced by large digital undertakings, are driven by processing of personal data.[1] Most internet services and products are available for free, but digital companies collect and analyse users' data for commercial gain in return. The vast amount of personal data that these companies can obtain has led to new ways for them to misuse their market dominance. The novelty of challenges introduced by extensive data acquisition has forced competition laws to accommodate the concept of abuse.[2] The market power of large digital companies is linked to the potential threat to user privacy through the collection and use of personal data. In addition, such data-opolies are powerful in controlling digital behaviour, as well as market

[1] Anca Chirita, 'Data-Driven Unfair Competition in Digital Markets' [2023] Boston University Journal of Science & Technology Law 241; Jan Trzaskowski, 'Data-driven value extraction and human well-being under EU law' [2022] Electronic Markets 447; Christophe Samuel Hutchinson and Diana Trescakova, 'The challenges of personalized pricing to competition and personal data protection law' [2021] European Competition Journal 105; J Cremer, Y de Montjoye and H Schweitzer, 'Competition policy for the digital era' (European Commission 2019) 30 <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 10 December 2019 (hereinafter: Cremer Report); UK Government, 'Report of the Digital Competition Expert Panel, Unlocking Digital Competition' (March 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 10 December 2019 (hereinafter: Furman Report); CMA, 'Online Platforms and Digital Advertising Market Study' (July 2020) < https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> accessed 15 November 2022 (hereinafter: 'Online Platforms and Digital Advertising Study'); Ben Holles de Peyer, 'EU Merger Control and Big Data' (2017) 13 (4) Journal of Competition Law & Economics 767.

[2] See primarily, Case B6-22/16 *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*. <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108> Accessed 28 August 2019 (hereinafter: Facebook case); Case KVR 69/19, *Facebook v Bundeskartellamt* <https://www.bundesgerichtshof.de/SharedDocs/Termine/DE/Termine/KVR69-19.html;jsessionid=F09CB5804920B1DDFF6B994C11C0E3D8.2_cid286?nn=11439166> accessed 30 June 2020; OLG Düsseldorf (2019). Order of 26.08.2019, Case VI-Kart 1/19 (V) ECLI:DE:OLGD:2019:0826.VIKART1.19V.0A; Case KVZ 90/20, *Facebook,* BGH, 15.12.2020. Monopolkommission, 'Competition policy: The challenge of digital markets' (2015) Special report No. 68 <https://www.monopolkommission.de/index.php/en/press-releases/52-competition-policy-the-challenge-of-digital-markets> accessed 20 November 2022. Also, the discussion in this thesis refers to the practices of data fuelled companies, as the whole industry generates personal or industrial data on a big scale sufficient for machine learning purposes. I use examples of Google (Alphabet); Apple; Facebook (Meta); Amazon; and Microsoft (hereinafter: GAFAM) practices as these companies are the key data market players.

forces.[3] The ability of digital firms to collect and process an unprecedented amount of personal data has given rise to online privacy issues, which while at first glance falling outside the competition law scope, have an impact on the competitive process in online markets.[4]

This thesis aims to explore the relationship between competition law and data protection, addressing the critical question:

> *To what extent could the existing EU competition law framework accommodate a privacy-related theory of harm?*

The primary objective of this thesis is to examine the potential role of protecting individuals' privacy as a crucial factor in determining abuse of dominance under Article 102 of the Treaty on the Functioning of the European Union (TFEU). Particular attention is given to the practices of digital data-opolies, which collect and process a magnitude of personal data, and potentially limit effective competition to the detriment of consumers. This increased attention arises due to their potential to curtail effective market competition, consequently disadvantaging consumers. The precise meaning of the competition perspective on user privacy appears problematic, as reduction of privacy may not necessarily amount to a competitive issue. Simultaneously, any reduction of privacy equally may not result immediately as a privacy breach if the data processors comply with data protection law.

This thesis evaluates the extent to which the existing EU competition law framework has the capacity to effectively address and regulate instances of exploitative abuses as per Article 102 TFEU, with a specific emphasis on protecting individuals' privacy.[5] The thesis proposes that exploitative theories of harm as per Article 102 TFEU can acknowledge privacy-related harms in their assessment in certain instances, which will be discussed in this research. It is important to strike the right balance where competition law could remediate any privacy-related harms and enhances consumer welfare. Acquisition of data on its own does not

---

[3] Data-opolies are defined as companies that control a key platform which attracts sellers, advertisers, software and app developers, and users. Maurice E Stucke, 'Should We Be Concerned About Data-Opolies?' [2018] Geo L Tech Rev 275, 275.

[4] *Facebook case* (n 2); *Case KVR 69/19* (n 2)*; Case VI-Kart 1/19* (n 2).

[5] Consolidated Version of the Treaty on the Functioning of the European Union, 2008 OJ C 115/47, art 102.

amount to abuse of a dominant position and could be used to provide a competitive advantage. Instead, the crucial element of antitrust law violation is some form of misconduct that violates competition. In other words, it is conduct that not merely involves data mistreatment and breaches of user privacy but conduct that must also harm competition. With regards to privacy-related harms, this thesis suggests that exploitative theories of harm, under Article 102 TFEU, might ensure that competition authorities acknowledge privacy-related harms in competition assessments.

1.2. Setting the context

The emergence of the digital economy has introduced innovative business models focusing on zero-price markets and multi-sided platforms, leveraging extensive business ecosystems. Digital platforms can harvest data, based on user consent, without users' understanding of the real value of such an exchange, which is then monetised through targeted advertising, personalised recommendations, and other means.[6] This revenue model allows digital platforms to thrive while appearing to offer free or inexpensive services to users.

In the realm of digital economy, the rationale behind setting a price of zero typically aligns with the following categories within their business models. Firstly, the collection of personal data has become a part of digital business models for monetarisation through advertising and sale of data, improving service quality, and developing new products.[7] Secondly, digital business models aim at advertising to monetise user engagement and generate revenue through targeted promotional content.[8] Offering free digital products and services to attract users' attention, subsequently directing them to advertising, is a well-established business model in various sectors.[9] Yet, in the digital economy, advertising can be tailored to

---

[6] Notably see, Cremer Report (n 1), Furman Report (n 1).

[7] G Malgieri and B Custers, 'Pricing privacy: The Right to Know the Value of Your Personal Data' [2018] CLSR 296; Diane Coyle and Annabel Manley, 'What is the Value of Data? A review of empirical methods' (2022) Bennett Institute for Public Policy <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/07/policy-brief_what-is-the-value-of-data.pdf> accessed 17 May 2023; David Nguyen and Marta Paczos, 'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective' (2020) OECD < https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf> accessed 17 May 2023.

[8] Maurice E Stucke and Alan P Grunes, *Big Data and Competition Policy* (OUP 2016) ch 1

[9] B Martens, 'An Economic Policy Perspective on Online Platforms' (2016) Institute for Prospective Technological Studies Digital Economy Working Paper < https://joint-research-centre.ec.europa.eu/system/files/2016-05/JRC101501.pdf> accessed 12 June 2022.

individual consumers. For example, digital platforms such as Google and Facebook leverage users' attention to revenue from advertising, as well as excessively collecting and proceeding users' data. Thirdly, digital platforms focus on developing a robust consumer base by offering engaging and valuable services that cater to the needs and preferences of their target audience.[10] In fact, by offering zero-priced products, the digital company could generate further revenues from consumers. This can be achieved through tactics such as providing limited-free trails, including a paid option with enhanced features, or selling complementary products, as well as leveraging the established relationship with consumers, who have been already using zero-priced digital services and goods.[11] Streaming services such as Netflix and Spotify, offer users premium content for recurring fees. In addition, offering products for free can be a strategic move to gain marketshare, especially if competitors offer similar products.[12] Freemium models provide basic services for free, while offering upgrades for a fee, frequently observed in gaming applications and software platforms. It is also possible for digital firms to offer free goods that aim to accumulate a large user base that could increase its attractiveness as a merger target for other firms.[13] Moreover, online marketplaces such as eBay or Airbnb charges transaction fees for facilitating interaction between users. Lastly, altruism and other long-term objectives play a significant role in shaping the dynamics of the digital economy. Some digital platforms, referred to as "open sources" are available at zero price and do not rely on personal data collection and/or advertising revenue.[14] Such technologies are offered without profit motivation, aiming to ensure broader views about innovation and users' accessibility. Some for-profit firms engage in the advancement of open-source technologies, like the Linux operating system, as they recognise the value they can derive from such contributions.[15]

---

[10] Gregory Day and Abbey Stemler, 'Infracompetitive Privacy' (2019) 105 Iowa Law Review 61.

[11] Michael G Jacobides and Ioannis Lianos, 'Ecosystems and competition law in theory and practice' [2021] Industrial and Corporate Change 1199.

[12] J Barnett, 'The costs of free: commoditization, bundling and concentration' [2018] Journal of Institutional Economics 1097.

[13] D Rubinfeld and M Gal, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' [2016] Antitrust Law Journal 521.

[14] Paško Bilić, Toni Prug, and Mislav Žitko, *The Political Economy of Digital Monopolies Contradictions and Alternatives to Data Commodification* (Bristol University Press 2021).

[15] J Newman, 'The Myth of Free' [2017] George Washington Law Review 86.

Personalised advertising is a focal point for competition authorities, especially concerning the market dynamics of major players like Facebook and Google. It is intricately connected to the broader discussion about data exploitation and the core revenue strategies for large digital undertakings. One of the possible advantages of personalised advertising is the potential to personalise advertising at scale.[16] Personalised advertising allows companies to expand their reach and inform consumers about their fresh products, services, or offers.[17] The more data is collected, the more knowledge acquired from its analysis might become widely distributed,[18] which in turn facilitates the competitiveness and growth of individual players in the digital market.[19] Technological progress in data analysis is facilitating the prediction of personality traits and attributes, even from a small extract of digital records of human behaviour, such as 'likes' on Facebook.[20] Certain personalised, ads could work well in search engines where ads can be tied to a uses' search keywords, such as those for niche websites, or specific major publishers serving valuable demographics, like affluent individuals sought after by luxury brands.[21] Some consumers consider personalised advertising as a "magic trick of the Internet", as they correspond to enhanced consumer experience, with users seeing ads that resonate with them.[22] In addition, personalised advertising offers new opportunities for advertisers, especially for implementing certain

---

[16] S Boerman, S Kruikemeier, F Zuiderveen Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' [2017] Journal of Advertising 363.

[17] C Ham, 'Exploring how consumers cope with online behavioral advertising' [2017] nternational Journal of Advertising 632.

[18] MS Gal and O Aviv, 'The Competitive Effects of the GDPR' [2020] JCLE 1, 8.

[19] Elias Deutscher and Stavros Makris, 'Exploring the Ordoliberal Paradigm: The Competition-Democracy Nexus' [2016] Comp LRev 181; J Schumpeter, *Capitalism, Socialism, and Democracy* (George Allen & Unwin, 1954); KJ Arrow, 'Welfare and the Allocation of Resources for Invention' in R Nelson (ed) *The Rate and Direction of Economic Activities: Economic and Social Factors* (NBER Books 2016); T Valletti, 'Doubt Is Their Product": The Difference between Research and Academic Lobbying' (*ProMarket,* 28 September 2020) <https://promarket.org/2020/09/28/difference-between-research-academic-lobbying-hidden-funding/> accessed 17 January 2023.

[20] M Kosinski, D Stilwell and T Graepel, "Private Traits and Attributes are Predictable from Digital Records of Human Behaviour" [2013] Proceedings of the National Academy of Sciences of the United States of America 5802.

[21] Garret Johnson, "Economics of Digital Ad Identity" (2020) (paper presented at W3C Workshop on Web and Machine Learning) <https://docs.google.com/presentation/d/1PKHVtO6hgwBJS1vafLyvG_IwupLhfCSelzczvltxjqc/edit#slide=id.p1> accessed 14 April 2023.

[22] Niklas Fourberg, Serpil Taş, Lukas Wiewiorra, 'Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice' (EU Parliament, 2021) 31 < https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf> accessed 12 April 2024.

marketing campaigns, which is an indication of competitive differentiation. For example, the Australian Competition and Consumer Commission found that digital platforms offered a fresh advertising opportunity for small to medium-sized enterprises that might have found traditional newspaper or TV and radio advertising costs prohibitive. For many of these businesses, online advertising has become integral to their operations, with some thriving solely through online strategies, cultivating a brand and customer base exclusively via social media.[23]

As large digital undertakings have access to valuable information on user behaviour, preferences, and interests, which they might utilise to acquire an unfair advantage over their consumers.[24] Having control over a large quantity of data, and an ability to analyse, it might form a source of market power for incumbent market players.[25] These actions can distort competition, reduce innovation, and ultimately harm consumers.[26] Several national competition authorities (NCA) across Europe conducted sector inquiries in an effort to map out an understanding of the competitive complexity introduced by the digital advertising sector. For example, the Competition and Markets Authority (CMA) considered digital advertising primarily relating to Facebook's and Google's position.[27] According to the CMA, Facebook and Google could exploit their market power in display and search advertising respectively to increase revenue.[28] In addition, the CMA noted a possible concern of self-preferencing, as Google or Facebook could treat their advertising services and inventories

---

[23] Australian Competition and Consumer Commission, 'Digital Platforms Inquiry: Final Report' (2019) <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20%20final%20report.pdf> accessed 14 May 2020.

[24] N Economides and I Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective' [2021] J Compet Law Econ 765, 765; A Ezrachi and V Robertson, 'Competition, Market Power and Third-Party Tracking' [2018] World Comp: L&C Rev 5, 5.

[25] 'Competition policy: The challenge of digital markets' (n 1).

[26] Stucke and Grunes (n 8); A Lambrecht and CE Tucker, 'Can Big Data Protect a Firm from Competition?' (*CPI,* 2017) <https://www.competitionpolicyinternational.com/can-big-data-protect-a-firm-from-competition/> 3, accessed 3 April 2020; Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' (2016) <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=7EE1625AF7E8DDAF12967AE0549C9C23.2_cid381?__blob=publicationFile&v=2> accessed 10 February 2020; M Stucke, *Breaking Away How to Regain Control Over Our Data, Privacy, and Autonomy* (OUP 2022) 14

[27] 'Online platforms and digital advertising' (n 1) para 8.153

[28] ibid, para 8.154.

more favourably than similar services offered by third parties.[29] Furthermore, the CMA highlighted concerns regarding large digital platforms, including: (i) their capacity to monetise content more effectively owing to data advantage; (ii) transparency regarding the processing of data, including access to data, and concerns over fees in open display advertising; (iii) their interpretation of data protection regulation in a manner reinforcing their competitive edge.[30] In particular, the CMA spotted concerns of personalised advertising, including possible users' manipulation, self-preferencing, complaints over unclear terms and conditions and/or lack of transparency and information asymmetries.[31] Similar concerns were also noted by the Spanish competition authority, which pointed out that Google's and Facebook's business models were characterised by a lack of transparency about prices and conditions applied in demand-side consumers, asymmetry of information and self-referencing.[32] Also, French's Autorité de la Concurrence noted that Google and Facebook stood out with a significant competitive advantage among internet users. This advantage is further augmented by their vertical integration, which encompasses both demand and supply facilitation, along with access to vast data reservoirs enabling highly accurate targeting capabilities.[33]

The pivotal role of users' data in online advertising, especially targeted advertising, naturally prompts concerns regarding the safeguarding of this data from a privacy law standpoint. The acquisition of extensive amounts of personal data by large digital undertakings has created opportunities for them to exploit their dominant position in new ways.[34] The significant influence of major digital firms in the market is closely linked to potential violations of users' privacy due to their gathering and utilisation of personal data. While Article 102 TFEU has

---

[29] 'Online platforms and digital advertising' (n 1) para 8.157.

[30] ibid.

[31] ibid, paras 8.157–8.166.

[32] CNMC, 'E/CNMC/002/2019 Study on the competition conditions in the online advertising sector in Spain' (2021) <https://www.cnmc.es/sites/default/files/3696007_0.pdf> accessed 10 March 2024.

[33] Autorité de la Concurrence, 'Sector-specific investigation into online advertising' (Press release, 2018) <https://www.autoritedelaconcurrence.fr/en/press-release/6-march-2018-sector-specific-investigation-online-advertising> accessed 30 April 2024.

[34] See, Ioannis Lianos and Bruno Carballa Smichowski, 'Economic Power and New Business Models in Competition Law and Economics: Ontology and New Metrics' (2021) Centre for Law, Economics and Society Research Paper Series: 3/2021 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3818943> accessed 12 November 2022.

proven effective in addressing traditional antitrust concerns, such as predatory pricing and exclusive dealing, it struggles to incorporate privacy-related harms that arise from the collection and use of personal data by online dominant companies.

Before this thesis turns to question the extent to which traditional competition law could incorporate possible privacy-related theories of harm, I discuss one question concerning zero price markets: what is the key nature of transactions between digital services and products providers and consumers of zero-priced digital goods? The monetary price of zero does not suggest that users are not giving anything up in exchange for the digital products they receive.[35] In practical situations, consumers frequently pay with multiple currencies, such as privacy, attention, and sometimes money. Hence, when evaluating under Article 102 TFEU, it is essential to consider all components forming the price paid by a consumer. I offer a brief overview of a specific blend of different types of payments, including personal data, user attention, and conventional monetary transactions when using digital platforms.[36] There are two scenarios available:

(1) Users pay for digital products with attention and privacy

The inception of this thesis arises from recognising that individuals lack control over their data within the realm of the digital sphere. Individuals are unaware of the true value of the data when exchanging it for access to ostensibly "free" digital services and individuals cannot accurately assess the value of personal data to determine the fairness of such exchanges.[37] The demand-side problem in digital zero-price markets includes characteristics of informational asymmetries and consumer behaviour biases.[38] In other words, individuals

---

[35] Nathan Newman, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2014) 40 William Mitchell Law Review 849, 857; D Evans, 'The Antitrust Economics of Free' (2011) John M. Olin Law & Economics Working Paper, University of Chicago, No. 555 <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article =1483&context=law_and_economics> accessed 30 March 2024. Evans argues that the notion of free goods lacking economic value is flawed. Even when priced at zero, businesses must decide on supply levels, and consumers consider the resources needed to access and utilise these items. In competitive markets, setting a "free price" simply means pricing at zero, treating it as any other numerical value.

[36] Daniele Condorelli and Jorge Padilla, 'Data-Driven Envelopment with Privacy-Policy Tying' (2021) <https://www.condorelli.science/PEPPT.pdf> accessed 6 November 2022; S Savage and D Waldman, 'Privacy tradeoffs in smartphone application' [2015] Economic Letters 137.

[37] Cremer Report (n 1); Furman Report (n 1).

[38] Cremer Report (n 1) 77.

have no influence on the terms of digital transactions, leaving consumers susceptible to manipulation.[39] More generally, consumers often overlook or fail to grasp the implications of the terms and conditions governing zero-price services, which establish transaction boundaries, while also facing attention constraints.[40] In these cases, users' attention and data (and privacy) play a significant role in shaping the revenue of digital platforms and service providers, which influence content customisation and advertising targeting, as indicated by the CJEU *Facebook* case.[41] This thesis will mostly focus on this scenario.

(2) Users pay for digital services in a price expressed by money

Some digital platforms might offer subscription-based or pay-per-use models where digital platforms seek alternative revenue streams and/or where users prefer ad-free experiences.[42] In such models monetary transactions directly occur. In such instances, hypothetically, users could be subjected to abuses of excessive pricing due to unfairly imposed prices to accept free-ads versions. In fact, users would be still required to transfer data. For example, Facebook launched a paid version of its main platforms, Facebook and Instagram, which are ad-free.[43] Facebook introduces a payment option where users can choose between paying for an ad-free experience or accepting ads, similar to a paywall setup. However, users can still access these platforms for free if they agree to view ads. Users should have the option to choose an alternative if they would rather not make a payment, and the pricing for the paid option should be fair. The rationale behind such payment is that digital platforms want compensation for the ad revenue they miss out on because they cannot provide

[39] A Acquisti, K Brandimarte, G Loewenstein, 'Privacy and human behaviour in the age of information' (2015) Science.

[40] ICO, 'Investigation into Data Protection Compliance in the Direct Marketing Data Broking Sector' (2020) <https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data- protection-compliance-in-the-direct-marketing-data-broking-sector.pdf> accessed 10 December 2020; EDPS, 'Opinion 8/2016: The Coherent Enforcement of Fundamental Rights in the Age of Big Data' (2016) 9 < https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf > accessed 14 August 2022; EDPS, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy' (2017) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 20 April 2020

[41] Case C-252/21 *Meta Platforms and Others* (Conditions Générales d'Utilisation d'un Réseau Social). For the same of clarity, I discuss this case throughout the thesis as 'Facebook case'. I will emphasise what decision I will be referring to throughout the discussion.

[42] Noyb, '28 NGOs urge EU DPAs to reject "Pay or Okay" on Meta' (2024) < https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta> accused 20 April 2024.

[43] ibid.

personalised ads, which rely on tracking users' online activities. In this scenario, there are still questions about the extent of user choice and the balance between privacy rights and access to services. For those unwilling to pay and without alternative providers, the ad-supported free version may be the only viable choice, limiting options to consenting to data use. Yet, this scenario is highly hypothetical, as users could face significant barriers in fully transitioning from digital services and products if their provider enjoys a dominant position as a primary gateway for users and businesses.[44] Correspondingly, large digital undertaking could restrict users' ability to exercise choice and switch to alternative platforms, further complicating the issue of consent and data use, and users' privacy.

1.2.1. Mapping the Current Landscape: Navigating Article 102 TFEU and Privacy

The application of Article 102 TFEU to data privacy harms raised concerns regarding the balance between competition law and data protection law. It is necessary to consider the extent to which the traditional competition law toolbox can incorporate privacy-related harms during its anticompetitive assessment. In essence, many has perceived the EU privacy regime as the most advanced and offering the most attractive personal data protection. Article 16 TFEU serves as a basis for EU data protection, which recognises that everyone has a right to protection of their data[45] Further protection of personal data is offered by the Charter of Fundamental Rights of European Union (the Charter), where Article 8 recognises personal data as a proactive right that reaches beyond an individual's protection against the intervention of a state.[46] When exploring constitutional theories of balancing in EU law, especially in the context of conflicting rights which arise in the application of competition law to digital platforms, the doctrine of proportionality enables courts to address conflicting rights and norms; one can seek resolution by evaluating their comparative importance

[44] Christophe Carugati, 'The 'pay-or-consent' challenge for platform regulators' (Bruegel, 2023) < https://www.bruegel.org/analysis/pay-or-consent-challenge-platform-regulators#footnote2_ricgd6g> accessed 24 November 2023.

[45] TFEU (n 5) article 16: "1. Everyone has the right to the protection of personal data concerning them.
2.The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

[46] Charter of Fundamental Rights of the European Union 2010 OJ C 83/02, article 8.

(balancing) and imposing conditions, such as the requirement of necessity.[47] The process of digitalisation and the convergence of physical and online interactions have minimised geographical separations and overcome physical obstacles. However, digitalisation also introduced challenges to the societal structures, establishing several tensions. Especially, concepts such as platform, surveillance capitalism,[48] and data power[49] explain how the digital information environment could potentially undermine our core rights. In such instances, assessing the validity of a measure that encroaches upon the fundamental right to privacy and data protection. However, determining what qualifies as proportionate in a broader sense, especially concerning data protection, is a complex challenge. The jurisprudence of the Court of Justice of the European Union (CJEU) has frequently faced criticism for its lenient and somewhat flexible approach to assessing proportionality.[50] The CJEU appears to be applying a somewhat flexible and discretionary approach when it comes to assessing proportionality in the context of personal data protection.[51] In competition cases, the application of the proportionality test might be capable of finding a middle way, during an investigation of possible users' exploitation, where privacy is being used by Big Tech as a shield.[52] In such instances, the EU Commission (the Commission) "plays the parts of law-maker, policeman, investigator, prosecutor, judge and jury, subject to review by the EU Courts."[53]

Under Regulation 1/2003, the Commission can decide on finding and termination of abuses under Articles 101 and 102 TFEU, order interim measures or decide if Article 101 or 102

---

[47] The doctrine of proportionality is only mentioned as a means to supplement the discussion. It is beyond the scope of this thesis to focus on this doctrine deeper. G De Gregorio, 'The rise of digital constitutionalism in the European Union' (2021) 19(1) International Journal of Constitutional Law 41.

[48] S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

[49] O Lynskey, 'Grappling with ‘data power’: Normative nudges from data protection and privacy' (2019) 20(1) Theoretical Inquiries in Law 189.

[50] Audrey Guinchard, 'Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law' (2018) 24 European Law Journal 434.

[51] Joined cases *Volker und Markus Schecke GbR* (C-92/09) and *Hartmut Eifert* (C-93/09) v Land Hessen, 17 June 2010, ECLI:EU:C:2010:353, Opinion of Advocate General Sharpston.

[52] I covered this argument in Chapter 4, section 4.2.2(2) where I discussed Google Privacy Sandbox incentive.

[53] Alison Jones, Brenda Sufrin, and Niamh Dunne, *EU Competition Law: Text, Cases, and Materials* (7th edn, OUP 2019)

TFEU is not applicable for the situation in question.[54] In the context of privacy-related harms, it remains ambiguous how to balance the conflicts of privacy and competition law. In such scenarios, there is often a need to strike a 'balance' between the essential rights at play. Sometimes, one of the rights in question may not be a fundamental right in the traditional sense but could be an economic liberty, like the free movement of goods, as acknowledged in the fundamental EU Treaties.[55] In other words, it is important to consider a balancing frame that focuses competitive effects of an infringement in question but ignores different values.[56] Such balancing activity would largely depend on specific facts of the case, considering the broader impact of the possible privacy-related infringement on competition law and weighting possible negative and positive impacts on competition law.

The protection of data privacy has been ‘enriched’ with the implementation of the General Data Protection Regulation (GDPR), which strengthened the protection of personal data and, simultaneously, users’ privacy.[57] Article 1 GDPR emphasises on “protection of natural persons with regard to the processing of personal data” and ensure “the free movement of personal data within the Union”.[58] The GDPR’s fundamental principle is the requirement to establish a legal basis for personal data processing,[59] as any information acquired relating to natural persons which allows for their potential identification. Importantly, the key feature of the GDPR’s regime is consent — which sets a basic requirement for the effectiveness of the legal consent for processing — which must be unambiguous, specific, informed and freely given,[60] granted by individuals by clear affirmative action, or by a statement which signifies a consent to process their personal data. These four criteria are closely linked and

[54] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance) (hereinafter: Regulation 1/2003), articles 7-10.

[55] See for example, Case C-112/00 *Schmidberger* [2003] ECR I-5659, para 77, where the CJEU considered: "the need to reconcile the requirements of the protection of fundamental rights in the Union with those arising from a fundamental freedom enshrined in the Treaty."

[56] *Meta Platforms* (n 41).

[57] 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) (hereinafter: GDPR).

[58] ibid, article 1

[59] ibid, article 4(2).

[60] Ibid, article 7, recitals 32, 33, 42, 43.

depend on each other. In order words, freely giving consent is a requirement of granularity of consent, whereas a requirement for specific consent is closely linked with informed consent, as both criteria aim to safeguard transparency.[61] The conditions for a consent are provided in Article 7 GDPR, which states:

> "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data"[62]

Consequently, the burden of proof is on the data controller, defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"[63] Data controllers have a crucial function in implementing GDPR, as they are the primary entities responsible for carrying out the requirements outlined in the regulation.[64] Fundamentally, consent is based on the idea that users should be in control of their data, emphasising the importance of consent stems from its role in preserving individual autonomy. Simultaneously, users' autonomy is a prerequisite for consent as users' consent must reflect on users' wishes and considerations when making a decision.[65]

Although consent for a lawful processing of personal data is required, individuals are unable to thoroughly consent to the real purpose of data processions: consent today is a matter of box-ticking. Recital 32 GDPR emphasises that user consent includes:

> '[T]icking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates

---

[61] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> 14-15 accessed 4 April 2023. (hereinafter: 'EDPB Consent Guidelines')

[62] GDPR (n 57) article 7(1).

[63] ibid, article 4(7). For the purpose of the discussion, it remains important to emphasise the difference between a data processor and a data controller. For example, a social media company gathering personal information, they are classified as the "controller" because they decide both the method and the purpose behind the data processing. On the other hand, a data processor is either legal person, public authority, agency or other body processing the same data on behalf of the data controller (ibid, article 4(8)).

[64] C Kuner, LA Bygrave, C Docksey and L Drechsler, *The EU General Data Protection Regulation: A Commentary* (1st edn, OUP 2020) 146.

[65] K Wiedemann, 'Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary' [2021] IIC 915.

in this context the data subject's acceptance of the processing of his or her personal data'.[66]

GDPR is inherently characterised by the notion that data subjects have a right to informational self-determination, which emphasises users' control over their personal information. Under GDPR, users can decide about the use of their data, or users are at least aware of what data processing activities involve.[67] In terms of assessing the validity of consent, competition law lacks the relevant tools to assess if consent has been freely given.[68] However, using GDPR as a normative point of reference can be significant for establishing a theory of harm under Article 102. The validity of user consent is problematic in the digital environment due to both the market position of large digital undertakings and possible bundling within Article 102 TFEU, as users might offer consent to several digital products and services offered by a large digital undertaking.

Digital service and product providers can collect and process their users' personal data without their adequate understanding of the data-collecting and processing activities; an unprecedented collection of personal data has opened new opportunities for digital firms to abuse their market power, raising also antitrust issues. Despite such shortcomings, the GDPR aims to inherently safeguard informational autonomy through granting users a sense of control over their data by requiring consent. By virtue of Article 6(1) GDPR, the processing of personal data is only lawful when a data controller has a legal basis for it, including (a) reasoned consent from the data subject,[69] (b) processing requirements complying with legal obligations, (c) legitimate interest for balancing of the interests concerned. Data processing under this legal basis is only legal if individuals involved are part of an agreement (i.e. they

[66] GDPR (n 57) recital 32

[67] Case 1 BvR 209/83 et al., *Volkszählungsurteil*, 15 December 1983, 65 BVerfGE 1

[68] Chun Sang Wong and Sze Lam Chan, 'At the Junction of Consumer Protection: Dual Role of Data Protection in EU Law' (2021) 6(2) London School of Economics Law Review 109

[69] GDPR (n 57) recital 43 provides that the notion of "freely give" has to be interpreted: "[I]n order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case (…)."

offered a valid consent), and the data handling is essential for carrying out that agreement.[70] Under Article 6(1) GDPR, this variation is an expression of informational self-determination, as a data subject's explicit consent is the basis for justifying the data processing activities carried out by the data controller.[71] The notion of transparency is directly interlinked with the control paradigm.[72] The concept of transparency is established in Article 5(1)(a) GDPR. This fundamental duty is intricately connected to principles of fairness and serves as a pivotal, all-encompassing responsibility.[73] Furthermore, Articles 13 to 15 GDPR prominently impose obligations on data controllers to inform data subjects about the data processing activities at the time when their data is collected. Yet, the transparency obligations are not only confined to Articles 13 to 15 GDPR but are prevalent in different GDPR contexts. For instance, under Article 4(11) GDPR, consent must be given in an informed manner, and data subject have to be provided with information without any undue delay in the case of a data breach.[74] The concepts of control and transparency are closely connected, as having meaningful control is challenging without at least some level of transparency.

Yet, such exhaustive legal bases could differ significantly if one analyses how much power users indeed have in the decision-making process over their personal data. In this respect, control and transparency can have direct impact on users' ability to decide whether to enter a contract with a digital undertaking or not.[75] Accordingly, the notion of consent is two-fold. Firstly, data subjects have a right to exercise a certain degree of control over what happens to their personal data. Secondly, data subjects have a right to remain informed as to what happens with their data. The legal basis of consent will therefore depend on whether the data subject wants their personal data to be processed or not, and this is a manifestation of

[70] The GDPR also applies when the individual has specifically asked for actions to be taken before the contract is finalised. GDPR (n 57) article 6.

[71]Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' [2021] JIPITEC 246.

[72] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (17/EN, WP260 rev.01, as last revised and adopted on 11 April 2018) para 4.

[73] ibid; Klaus Wiedemann, 'Can Data Protection Friendly Conduct Constitute an Abuse of Dominance under Art. 102 TFEU?' (2023) Max Planck Institute for Innovation and Competition Research Paper No. 23-15.

[74] GDPR (n 57) article 31(1)(2).

[75] Zohar Efroni, 'Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing' (2019) 3 EDPL 352, 354-355.

granting users the control and the choice for data collection and processing activities.[76] According to Article 7(4) GDPR, the term 'free given' consent is when:

> "[T]he performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[77]

This means that large digital undertakings can only collect data for purposes known and communicated to the users. Apart from this specific requirement, each user has to declare their consent by a statement of clear and affirmative action.[78] GDPR offers an insufficient response to the exploitation of personal data: data protection law does not recognise the long-term harms to the platforms' users, including the special responsibility that could ensure the position of power of some digital platforms. In certain situations, consent might be invalid in certain situations in which the data controller demands consent for the collection and analysis of an unreasonable amount of personal data. In this respect, Article 7(4) GDPR plays an important role in the consideration of data as counter-performance.[79] In fact, its scope and application are difficult to be defined. In the *Facebook case,* the CJEU expressed doubts as to whether consent can be seen as freely given in the instance of a large digital undertaking's dominance. In this respect, according to the CJEU's perspective, having access to personal data has evolved into a critical aspect of competition within the digital economy. Hence, disregarding GDPR when evaluating abuse of dominance cases from a competition standpoint would fail to acknowledge the current economic landscape and could potentially weaken the effectiveness of EU competition law.[80]

Recital 43 GDPR provides more guidance on the assessment of a freely given consent, indicating that:

---

[76] EDPB Consent Guidelines (n 61).

[77] GDPR (n 57) article 7(4).

[78] ibid, article 4(11).

[79] Josef Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' in A De Franceschi and R Schulze (eds), *Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice* (Beck 2019); Zohar Efroni, 'Gaps and Opportunities: The Rudimentary Protection for "Data-Paying Consumers" under New EU Consumer Protection Law' (2020) 57(3) Common Market Law Review 799.

[80] *Meta Platforms* (n 41) para 51.

> "[C]onsent should not provide a valid legal ground for the processing of personal data in a specific case where there is between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."[81]

There are two lessons to be learnt from Recital 43 when it comes to assessing the normative links between competition law and the GDPR in cases where a digital firm's business model is based on a large-scale content-based processing of personal data. In fact, the discussed lessons arguably demonstrate a broader dissatisfaction with how the GDPR is being enforced so far.[82] I focus on the practical problems associated with the application of the GDPR though the lens of competition law. Firstly, I argue that the problems of behavioural issues of consent forms are interlinked with the terms and conditions shorthand. Kerber argued that:

> "[E]specially the examples of Google and Facebook with their often alleged dominant market positions have raised the question whether weak competition might lead to an excessive collection of private data and to an insufficient provision of privacy options for fulfilling the different privacy preferences of users"[83]

One of the specific shortcomings of the GDPR application relates to the validity of consent obtained by large digital undertakings. Large digital undertakings can secure user consent by taking advantage of the fact that users have limited alternatives or are locked into their services. This allows these companies to appear compliant with GDPR regulations on the

---

[81] GDPR (n 57) recital 43.

[82] The GDPR is subject to a possible reform, due to the general dissatisfaction with its application. The EU lacks a singular data protection authority responsible for enforcing the GDPR. Rather, each member state has its own regulatory authority tasked with enforcing data protection regulations. These authorities are designated to have the necessary competence to carry out the assigned tasks and exercise the granted powers on the MS territory. Government agencies, private companies, privacy activists, and civil society groups have expressed worries about the implementation of the law, citing issues such as the high costs associated with initiating a legal case, variations in procedures among different member states, and the extended delays in reaching resolutions. Special attention has been paid to the Irish Data Protection Authority and its bottleneck status. The Irish Data Protection Authority frequently finds itself addressing the most prominent and well-publicised cases, due to the significant presence of major technology companies in Ireland. For example, Irish Data Protection Authority has imposed a historic €1.2 billion fine on Meta, the parent company of Facebook, for violating GDPR. The possible reform might be helpful in tacking Big Tech abuses. However, it is beyond the scope of this thesis to focus on data protection authorities mandate the possible GDPR reform in details. I will briefly discuss the institutional overview in Chapter 3. See, J Liboreiro, 'Brussels pitches GDPR reform but without opening 'Pandora's box' (euronews.com 2023) <https://www.euronews.com/my-europe/2023/07/04/brussels-pitches-gdpr-reform-but-without-opening-pandoras-box> accessed 15 October 2023; Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Additional Procedural Rules Relating To The Enforcement Of Regulation (Eu) 2016/679.

[83] Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' [2016] J of Intellectual Property L & Practice 856, 860.

surface, even if user consent has not been freely given. Secondly, an exercise of a freely given consent is a manifestation of a consumer choice, where users decide if they prefer a more or less data processing when using digital services and products.[84] For several digital business models, especially those which assume personal data as the role of contractual consideration, the legal basis of a freely given consent according to Article 6(1)(a) GDPR is vital. Advertisers which rely on third-party tracking are required to have the user's consent as well. Yet, the debate on how the consent is being received is the key consideration in this dispute, as the market power of a large digital undertaking could lead to clear imbalance for users accessing offered digital services and products.[85] A simple click to "consent" to offered terms of service acts like a butterfly effect, which has got a capacity of introducing potential negative exploitative harms on the end users and the overall functioning of the market. Similarly, in the *Facebook case*, the CJEU clarifies that a data controller's dominance does not invalidate users' ability to give a valid consent.[86] When personal data is aggregated across various digital services, consent is only valid when users can either grant or decline consent for any data processing that exceeds what is necessary for fulfilment of a contract. In this respect, I argue that a consent-related violation may be considered while determining the exploitative abuse of dominant position of digital undertakings. The assessment of exploitation needs to be considered on the case-by-case basis, which would allow to establish a link that a consent-related violation indeed resulted in infringing competition law as per Article 102 TFEU. The same assessment is consequently required in the instances of economic imbalance between the parties. Equally, this must be done if the data controller is a dominant undertaking under competition law.

Concerns regarding to any potential data privacy-related harms have never played a prominent role for competition law. EU competition law is concerned with market power that might negatively impact consumer welfare.[87] Competition law adopts the market failure

---

[84] I am going to consider several examples in this thesis. The most notable example is the BKartA's *Facebook case* (n 2), which is discussed in chapter 3, section 3.5.

[85] Case C-252/21, Request for a preliminary ruling, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social) ECLI:EU: C:2022:704, Opinion of AG Rantos, para 75 (hereinafter: '*Meta Platforms, Opinion of AG Rantos*').

[86] *Meta Platforms* (n 41)

[87] European 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 19. (hereinafter: 'Guidance on the Commission's Enforcement Priorities in Applying Article 82')

approach which is concerned with the fact that consumer welfare might be reduced because of limited data protection offered in the market for personal data acquisition.[88] The traditional EU-level approach to privacy infringements, as per the case of *Asnef-Equifax,* indicates that:

> "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law."[89]

Later, in regards *Microsoft/LinkedIn* and *Facebook/WhatsApp,* the EU Commission (hereafter 'the Commission') offered a more nuanced approach to data within EU competition law, as the Commission relied on the user privacy protection to assume the impact of combining the two companies' databases.[90] The Commission, in the merger decisions of *Facebook/ WhatsApp* and *Microsoft/LinkedIn*, acknowledged the dimension of privacy and based their assessment on price considerations;[91] therefore, the assessments focused on the prevailing approach of the economic considerations in the competition law investigations. In both merger cases, the Commission noted that privacy could act as an important competitive parameter. However, in both merger cases, the Commission focused on securing a competitive process and did not provide any guidance on data protection within the competition law sphere, missing an opportunity to instruct on the privacy-related concerns in competition law. The situation evolved in 2019 when the Bundeskartellamt (BKartA), under German Competition Act (GWB), extended the debate on the relationship between competition law and privacy. The BKartA's proceedings against Facebook introduced a potential new angle to the theory of harm, indicating that the privacy breaches might amount to the abuse of a dominant position:[92]

> "[p]rocessing data from third-party sources to the extent determined by Facebook in its terms and conditions is neither required for offering the social network as such nor for monetising the network through personalised advertising, as a personalised

---

[88] Economides and Lianos (n 24) 765.

[89] Case C-235/08 *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios* ECR I-11125. [2006] para 177.

[90] Case M.8124 *Microsoft/LinkedIn* [2016] C(2016) 8404 final; Case M.7217 *Facebook/WhatsApp* [2014] OJ C 417/4.

[91] ibid.

[92] *Facebook case* (n 2) 10.

> network could also be based to a large extent on the user data processed in the context of operating the social network."[93]

The BKartA's approach of incorporating data protection rationales into competition law assessment indicates a remarkable shift to open more discussion with regards to considering privacy-related-harms in competition cases. The BKartA's investigation relied on at least two several theoretical assumptions which challenged traditional competition law approaches and introduced the possibility to incorporate privacy-related harms into realms of competition law. These assumptions include (i) the intersection between data privacy and the market, and (ii) the novel relevance of exploitative theories of harm in digital markets.

According to the BKartA's investigation, Facebook's unlawful and misleading data privacy policies resulted in abusing its market dominance by reducing the overall quality of its social networking services. By investigating the offered terms of service, Facebook's conduct was seen as a form of an exploitative theory of harm. The BKartA insisted that the consent of users might be seen as being forced since in the opinion of the BKartA: "[v]oluntary consent to [users'] information being processed cannot be assumed if their consent is a prerequisite for using the Facebook.com service in the first place."[94] The BKartA added that combining data from various sources was seen as a feature not necessary for the functioning of the social network. Hence, such conduct was not conditional to users' consent and constituted a privacy breach. Yet, within the scope of the BKartA's decision, nothing indicated that the GDPR's consent requirement was grounded on the market power of the data controller. The GDPR remains silent on the theory of competitive harm and does not differentiate based on market power considerations, and consequently remains silent on the dominant firm's responsibility to protect and guarantee special privacy responsibly**.** However, the interest of the BKartA was not to establish privacy violation itself. Any direct breaches of users' privacy protections are outside the scope of competition law and remain within the remit of the GDPR. Instead, the BKartA used the privacy violation as an indication of an exploitative abuse of Facebook's dominant position.[95] Hence, the definition of privacy violations is difficult to ascertain by anticompetitive means. Equally, privacy degradation is noted to be outside the interpretation of EU competition law due to potential difficulties in linking

[93] *Facebook case* (n 2) 10..

[94] ibid.

[95] ibid.

privacy terms to consumer welfare harm. On the same note, the competition Commissioner recognised potential scope for competition law enforcement in cases where only a small number of companies controlling data needed to satisfy consumers, as competition law could provide power to drive rivals out of the market and exploit consumers.[96] Equally, AG Rantos opined that an *incidental* consideration of GDPR could be admissible for competition law assessment.[97] This could only be achieved if the GDPR is introduced into a wider scope of the legal and economic context surrounding the conduct.[98] Such argument has also been accepted in the *Facebook case,* where the CJEU adopted AG Rantos' line of reasoning. The CJEU emphasises that the breach of an area of law can play a role in assessing a possible violation of competition law, as recognised in cases of *AstraZeneca* and *Allianz Hungaria.*[99] Hence, an incidental consideration of GDPR in cases of possible competition law infringement should not be seen as unexpected. Correspondingly, the CJEU concurred that while compliance with the GDPR has not automatically ruled out the finding of an abuse, it can be taken into consideration as part of the comprehensive assessment.[100] In this context, it may serve as a crucial indicator in determining if the conduct employs strategies in accordance with merit-based competition.

This thesis argues that EU competition law cannot escape privacy concerns, though no consensus remains as to an optimal method of evaluating data in EU competition law. The current debate regarding the prominence of digital platforms in offering free products (and services) to consumers and generating revenue through data collection has fostered discussion as to whether non-price elements — in this example, privacy — could become a parameter of competition law analysis. Hence, the transition from price-driven to data-driven markets introduces questions on whether existing competition law enforcement can sufficiently address privacy-related harms to competition and how competition law should interact with such harms.

---

[96] European Commission, 'Speech of Competition Commissioner Vestager, 'Competition in a big data world' (2016) *DLD 16 Munich*, 17 January 2016, <https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big- data-world_en.> accessed 10 October 2019.

[97] *Meta Platforms, Opinion of AG Rantos* (n 85) para 24.

[98] ibid, para 23.

[99] *Meta Platforms* (n 41) para 110; C-457/10 P *AstraZeneca/Commisson* ECLI:EU:C:2012:770; C-32/11 *Allianz Hungária Biztosító and Others* ECLI:EU:C:2013:160.

[100] *Meta Platforms* (n 41) paras 62 and 110.

This thesis adopts the position that EU competition law should support the prevailing approach — any privacy-related harms in cases concerning the abuse of a dominant position as per Article 102 TFEU should be considered through the spectrum of protecting a competitive equilibrium in a hypothetical market. The concept of privacy appears to be a multi-dimensional and dynamic issue,[101] requiring careful consideration of all dimensions and the interests of parties in relevant markets.[102] In order to fully apprehend the relationship between competition law and privacy-related harm, an assessment of theories of harm sits at the heart of this thesis. This enables a demonstration of the extent to which competition law might indeed remediate privacy-related harms. Subsequently, a sophisticated assessment of EU competition law enforcement is crucial and timely, considering the economic and legal focus on data processing practices in general and the ever-increasing significance of competition law being a key theme for digital businesses, particularly in the context of the growing reliance of personal data processing.

1.2.2. Article 102 TFEU and Digital Markets Act

To present an in-depth content of the dynamic debate on the intersection between competition law and data protection, it is important to emphasise that EU has identified the lack of effective competition in certain digital markets and the ability of digital platforms to engage in harmful anti-competitive behaviour.[103] In an attempt to regulate digital markets and address introduced challenges posed by large digital undertakings, the EU Commission proposed the Digital Markets Act (DMA).[104] While the primary focus of this thesis is on Article 102 TFEU, this thesis acknowledges that the DMA is an important and relevant legal

---

[101] L Bergkamp, 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' [2002] CLSR 31; Jonida Milaj, 'Safeguarding Privacy by Regulating the Processing of Personal Data – An EU Illusion?' [2020] EJLT 1.

[102] P Thibodeau, 'The Internet of Things Could Encroach on Personal Privacy' (2014) < https:// www.computerworld.com/article/2488949/emerging-technology/the-internet-of-things-could-encroach-on-personal-privacy.htm> accessed 2 October 2019; Paul M Schwartz, 'Global Data Privacy: The EU Way' [2019] NYU L Rev 772.

[103] Cremer report (n 1); Luís Cabral, Justus Haucap, Geoffrey Parker, Georgios Petropoulos, Tommaso Valletti and Marshall Van Alstyne, 'The EU Digital Markets Act A Report from a Panel of Economic Experts' (European Commission 2020) < https://ide.mit.edu/wp-content/uploads/2021/02/jrc122910_external_study_report_-_the_eu_digital_markets_act.pdf> accessed 6 May 2023; Monopolkommission, 'Recommendations for an effective and efficient Digital Markets Act' (2021) 9 <https://www.monopolkommission.de/en/reports/special-reports/special-reports-on-own-initiative/372-sr- 82-dma.html> accessed 9 April 2023.

[104] Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1 (hereinafter: DMA); N Petit, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review' [2021] JECL & Pract 529.

instrument in the context of the digital competition. Understanding the DMA is essential when discussing Article 102 TFEU, as the DMA represents a contemporary legislative effort to address competition issues in the digital realm. While the DMA may initially appear similar to Article 102 TFEU, it distinguishes itself as a separate tool with distinct objectives and aims to safeguard different legal interests.

The DMA aims to improve 'fairness' and 'contestability' in the digital sector,[105] by addressing the concerns about the market power of large digital platforms.[106] According to Recital 10 DMA, the Regulation aims to achieve: "an objective that is complementary to, but different from that of protecting undistorted competition on any given market, as defined in competition-law terms".[107] To achieve this, the Commission pinpoints large digital undertakings, defined as 'gatekeepers' using different standards, such as their magnitude, market influence, and market impact. In other words, the DMA dictates a law of gatekeeping focusing on the Internet distribution layer and covers digital enterprises that control end users' access to supply of digital products and services.

The Commission has primarily relied on ongoing or concluded legal proceedings concerning the abuse of dominant market positions under Article 102 TFEU as a foundation for the obligations outlined for gatekeepers in the DMA.[108] Article 102 TFEU provides a broader framework for preventing anti-competitive behaviour by dominant companies, while the DMA specifically targets digital platforms that hold significant market power and aims to regulate their behaviour to protect consumers interests. As per Article 2(1) DMA, a gatekeeper is defines as a 'provider of core platform services designated pursuant to Article 3 DMA.'[109] The DMA's scope is limited to eight core service providers, including online intermediation services, online search engines, and/or online social networking services.[110]

---

[105] DMA (n 104), article 1(1); recitals 2, 4, 6, 8, 10, 12, 15–16, 28, 32–33, 58, 65–66, 77–79.

[106] Marco Cappai and Giuseppe Colangelo, 'Taming digital gatekeepers: the more regulatory approach to antitrust law' (2021) 41 Computer Law & Security Review 105559.

[107] DMA (n 104) recital 10.

[108] Meltem Gündoğar, 'EU's Approach To Abuse Of Dominance Concerning Online Platforms: A New Era For Eu Competition Policy?' Europa Kolleg Hamburg Study Paper No.02/2023 < https://europa-kolleg-hamburg.de/wp-content/uploads/2023/01/Study-Paper-Meltem-Guendogar-pdf.pdf> 14 March 2024.

[109] DMA (n 104), article 2(1).

[110] ibid, article 2(2).

The DMA introduces obligations on firms designated as gatekeepers: the DMA does not refer to prohibitions as its scope is proscriptive and prescriptive. They include assessing quantitative data on metrics such as market shares, earnings, and user engagement, as well as evaluating qualitative aspects such as a company's conduct and its influence on the market.[111] Hence, not all digital undertakings are considered gatekeepers, as well as not all gatekeeping positions are a concern.

The scope of the DMA is defined to a two-staged process: (i) the nature of the services provided, because of an economic position that could confer on the gatekeeping position; (ii) an online platform's designation as a gatekeeper. Such economic features are used to support the definition of gatekeepers. The Commission will employ a mix of objective and subjective criteria to determine whether a business qualifies as a gatekeeper. As per Article 3(1) DMA, the three-step cumulative test of gatekeeping intends to cover instances of platforms.[112] Firstly, a platform needs to have a significant market power. In the internal market, captivating a turnover exceeding €6.5 billion. Secondly, a platform must be a core point for access by end users. Third condition relates to the application of the DMA to the condition of durability. Such provision excluded the applicability of DMA in instances where the competitive process could be dissolved at the lower cost.

One competitive advantage held by large digital undertakings is their capacity to gather, merge, and analyse end users' data sourced from various channels within their ecosystems.[113] Distinguishing data-related harms could potentially lead to breaches of Article 102 TFEU and the DMA. The question is therefore to understand how exactly to understand DMA alongside Article 102 TFEU. It is beyond the scope of this thesis to focus extensively on the DMA. Although traditional competition law and the DMA can be enforced

[111] DMA (n 104) recital 3.

[112] ibid, article 3: "An undertaking shall be designated as a gatekeeper if: (a) it has a significant impact on the internal market; (b) it provides a core platform service which is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future."

[113] Jan Krämer, Daniel Schnurr and Sally Broughton Micova, 'The Role of Data for Digital Markets Contestability' (CERRE Report, 2020) < https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/> accessed 12 April 2024; Marco Botta and Danielle Borges, 'User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with Article 5(2) DMA' Robert Schuman Centre for Advanced Studies Research Paper No. 2023_68

in parallel, it is unclear whether and to what extent the Commission and the NCAs would continue to sanction digital gatekeepers under Article 102 TFEU. To enrich the discussion in this thesis, I briefly discuss two elements to understand the relationship between Article 102 TFEU and DMA better: (1) several provisions of DMA are closely associated with how Article 102 TFEU was previously applied to online platforms; (2) the potential intersection between DMA requirements and the prohibition of exploitative abuse of dominance raises concerns about the violation of the *ne bis in idem* principle.

Many practices outlined in the DMA are closely linked to the previous application of Article 102 TFEU to online platforms. As this thesis focuses on exploitative theories of harm and privacy, I turn to discuss the possible overlap between the DMA and the prohibitions against unfair trading conditions and excessive pricing as per Article 102 TFEU, which could result in excessive data collection.

The DMA does not fundamentally aim to remediate something distinct from preventing market foreclosure and exploration by dominant undertakings, which Article 102 TFEU addresses.[114] The considerable overlaps between Article 102 TFEU and the DMA, if interpreted sympathetically, should not fundamentally alter the understanding of what and why they protect. The interaction between the GDPR and Article 102 TFEU involves examining abusive behaviour in excessive data collection, using data protection principles as a reference point or standard for evaluation.[115] While considering the relationship between competition law and privacy, the aspects relating to the data combination prohibition under Article 5(2) DMA could act as a proxy in discussing such overlaps. According to Article 5(2) DMA, gatekeepers cannot process personal data gathered from third-party applications and websites, alongside the data collected within their ecosystem.[116] Secondly, gatekeepers are prohibited from cross-using personal data collected within the core platform service with user data collected from other services provided by the gatekeeper.[117] Additionally,

[114] A Reyna, 'Why The DMA Is Much More Than Competition Law (And Should Be Treated As Such)' (Chilling Competition, 2021) <https://chillingcompetition.com/2021/06/16/why-the-dma-is-much-more-than-competition-law-and-should-not-be-treated-as-such-by-agustin-reyna/> accessed 6 April 2024.

[115] *Meta Platforms* (n 41)

[116] DMA (n 104) article 5(2)(a), see also *Meta Platforms* (n 41)

[117] ibid.

gatekeepers cannot compel end users to sign in to additional services, thereby forcing them to accept data combination requirements.[118] Together, these four prohibitions constitute a general prohibition on 'data combination' by gatekeepers. The gatekeepers hold responsibility for ensuring compliance with these provisions. It is expected that gatekeepers relying on data collection will utilise this exception and seek user consent. Such interpretation has been recently followed in the German *Google* decision, under §19(a) GWB, where it was argued that a gatekeeper may be prohibited from requiring users to consent to the processing of data from other services of the company or a third-party provider as a condition for using the services, without providing users with adequate options regarding how and for what purposes such data are processed.[119]

In addition, it is worth pointing out the CJEU's Facebook case, where it has been highlighted that even if the data controller is a dominant online platform -- this does not automatically invalidate the consent of the data subject.[120] According to the CJEU judgement, the validity of consent should be evaluated on a case-by-case basis, considering the extent of users' freedom of choice in refusing particular data processing requests, rather than being tied to the platform's dominant position.[121] Although the *Facebook* case addressed a competition law matter, the interpretation offered by the DMA might be similar to the notion of consent within Article 5(2) DMA. This approach supports a literal reading of Article 5(2) DMA, explicitly allowing gatekeepers to engage in data combination and cross-use activities following the acquisition of user consent. To some extent, the Facebook case ruling seems to challenge this idea by indicating that to ensure a user's consent is freely given (based on a combined interpretation of Article 102 TFEU and the GDPR), the user should have two viable options for contracting with the gatekeeper: either by providing data or by abstaining from

[118] DMA (n 104) article 5.

[119] Botta and Borges (n 113); Competition Act in the version published on 26 June 2013 (Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245), as last amended by Article 2 of the Act of 19 July 2022 (Federal Law Gazette I, p. 1214) (GWB); Bundeskartellamt, 'Decision B7-70/21, Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB, adopted in the administrative proceedings involving Alphabet Inc., Google Ireland Limited and Google Germany GmbH' <https://www.bundeskartellamt.de/SharedDocs/Entschei-> accessed 1 May 2024.

[120] *Meta Platforms* (n 41) para 147.

[121] ibid.

providing data. It is yet uncertain whether and to what degree individual gatekeepers will implement privacy settings to adhere to Article 5(2) DMA.[122]

Secondly, the potential intersection between DMA requirements and the prohibition of exploitative abuse of dominance raises concerns about the violation of the *ne bis in idem* principle. The relationship between the DMA and the competition law is defined by the DMA itself, which explicitly states that the DMA does not affect the application of Article 102 TFEU.[123] This means that practices considered as abusive under Article 102 TFEU should be still punishable even if they also breach the DMA, and vice versa.[124] In practice, there will be questions on how to combine the enforcement of EU competition law and the DMA optimally when dealing with dominant gatekeeper platforms.

In distinguishing between Article 102 TFEU and the DMA, it is necessary to differentiate between being tried twice and experiencing dual punishment. To start with, I turn to discuss the concept of being tried to be punished twice. The application of the DMA should not impede the application of Article 102 TFEU, provided they arise from the same circumstances.[125] Simultaneously, the conclusion of the proceeding under Article 102 TFEU should not preclude proceeding under the DMA. However, if the termination of a proceeding under one law means that a proceeding under the other law is no longer possible, it would contradict the assertion that DMA does not affect the application of competition law. In principle, Article 50 of the Charter prohibits subjecting the same defendant to be trialled again based on the same circumstances, after they have been finally convinced or acquitted.[126] Yet, the Commission approach suggests applying the CJEU's

[122] Botta and Borges (n 113).

[123] DMA (n 104) Articles 1(6) and Recital 10.

[124] T Breton, 'DSA/DMA Myths – Will the EU regulation create legal uncertainty?' (Blogpost, Linkedin, 2021) < https://www.linkedin.com/pulse/dsadma-myths-eu-regulation-create-legal-uncertainty-thierry-breton/?published=t> accessed 20 March 2024.

[125] DMA (n 104) Articles 1(6) and Recital 10.

[126] See, Case C-617/10 *Åkerberg Fransson*, Judgement of 26 February 2013, ECLI:EU:C:2013:105, para 34.

'threefold identity' case law.[127] It could also apply to the relationship between Article 102 TFEU and the DMA. Two arguments underpin this approach.

Firstly, the Commission indicates that competition law and the DMA serve different legal interests.[128] Such the distinction is protected in the legal interests at the core of competition law cases concerning the *ne bis in idem* principle, based on the "threefold identity" concept.[129] Presumably, the Commission is also likely to emphasise the disparity in protected legal interest to maintain the option of trying a defendant twice if necessary.[130]

Secondly, the Commission previously imposed a competition law fine on a company that faced penalties in national proceedings unrelated to competition law. In *Telekomunikacja Polska,* the Commission penalised Telekomunikacja Polska for breaching Article 102 TFEU after the Polish telecommunications authorities fined the company for a breach of national telecommunications law.[131] The Commission rejected the Telekomunikacja Polska's argument that it was a breach of *ne bis in idem* principle, referring to the requirement in competition case law for an identity of the protected legal interests, which was not present in this case.[132] The Commission adopted a similar approach in the *bpost* case, where the Commission argued for the application of the criterion of the identity of the protected legal interest, as applied in competition law.[133] Hence, the logical presumption is to indicate that the Commission stance's proposes a possible extension of the application of the "threefold identity" case law to the interaction between the DMA and Article 102 TFEU. This would

---

[127] Case T-329/01 *Archer Daniels Midland v Commission*, Judgement of 27 September 2006, ECLI:EU:T:2006:268, para. 290; Case T-38/02 *Groupe Danone v Commission*, Judgement of 25 October 2005, ECLI:EU:T:2005:367, para. 185; Case T-59/02 *Archer Daniels Midland v Commission*, Judgement of 27 September 2006, ECLI:EU:T:2006:272, para. 61

[128] Lukas Harta, 'Abuse of Dominance and the Digital Markets Act Big Tech companies at risk of double jeopardy' (CepInput, 2021) <https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepInput_Marktmissbrauch_und_DMA/cepInput_Abuse_of_Dominance_and_DMA.pdf> accessed 13 February 2023.

[129] ibid.

[130] ibid, 8.

[131] Case COMP/39.525 T*elekomunikacja Polska,* European Commission, 22.6.2011

[132] ibid, para. 135.

[133] Case C-117/20 *bpost*, Opinion of 2 September 2021, ECLI:EU:C:2021:680, para. 30.

effectively circumvent any issues with the legal principle of ne bis in idem and make trying a defendant twice appear unproblematic.

The CJEU has not expressed an opinion on the *ne bis in idem* principle application in the cases where competition law coincides with another area of law. The CJEU practice demonstrates that the court only has exclusively focused on the identity of the protected legal interest in cases related to competition law.[134] A preliminary review of existing case law indicates that the CJEU might, in fact, allow the Commission to prosecute twice. Such an assumption can be made on the fact that the courts have not yet invalidated a fine imposed by the Commission on the grounds of a violation of the *ne bis in idem* principle.[135]

However, the CJEU should exercise caution in applying the precedent established in cases concerning threefold identity to the interaction between Article 102 TFEU and the DMA. When assessing cases exclusively within the realm of competition law, the criterion of the threefold identity could be inappropriate, as the CJEU typically demands only the identity of legal facts, dismissing the requirement for the identification of the protected legal interests.[136] For the sake of clarity in interpretation of the *ne bis in idem* principle, it is advisable to abandon the criterion of identity of the protected legal interest in the context of competition law as well.[137] The interpretation of the *ne bis in idem* principle might vary across different legal spheres. However, in its fundamental essence, its interpretation should remain largely consistent regardless of the specific area of law involved.[138] The examination of whether the identity of the protected legal interest is a fundamental criterion is central to the essence of the *ne bis in idem* principle. Consequently, when interpreting Article 50 of the Charter, the emphasis should be not on the threefold identity criterion, which also requires the protected legal interest to be the same to prohibit a second trial, but solely on the identity of the defendant and the factual circumstances. Based on this rationale, there

---

[134] Case C-17/10 *Toshiba Corporation*, Opinion of 8 September 2011, ECLI:EU:C:2011:552, para. 116

[135] G Monti, 'The Digital Markets Act – Institutional Design and Suggestions for Improvement' (2021) TILEC Discussion Paper DP 2021-004.

[136] Harta (n 128).

[137] Case C-617/17 *Powszechny Zakład Ubezpieczeń na Życie*, Opinion of 29 November 2018, ECLI:EU:C:2018:976, para. 46; R Nazzini, 'Parallel Proceedings in EU Competition Law: *Ne Bis in Idem* as a Limiting Principle' in Bas van Bockel (ed) *Ne Bis in Idem in EU Law* (CUP 2016).

[138] See *Toshiba Corporation* (n 134); Case C-151/20 *Nordzucker,* ECLI:EU:C:2021:681, para. 39.

should not be a visible broadening of the application of the threefold identity criterion to the interaction between Article 102 TFEU and the DMA. Instead, the CJEU should concentrate exclusively on the identity of the defendant and the facts. If both criteria are met, a ruling under the DMA should prohibit proceedings under Article 102 TFEU, and vice versa.

Next, I address the potentiality of facing punishment twice. The Commission's stance on whether it is possible to punish an undertaking twice for breaching Article 102 TFEU and the DMA is less definitive.[139] The application of the DMA is "without prejudice" to the application of Article 102 TFEU.[140] In other words, if interpreted literally, the Commission could permit a dual punishment for a defendant. Otherwise, enforcing the DMA would impact the enforcement of Article 102 TFEU, particularly regarding sentencing. The DMA would influence the application of Article 102 TFEU to the extent that, during sentencing, the Commission would need to consider any fines imposed in DMA proceedings. Such interpretation finds its support in the case of *Telekomunikacja Polska*, discussed above.

Nevertheless, considering the established case law, it could be inferred that such an offset is mandatory. In instances where fines are imposed by competition authorities in Member States, the Commission is obliged to decrease the fines it imposed by the sum imposed by the Member State's competition authority for the same factual circumstances.[141] In fact, there is no rationale to suggest that the relationship between Article 102 TFEU and the DMA could change this. In both scenarios, the absence of identity of the protected legal rights is the reason why the prohibition of double jeopardy does not apply. Both instances involve the action of an undertaking within the European market, rather than actions in both the European and a non-European market. If Article 102 TFEU and the DMA overlap, the Commission will impose fines in both cases. This further supports the argument for an obligation to offset fines, as the connection between the two proceedings is stronger when the Commission manages both sets of proceedings, compared to situations where one takes place before the Commission and the other before a Member State authority.

---

[139] Harta (n 128).

[140] DMA (n 104) Articles 1(6) and Recital 10.

[141] Harta (n 128).

1.3. Hypothesis

Against this background, this thesis aims to analyse to what extent the existing EU competition law framework can effectively accommodate privacy-related harms in cases concerning the abuse of a dominant position as per Article 102 TFEU. While Article 102 TFEU traditionally focuses on price-related abuses, this thesis explores whether privacy-related harms arising from dominant firms' practices should also be recognised as a dimension of abuse. For example, the exploitation of users' data through exclusionary practices or coercive data collection methods by dominant undertakings might result in compromised privacy and distortion of the competitive process. By examining instances where privacy-related harms have potentially aggravated the abuse of dominance, this thesis investigates whether a broader interpretation of harm, beyond direct economic consequences, can be justifiable. The precise meaning of the competition perspective on user privacy appears problematic, as reduction of privacy may not necessarily amount to a competitive issue; any reduction in privacy equally may not immediately result in a privacy breach if data processors comply with data protection law.

To evaluate the aforementioned objective, the following hypothesis is considered.

Article 102 TFEU provides a sufficiently broad and flexible framework to address exploitative privacy-related harms, as it does not provide an exclusive list of theories of harm.[142] The Court in *Servizio Elettrico Nazionale* emphasised that Article 102 TFEU aims to protect "maintenance of the degree of competition existing in the market or the growth of that competition,"[143] and Article 102 TFEU intervenes in conducts "undermining an effective

---

[142] *TFEU* (n 5), Article 102: "Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist in:
(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
(b) limiting production, markets or technical development to the prejudice of consumers;
(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts."
Therefore, there are no clear theories of harm being deduced. The list of potential theories of harm could be over-inclusive.

[143] Case C-377/20 *Servizio Elettrico Nazionale* ECLI:EU:C:2022:379, para 44.

structure of competition"[144] It might be noted that the CJEU does not reduce Article 102 TFEU to only protecting consumer welfare, recognising its possible plurality of pursued goals. It is evident that substantive antitrust assessment focuses on competition problem that arises from firms' behaviour. The CJEU approach suggests that the dominant undertaking needs to engage in competition on the merits, which ensures the practice does not undermine the effective structure of competition otherwise seen as a violation of Article 102 TFEU.[145] In this view, the CJEU supports a broader consumer welfare approach, as a consolidating approach to Article 102 TFEU. AG Kokott discusses this as follows:

> "Regard must be had to the fact that independence of economic participants constitutes one of the basic requirements for competition to function. Accordingly, the provisions of the Treaty relating to competition are based on the concept that each economic operator must determine independently the policy which he intends to adopt on the common market."[146]

Here, two important aspects are provided about the independence of economic participates which allows for the healthy functioning of an internal market. Firstly, consumer welfare and competition law apply to a wide range of economic participants, not just businesses. Secondly, consumer independence is a crucial factor for healthy competition and is thus a fundamental requirement for well-functioning markets. In other words, when evaluating a possible consumer harm, it should encompass not only the negative impact on the consumer's choice but also the ability of consumers and all market participants to make autonomous decisions for themselves regarding economic issues.[147]

Privacy-related harms connote harms directed towards a digital consumer: the direct harm of the digital firms' extensive data acquisition could amount to exploitative theories of harm, where users are directly harmed, and privacy could be acknowledged as an element of

---

[144] ibid.

[145] ibid, para 45.

[146] Case C-8/08, *T-Mobile Netherlands BV, KPN Mobile NV, Orange Nederland NV and Vodafone Libertel NV v Raad van bestuur van de Nederlandse Mededingingsautoriteit* ECLI:EU:C:2009:110, para 52.

[147] See, Rupprecht Podszun, 'The Consumer as a Market Player: Competition Law, Consumer Choice and Data Protection in the German Facebook Decision' (SSRN, 2023) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4400552> accessed 17 October 2023.

abusive behaviour.[148] Competition authorities can take into account non-competition public policy considerations in the determination of whether a particular behaviour hampers competition and as a proxy to ensure fair competition and consumer welfare, as demonstrated in AG Rantos' and the CJEU's approach in *Facebook* case, where privacy-related harms were only admissible as a broader concern allowing to demonstrate competitive restrain.[149] In AG Rantos' opinion, the BKartA has not penalised a breach of GDPR by Facebook but applied the data protection rules under the framework of competition law. In other words, AG Rantos incidentally applied GDPR to review an alleged abuse of dominance.[150] The incidental consideration of GDPR comes into play as a balancing process. In such an instance, a possible incidental consideration of privacy-related harms in competition law would prescribe for a 'balancing process'. In fact, such approach will not constitute an expansion of the competition legal order to encompass other areas of law, such as data protection, for the simple reason that competition law relates to tacking harms caused by market failures and seeks to remedy competitive harm. Furthermore, the incidental consideration of GDPR in reviewing an alleged abuse of dominance does not render a mutual respect. Instead, competition law framework aims to identifying practices "undermining an effective structure of competition" as violating Article 102 TFEU,[151] whole data protection rules should be interpreted and applied to promote the market functioning. The fundamental principle is that when a competition authority uses its authority, it should consider various factors, including whether the behaviour being examined involves using strategies other than those typically seen in fair competition, all while considering the legal and economic context in which this behaviour occurs. In this respect, evaluating whether the conduct complies with or violates the GDPR, not in isolation but considering all the relevant circumstances, can be a significant indicator of whether the behaviour relies on methods that deviate from fair competition standards. Both general values on the maximisation of consumer welfare and social and political priorities, that shape enforcement, could be part of the competition law parameter, if they introduce competitive restrains on a relevant market. It is significant to note that EU competition law is not a standalone statute but rather a component of a larger framework known as the TFEU. Competition authorities may

[148] *Meta Platforms* (n 41).

[149] *Meta Platforms, Opinion of AG Rantos* (n 85); *Meta Platforms* (n 41).

[150] *Meta Platforms, Opinion of AG Rantos* (n 85) 18.

[151] *Servizio Elettrico Nazionale* (n 143).

decide each case by adapting general principles to the case at hand. To this end, possible value pluralism efforts, that provide a framework for striking a balance between competition law and data protection, can help courts and competition authorities make decision-making based on evidence, principles, and context. In practice, this does not mean that competition law will be a panacea for all privacy problems. Competition law could contribute to effective privacy protection if privacy-related concerns directly influence competition.

1.4. Structure of the thesis and methodological remarks

This thesis consists of four substantive chapters set out specifically to establish whether EU competition law might acknowledge the privacy-related harms in cases concerning the abuse of a dominant position as per Article 102 TFEU.

Chapter 2 discusses the theoretical characteristics of the intersection between competition law and privacy. The chapter discusses that the intersection between competition law and data privacy is at the early stage. This chapter discusses the domains between competition law and privacy, outlining three theories on the relationship between competition law and privacy — integrationist, separatist and value pluralism theories. The discussion in this chapter demonstrates that both separatist and integrationist views are not prescriptive enough to provide sufficient guidelines for interpreters. On the assessment of coordination between policies, it is important to state that EU competition law does not exist as a stand-alone statute but is a part of a larger framework — the TFEU. Hence, competition can arguably be influenced by many factors beyond mere data in a particular market. As per the theory of value pluralism, the competition law assessment should comprise values such as economic freedom, consumer welfare, fairness, and legal certainty. Thereby, the competition authorities might decide every case by tailoring general principles to the specific case in question. Essentially, the cases of potential mutuality between competition law and data privacy law, and not their complementarity, are the most complex cases for the courts and agencies, these demanding new analytical tradeoffs, and methodologies. Even if these two regimes demonstrate a different scope of applicability, it is accepted that privacy could be acknowledged as part of quality-based competition. For that purpose, possible value pluralism attempts to provide a framework for balancing between competition law and data protection may assist the courts and competition authorities in reaching a context-specific and principled decision. In fact, this is not to suggest that competition law would be

a panacea for every privacy concern: privacy law may be only balanced to establish competition law abuse. Interestingly, the most complex cases for courts and competition agencies stem from a potential link between competition law and data privacy law, rather than a simple association between them. The search for the objectives outlined in Article 102 TFEU reveals that the concept of consumer welfare is broad enough to encompass theories of harm that involve exploitation. The doctrinal methodology is applied to this end. Findings from the legal literature form the basis for a normative analysis of the broader implications of why antitrust and data privacy interact and how these interactions might be understood.

Chapter 3 investigates instances where privacy issues have been confronted within antitrust investigations aimed at countering data accumulation strategies. The chapter demonstrates the decision-making practice embraced three prescriptive positions in the development of the intersection between competition law and data protection: from stressing that protection of data privacy law remained outside the scope of competition law to considering that competition law could potentially consider any privacy infringement in the wider scope of the legal and economic context surrounding conduct in question. The three-phase approach shows how the EU courts interpreted the intersection between competition law and data protection law, which points from the separation of data privacy and competition law, towards apparent acknowledgement of privacy-related harms in competition law. Until now, competition law enforcers have frequently employed a "separationist" approach. This is partly attributed to the organisational structure of competition agencies and the economics-centred character of antitrust enforcement. The challenges confronted, especially by competition agencies in the digital age, increasingly underscore that, for effectiveness, competition law enforcers must no longer remain impervious to the impact of other fields of study.

Chapter 3 uses the *Facebook case* to discuss how demonstrates that the inherent clash between data protection and competition law cannot be resolved simply by invoking an alleged synergy or complementarity. The BKartA applied the German competition law to assess whether the requirement of giving consent to combine personal data from various sources was prohibited as an exploitative abuse by a dominant undertaking, using data protection law as a benchmark to establish the abusive nature of Facebook’s conditions. This

chapter puts the *Facebook case* into context and discusses the concerns brought up by BKartA Facebook's case and AG Rantos and the CJEU's ramifications. AG Rantos and the CJEU assessed the intersection between competition law demonstrating that the incidental analysis of data privacy law in competition law assessment might as a proxy for findings an exploitative abuse in a broader economic manner. This statement raises two main issues surrounding the role of privacy-related harms in competition law. Firstly, whether the consent, as per the GDPR meaning, could effectively be given to a dominant undertaking; and secondly, whether the BKartA was competent enough to find the GDPR infringement in their competition law investigation. More generally, this chapter focuses on the application of GDPR by competition authorities, noting competition law enforcers can no longer insulate themselves from the influence of other disciplines if its indirect consideration allows them to capture competitive harm. This chapter challenges the notion that privacy and antitrust have a synergistic and complementary relationship. Additionally, it argues that the principles upheld by the Facebook case decision may not provide a definitive resolution to this issue. This chapter applies a doctrinal methodology, focusing on analysis of the relevant decision-making practice, case law, policy, and literature.

As the findings from Chapters 2 and 3 suggest, both competition law and data protection aim to avoid personal data exploitation and privacy restrictions, even if each area of law has different theoretical underpinnings. Competition authorities have shown a greater level of interest in theories of harm connected to privacy because of the emergence of the digital economy. For the simple reason that competition law is related to addressing harms brought on by market failures, this should not be considered an expansion of competition law to that of other areas of law, such as data protection. Chapter 4 offers an examination of the assumptions surrounding the exploitative theories of harm underlying privacy analysis in competition law, which is lacking. The chapter emphasises exploitative theories of harm, as BKartA's *Facebook case* places consumers at the centre, with a consumer being seen as a person with a right to informational self-determination and an individual responsible for determining the winner of the competitive race by carefully evaluating the various proposals. One urgent concern arises with the growth of Big Data analytics and data acquisition: to what extent (if any) could privacy violations be included when evaluating the level of competition? Particularly, it is debatable if EU competition law could and should develop theories of harm applicable to privacy-related harms. The assessment is based on

the consideration that the relationship between internet privacy and competition law is positive and direct. With this consideration in mind, the emphasis is given to an emerging topic: whether the protection of individuals' privacy might act as an eminent element of abuse of dominance. The chapter explains that most data-related anticompetitive investigations are not expressly focused on individuals' data privacy. However, competition law agencies have recently paid attention to novel instances of digital market-based abuses of dominance. The chapter looks at such abuses of dominance to discuss to what extent undertakings could rely on improvements of privacy to avoid anticompetitive liability, within the Article 102 TFEU context. Though this theory is at an early stage, competition law cases and discussions have begun to question whether the increased protection for individuals' data privacy could justify otherwise anticompetitive conduct. This is one of the most nascent interactions on the horizon between competition law and data privacy law. A doctrinal legal research methodology is applied in this chapter to analyse relevant EU legislation, case law, policy documents and literature in the field of data protection and competition law.

Chapter 5 combines the finding from this thesis to create a new approach of interpreting the relationship between competition law and privacy. As such, chapter 5 attempts to set practical boundaries between competition law and data privacy law. Consumers' perceived "core theme" is a lack of control over their personal data, which could cause market failures and affect how well a market protects users' privacy. The chapter introduces the privacy-trap theorem, developed by the author as an attempt to demonstrate that in certain instances privacy infringements can act as a proxy to trigger competition law assessment, which demonstrates that competition law could only answer privacy-related concerns if they directly influence competition. The chapter aims to propose a practical nexus between competition law and privacy protection, as competition law enforcers can no longer insulate themselves from the influence data protection law. Here, it is noted that the relationship between competition law and privacy is complimentary but pursues different objectives: competition law works to ensure efficient competition, while privacy law seeks to protect individuals' data privacy. The exploitation of personal data is, however, only partially addressed by data protection regulations. The long-term harm to platform users is not recognised by data protection regulation, and dominant businesses in a market have a unique obligation to not misuse their position. The emerging digital economy has raised concerns on the interaction between competition law and privacy and the need for a more

articulate approach to these areas of law, as they both aim to avoid the exploitation of consumers privacy. Crucially, there is no analytical framework to define the relationship between competition law and data protection when it comes to privacy-related concerns. By recognising the aggregation of personal data as a potential source of market power, competition law enforcement might provide recourse where companies use their market power to inflict harm degrading privacy. Such conduct will be only possible by balancing competition law with data privacy. In order words, when determining whether a situation constitutes an abuse of dominant position, a crucial factor to consider is the effect of the conduct in question on the competitive dynamics. Hence, in the *Facebook case*, a supposed consent-related violation of the GDPR by Facebook does not automatically mean that any consent-related violation of the GDPR by any dominant company is abusive *ipso facto.* Instead, competition law will acknowledge data privacy as balancing finding out an abuse of dominance. This chapter aims to map out the points of intersection between competition law and data protection and discusses why they deserve scrutiny. Furthermore, this chapter also makes use of doctrinal legal research methodology, analysing the EU legislation, case law, policy documents and literature in the field of data protection and competition law.

Chapter 2: Competition law and privacy: a new interface

2.1. Introduction

The chapter discusses that the interface between competition law and data privacy is at the early stage. Although the interactions between competition law and data privacy are increasingly acknowledged, the legal theory and practice remain new. This chapter describes three theories on the relationship between competition law and privacy — integrationist, separatist and value pluralism theories. The chapter mentions a potential overlap between privacy law and competition law. Separatist and integrationist ideologies are not sufficiently prescriptive to give interpreters adequate guidelines. Practically, the Commission continues to hold the position that consideration of other public policy interests, such as data protection, cannot be factored into a competition assessment. Regarding the evaluation of policy coordination, it is significant to note that EU competition law is not a standalone statute but rather a component of a larger framework known as the TFEU. The competition authorities may decide each case by adapting general principles to the particular case at hand. The chapter argues that competition could be driven by different factors other than data in a particular market. In essence, the most complex cases for courts and agencies are those involving potential mutuality between competition law and data privacy law, rather than their complementarity; these cases call for new analytical trade-offs and methodologies. This chapter does not argue that complementarity is an inaccurate description of the argued interface, only that it is incomplete. It is possible to accept that privacy may act as a broader parameter in determining competition law infringement, even if these two regimes show a different scope of applicability.

2.2. The existing theories on relationship between competition law and privacy

2.2.1 Separatist and Integrationist views

The literature recognises two key opposing views on the intersection between competition law and privacy.[152] The first theory considers data protection law as beyond the consideration of competition law.[153] The theory is referred to as the separatist view, which emphasises a doctrinal separation between EU competition mandate and its data protection mandate. Arguably, the separatist view originates from the *Asnef-Equifax* case,[154] where the CJEU rejected the interplay between competition law and data protection rules by stressing that data protection law was outside the scope of competition law. The CJEU found 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".[155] Essentially, the separatist theory views competition law and privacy as "complementary [in] nature," but not overlapping.[156] The central argument remains that incorporation of privacy concerns in competition law assessment would create confusion, especially when applied to consumer welfare standards.[157]

---

[152] Joseph Phelps, Glen Nowag and Elizabeth Ferrell, 'Privacy Concerns and Consumer Willingness to Provide Personal Information' [2000] J Public Policy Mark 27; Philipp Dimakopoulos, Slobodan Sudaric, 'Privacy and Platform Competition' (2017) Rationality & Competition Discussion Paper No 67 <https://rationality-and-competition.de/wp-content/uploads/discussion_paper/67.pdf> accessed 4 April 2020; Stefan Larsson, 'Putting trust into antitrust? Competition policy and data-driven platforms' (2021) 36 (4) European Journal of Communication 391; Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 Common Market Law 11; A Witt, 'Data, Privacy and Competition Law' (2021) Graz Law Working Paper No 24-2021 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3989241> accessed 16 April 2023; Agustin Reyna, 'Interdisciplinary Enforcement in Competition and Data Protection Law' (BEUC 2023) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4349827> accessed 16 April 2023.

[153] See, Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' [2015] Antitrust LJ 121, 138-43; James C Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity' [2013] Geo Mason L Rev 1129, 1146.

[154] *Asnef-Equifax* (n 89).

[155] ibid para 177; see also Case M.9660 – *Google/Fitbit* (Commission decision of 17 December 2020)

[156] Ohlhausen and Okuliar (n 153) 138-43.

[157] ibid, 139.

On the contrary, the integrationist approach accepts the inclusion of privacy into the competition law framework.[158] This is an expression of the long-standing debate as to whether competition law should include non-price elements in its substantive analysis.[159] Based on that, both price and non-price factors might improve consumer welfare. There is evidence to suggest that privacy and competition law could be integrated together or acknowledged as complimentary. For example, in 2014, European Data Protection Supervisor (EDPS) argued that:

> "privacy and the protection of personal data should be considered not as peripheral concerns but rather as central factors in the appraisal of companies' activities and their impact on competitiveness, market efficiency and consumer welfare."[160]

This is given as consumers are data subject, "…whose welfare may be at risk where freedom of choice and control over one's personal information is restricted by a dominant undertaking."[161] For that reason, the EDPS argued out of necessity to develop concepts of consumer harms, articulating the violations of data protection rights.[162] Essentially, when there is evidence that companies compete to offer privacy protection to consumers,[163] the integrationist approach considers if privacy-based competition might be impacted. This taxonomy may be both exploitative and exclusionary. Let us consider the practices of a hypothetical dominant internet-based company. In data-driven markets, consumer behaviour can be subject to biases in decision-making, which might steam from

---

[158] EM Douglas, 'Digital Crossroads: The Intersection of Competition law and Data Privacy' (2021) Temple University Legal Studies Research Paper No. 2021-40 <https://iapp.org/media/pdf/resource_center/Digital_Crossroads_The_Intersection_Competition_Law_Data_Privacy.pdf> accessed 4 August 2021; Wolfgang Kerber, 'Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law' [2022] The Antitrust Bulletin 280; Adrian Kuenzler, 'What competition law can do for data privacy (and vice versa)' [2022] Computer Law & Security Review 1.

[159] Christopher Townley, *Article 81 EC and Public Policy* (Hart Publushing 2009); G Monti, 'Article 81 EC and Public Policy' (2002) 39 Common Market Law Review 1090; O Odudu, *The Boundaries of EC Competition Law, the Scope of Article 81 EC* (OUP 2005); T Prosser, *The Limits of Competition Law* (OUP 2005).

[160] EDPS, 'Preliminary Opinion of the European Data Protection Supervisor. 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.

[161] ibid, 33.

[162] ibid, 34.

[163] Frank Pasquale, 'Privacy, Antitrust, and Power' [2013] Geo Mason L Rev 1009, 1009.

misinterpretation of their willingness to pay or the perception of quality offered.[164] Consumers could make unreasoned predictions about their demand: this might lead to consumer exploitation in the sense that such a dominant internet-based company collects more data than what consumers are willing to give if they had accurate expectations.[165] For example, if consumers use a data-fuelled product, then they have expectations to be informed on the extent of data collected and processed.[166] If privacy protection acts as a dominant internet-based firm's product or service feature, then consumers might be exploited if they make misjudgment of that quality, when end users are subject to behavioural manipulation. Hence, individuals' privacy protecting decisions could be influenced by an uncertain nature of privacy tradeoffs, in the context of commercial interest manipulation, which arguably can act as guiding the assessment of data-related anticompetitive harms.[167] In other words, arguably, there is a normative and dogmatic link between competition law and privacy protection in cases where a digital business model is based on the processing of personal data.

On a fundamental level, competition and data protection laws achieve different objectives.[168] Competition law aims to ensure undistorted competition within the internal market.[169] Competition is conceived as the best means to ensure allocation of resources and

---

[164] M Motta and M Peitz, 'Intervention trigger and underlying theories of harm - Expert advice for the Impact Assessment of a New Competition Tool' (EU Commission, 2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/kd0420575enn.pdf> accessed 12 November 2022.

[165] Case 26/75 *General Motors v Commission* [1975] ECR 1367; In the scope of traditional competition law, the practice of charging monopoly prices is a form of exploitative abuse: it is an abuse if prices are excessive when they do not reflect the good's economic value. I discuss this argument in relation to digital subscription fees and privacy in chapter 4, see section 4.2.3.

[166] Examples will be provided throughout this thesis. The most notable example remains the *Facebook case* (n 2), discussed in section 3.5.1. in Chapter 3.

[167] *Meta Platforms, Opinion of AG Rantos* (n 85).

[168] Maurice E Stucke and Allen P Grunes, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' [2015] Antitrust Source 1, 4; B Kira, V Since and S Srinivasan, 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' [2021] Industrial and Corporate Change 1337; Kuenzler, (n 158).

[169] Christopher Decker, 'Concepts of the Consumer in Competition, Regulatory, and Consumer Protection Policies' [2017] J Competition L & Econ 151, 156; A Lamadrid, 'On Privacy, Big Data and Competition Law (2/2) On the nature, goals, means and limitations of competition law' (Chillin'Competition, 2014) < https://chillingcompetition.com/2014/06/06/on-privacy-big-data-and-competition-law-22-on-the-nature-goals-means-and-limitations-of-competition-law/> accessed 6 July 2020; Simon Bishop and David Walker, *The Economics of EC Competition law — Concepts, Application and Measurements* (2nd ed, Sweet & Maxwell 2002) 20-21.

increase consumer welfare.[170] Consumer welfare is increased when consumers enjoy low prices, better quality and wider choice of innovative products or services.[171] In contrast, data protection law aims to ensure that individual consumers' right and interests as the data subjects will not be unfairly disadvantaged. Essentially, data protection does not exist solely as an element of quality within competition law analysis. Rather, data protection is a separate legal doctrine, one at odds with promoting competition. The basic approach of data protection law is that consumers have the right to control their personal data processing, by giving an informed consent; consumers as data subject should be able to decide what personal data is collected and for what purposes.[172] In other words, GDPR is focused on the informed choices of individual consumers and their reasonable expectations of data privacy.[173]

Both integrationist and separatist theories fail to explain how competition law interacts with data protection law in its capacity as a distinct legal doctrine. Separatist theory assumes any interaction between competition law and privacy as separate. However, the separateness of competition law and privacy does not preclude their mutuality. It remains correct to observe significant attempts to acknowledge an apparent mutuality between competition law and privacy. Data protection law would be highly relevant as a separate area of law that reduces competition and seeks disparate consumer data treatment. We are reminded that competition law should be based on economic objectives, while rejecting different social

[170] European Commission, 'Guidelines on the application of Article 81(3) of the Treaty' (2004/C 101/08) para 5: "Goals pursued by other Treaty provisions can be taken into account to the extent that they can be subsumed under the four conditions of Article [101(3)]"; Ohlhausen and Okuliar (n 153).

[171] Guidance on the Commission's Enforcement Priorities in Applying Article 82 (n 87) para 11: 'In this Communication, the expression "increase prices" includes the power to maintain prices above the competitive level and is used as shorthand for the various ways in which the parameters of competition — such as prices, output, innovation, the variety or quality of goods or services — can be influenced to the advantage of the dominant undertaking and to the detriment of consumers."

[172] GDPR (n 57), article 4.

[173] Pasquale (n 163).

and political considerations.[174] It is correct to assume that competition law remains doctrinally separate from external factors to competition policy issues, as competition law cannot act as a panacea for every social concern.[175] According to Ezrachi, such a puristic vision of competition law could be a mere illusion.[176] As discussed later, EU competition law is not designed as an impermeable discipline.[177] Categorically, with respect to the application of competition law to privacy-related harms, we are left with a problem. Even if we focus on competition as a means to only promote welfare, we are not able to categorically dismiss arguments based on market failure. In consequence, it is prudent to weight arguments carefully: competition law should continue to assess decisions involving personal data if personal data breaches are introduced in a wider scope of the legal and economic context surrounding the conduct.

The central disagreement between the separatist and integrationist views is whether privacy is a factor of competition law analysis. This is a significant question which I consider throughout this thesis. However, this question does not only consider the intersection between competition law and privacy, but also considers if privacy could constitute a part of the competitive theory of harm. Essentially, it remains unclear if privacy amounts to a quality factor or if privacy-harms should be considered in the wider scope of the legal and economic context surrounding anticompetitive conducts. Nonetheless, the argument that these two areas of law could intersect has merit. This argument does not prove that there is a hard conflict of law in which competition law requires actions that data protection law

---

[174] Ariel Ezrachi, 'Sponge' [2016] J Antitrust Enforc 1 for a discussion on whether competition law is a stable discipline. The article provides an overview of whether competition law could encompass non-economic goals. In the first line of the article, Ezrachi quotes R Hewitt Pate's speech: "What is the proper role of a competition agency? I think that is easy to sum up: promoting competition. Competition enforcers need to remain narrowly focused. There is a danger in focusing within our discipline on anything other than efficiency and consumer choices in making our decisions", (R Hewitt Pate, 'Competition and Politics' [6 June 2005] <http://www.justice.gov/atr/public/speeches/210522.htm> accessed 15 October 2022)

[175] See mostly, Ezrachi (n 174) It is beyond the scope of this thesis to provide a detailed discussion on the goals of competition law. For a discussion on the economic approach to competition law see Dieter Schmidtchen, Max Albert and Stefan Voigt, *The More Economic Approach to European Competition Law* (Mohr Siebeck 2007); Josef Drexl, Wolfgang Kerber and Rupprecht Podszun, *Competition Policy and the Economic Approach* (Edward Elgar 2012); Daniel Zimmer, *The Goals of Competition Law* (Edward Elgar 2012); Michal S. Gal, 'The Social Contract at the Basis of Competition Law: Should We Recalibrate Competition Law to Limit Inequality?' in Damien Gerard and Ioannis Lianos (eds), *Competition for the People* (CUP 2019)

[176] Ezrachi (2016) (n 174).

[177] ibid; Townley (n 159); Monti (n 159) 1090.

prohibits. GDPR offers only a partial response to personal data exploitation and fails to recognise the long-term harms to the platforms' users.

2.2.2. Theory of value pluralism

Both separatist and integrationist views are not prescriptive enough to provide sufficient guidelines for interpreters. From a practical perspective, the Commission's stance remains that competition assessment cannot take into consideration other public policy interests, such as data protection.[178] On the assessment of coordination between policies, it is important to state that EU competition law does not exist as a stand-alone statue but is a part of a larger framework — the TFEU.[179] Thereby, the competition authorities might decide every case through tailoring general principles to the specific case in question. In fact, the conceptual context of EU competition law implies the absence of a single unifying policy, as competition law does not exist in a vacuum and interwove with the society's values.[180]

Over the issue of the influence of external policies on competition law, the works of Townley or Van Rompuy identified four potential scenarios for coordination of EU external to competition policies.[181] The first scenario is referred to as the exclusion scenario — the TFEU enables for the potential external policy value to override and exclude competition policy — e.g. Article 346(1) TFEU "take measures for the protection of the essential interests of their security". Secondly, there is a possibility to 'compromise' — competition law would act as a balancing process if violations of competition law could be balanced, thereby acting like a 'balancing process'. Potentially, there are no instances of such balancing clauses. The same authors include the example of Article 34 TFEU, which could be balanced against any explicit public policy criterion. Thirdly, the TFEU introduced 'policy-linking' or 'cross-sectorial' clauses which require competition enforcement to consider other polices in 'definition and implementation'.[182] Such classes are recognisable in relation to environmental policy,

---

[178] *Asnef-Equifax* (n 89); Google/Fitbit (n 155).

[179] Guidelines on the application of Article 81(3) (n 170) para 42: "Goals pursued by other Treaty provisions can be taken into account to the extent that they can be subsumed under the four conditions of Article [101(3)]."

[180] William Galston, 'The Idea of Political Pluralism' in H Richardson and M Williams (eds), Moral Universalism and Pluralism (New York University Press 2008).

[181] B Van Rompuy, *Economic Efficiency: The Sole Concern of Modern Antitrust Policy* (Kluwer Law International 2012); Townley (n 159) 52-53.

[182] Townley (n 159) 53.

culture, and consumer protection. The fourth scenario relates to the silence of the TFEU. In this respect, the issue is left to any case law determination and traditionally it is intended to ensure a consistent interpretation across various policies and refuses to consider each policy in separation.[183] In practice, the Commission held that the protection of employment,[184] media pluralism,[185] environmental protection,[186] or regional development[187] could be seen as legitimate factors to be considered when reviewing agreements as per Article 101(3) TFEU. Furthermore, in the cases such as *Port of Genoa*[188] and *GVG/FS*,[189] the Commission examined the claims of dominant undertakings with the reasoning that anticompetitive conduct is objectively necessary for public policy considerations. Also, the EU Merger Regulation imposed the obligation upon the Commission to conduct the competition assessment with the consideration to achieve EU fundamental objectives.[190] Competition law cannot be reduced to a sole value, as it is not based on a unitary value. Arguably, competition law assessment comprises values such as economic freedom, consumer welfare, fairness, and legal certainty. EU competition law could be pluralistic in nature and seek an overlapping consensus to protect competitive equilibrium.[191] However, EU

---

[183] Case 283/81 *CILFIT and Lanificio di Gavardo SPA v Ministry of Health* (1982) ECHR 3415, para. 20.

[184] Case 42/84 *Remia v Commission* [1985] ECR 2545; Joined Cases 209/78 to 215/78 – *Heintz van Landewyck SARL v Commission* [1980] ECR 3125; Commission Decision of 4 July 1984, 84/380/EEC *Synthetic Fibres*, OJ 1984, L207/17.

[185] Commission Decision of 25 November 1981, IV/428, *VBBB/VBVB*, 82/123/EEC, OJ 25 February 1982, L54/36; CJEU 17 January 1984, *VBVB and VBBB vs. Commission*, Joined Cases 43 and 63/82*ECR*, 1984, p. 19; Commission Decision of 11 June 1993, IV/32.150 - *EBU/Eurovision System*, 93/403/EEC, *OJ*, 22 June 1993 L179/23, para. 62.

[186] See, Commission Decision of 8 December 1983, IV/29.955 – *Carbon Gas Technologie*, 83/669/EEC, *OJ*, 31 December 1983, L 376/17; Commission Decision of 12 December 1990, IV/32.363 – *KSB/Goulds/Lowara/ITT,* 91/38/EEC, *OJ*, 25 January 1991, L 19/25, para. 27; Commission Decision of 14 January 1992, IV/33.100 *Assurpol*, 92/96/EEC, OJ, 14 February 1992, L 37/16, para 38; Commission Decision of 24 January 1999, (IV.F.1/36.718. – *CECED*), 2000/475/EC, OJ 26 July 2000, L187/47, paras 51, 57; Commission Decision of 17 September 2001, COMP/34493 – DSD, 2001/837/EC, *OJ*, 4 December 2001, L319/1; Commission Decision of 16 October 2003, COMP D3/35470 — *ARA;* COMP D3/35473 — *ARGEV, ARO*, 2004/208/EC, *OJ*, 12 March 2004, L 75/59.

[187] Commission Decision of 23 December 1992, IV/33.814 - *Ford Volkswagen*, 93/49/EE, OJ, 28 January 1993, L20/14.

[188] Commission Decision 97/745/EF *Port of Genoa* [1997] L 301/27, para 21.

[189] Case No COMP/37685, *GVG/FS* (2004) para 136.

[190] Council Regulation (EC) No. 139/2004 on the Control of Concentrations between Undertakings (the EU Merger Regulation) [2004] OJ L24/1, recital 23.

[191] John Rawls, *Political Liberalism* (Columbia University Press 1993) 133-171.

competition law is unable to escape the unfavourable fact that antitrust, if applied broadly and without consideration of the underlying circumstances, may serve to restrict or even outright forbid large swaths of activity that the average European would deem to be extremely worthwhile.

From a data privacy perspective, enforcers, courts, and digital platforms are left with opposing legal pressures on personal data treatment. Data is valuable on the market and confers a competitive advantage. Hence, the increased appetite for data inevitably leads to collecting and processing of more data. In turn, this leads to enhanced profiling and insight about consumer preferences, and less online privacy. These tensions could encourage innovation brought about by data-driven competition with more competition enhancing consumer welfare. However, several unanswered questions remain, mainly what, and to what extent, should competition be traded at the margins for data privacy? This fluctuates around understanding privacy harms as competition harm law. However, companies, courts, and enforcers, preoccupied with analysing the complementarity between competition law and data privacy, are left with little understanding of how to address the exact nature of the relationship between competition law and data privacy law.

2.2.2.1 Assessing privacy-as-quality theory

While antitrust enforcers focused on price effect of products and services over the past few decades, one of concert of market power is degraded quality.[192] In situations where the digital product or service depends on harvesting and exploiting users' data, the digital provider's motive changes. It might reduce privacy protection and collect personal data above the competitive levels,[193] which could lead to exploitation of end users.

[192] See Maurice E Stucke and Ariel Ezrachi, 'When Competition Falls to Optimise Quality: A Look at Search Engines' [2016] Yale JL & Tech 70; Case ME/5525/12-Anticipated acquisition by Facebook Inc of Instagram Inc, 14 August 2012; also, Case AT.39740 *Google Search (Shopping),* 27 June 2017, paras. 273- 284
where it was found that "Google could alter the quality of its general search service to a certain degree without running the risk that a substantial fraction of its users would switch to alternative general search engines".

[193] See for example, 'Online Platforms and Digital Advertising Market Study' (n 1) para 2.84.

The theory of 'privacy-as-quality' is the most widely articulated perspective on the relationship between competition law and privacy.[194] The theory of 'privacy-as-quality' considers an increase or decrease in privacy in instances where privacy acts as a parameter of quality affected by competition in a market, and may generally negate consumer welfare.[195] Competition law at its core is concerned with a market power that negatively impacts consumer welfare;[196] the Commission Guidelines further determined that consumer welfare is considered by assessment of price and other factors, including innovation, choice and quality.[197] However, the reliance on price as a quality factor breaks down when a product or service is offered for free, as proved by the digital economy, which introduces an exponential increase of zero-priced services and products. Personal data collected by such entities is an alternative method of payment for accessing zero-priced digital products, or a dimension of the quality.[198] In such instances, privacy is attracting attention as a quality parameter: in *Microsoft/Yahoo!,* the Commission indicated that when a product is offered for free, quality becomes an essential competition parameter.[199] This reasoning has been acknowledged by the Commission in *Facebook/WhatsApp* and *Microsoft/LinkedIn* merger, as discussed in Chapter 3.[200]

---

[194] Geoffrey A Manne and R Ben Sperry, "The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework" [2015] CPI Antitrust Chronicle 1, 3-5; S Esayas, 'Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism' [2017] Faculty of Law, Stockholm University Research Paper No 43 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075239> accessed 17 November 2022; Douglas (n 158).

[195] TFEU (n 5) article 102; Katharine Kemp, 'Concealed data practices and competition law: why privacy matters' [2020] European Competition Journal 628; Lapo Filistrucchi, Damien Geradin, Eric van Damme, Pauline Affeldt, 'Market Definition in Two-sided Markets: Theory and Practice' [2014] JCL& E 293; Steven J Davis, Jack MacCrisken and Kevin M Murphy, 'Economic perspectives on software design: PC operating systems and platforms' in David Evans (ed) *Microsoft, Antitrust and the New Economy: Selected Essays* (Kluwer 2002) 361; Case C-27/76 *United Brands Company and United Brands Continentaal v Commission*, [1978] EU:C:1978:22.

[196] The concept of "dominance" has been traditionally understood as "a position of economy strength" enjoyed by a particular undertaking in a particular market. Such position has enabled that dominant undertaking to influence the conditions under which that competition will develop. See *United Brands* (n 195) paras 65, 113; Case C- 85/ 76, *Hoffman-La Roche & Co v Commission* [1979] ECR 461, paras 38-39.

[197] Guidance on the Commission's Enforcement Priorities in Applying Article 82 (n 87) para 19.

[198] Eleonora Ocello, Cristina Sjödin, and Anatoly Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case' (2015) 1 European Commission-Competition Merger Brief 6; Mauro Luis Gotsch and Marcus Schögel, 'Addressing the privacy paradox on the organizational level: review and future directions' [2023] MRQ 263.

[199] Case No COMP/M.5727 – *Microsoft/Yahoo!* OJ L 24, 29.1.2004, para 101.

[200] See for example *Facebook/WhatsApp* (n 90) para 125, and FTC, *Google/DoubleClick* [2008] FTC File No. 071-0170 6: "[W]e investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as consumer privacy."

Several antitrust agencies view the ‘privacy-as-quality' theory as limiting their role in assessing privacy concerns. Such examples are covered in more detail in Chapter 3 when I discuss the Commission and Courts response to measuring privacy in competition law assessment. The current approach underlines no nexus between competition law and standalone privacy-related harms.[201] In other words, ‘pure’ privacy harms are seen as being beyond the scope of competition law, and they should be resolved based on data privacy law. However, digital markets have unquestionably linked competition law with data privacy law concern: the ability to collect and process unlimited quantity of data placed companies in a position where the data helps them to achieve a stronger position in the market. The major concern is, therefore, how privacy affects competition law. Potentially, it could be possible to inject privacy-related harms, which are non-economic, and subjective or normative, into the competition law realm. However, competition law authorities should remain careful and should not overextend its own remits. For purposes of clarity, competition law and data protection should remain distinct. This should not constitute an expansion of the competition legal order to encompass other areas of law, such as data protection. If competition law enforcement considered any possible data protection breach within its assessment, this could disturb the functioning of consumer welfare by blending in non-economic harms. Arguably, such an argument is invoked both in response to calls for competition law to protect privacy, and in opposing the application of competition law to pursue broader, unrelated to economic efficiency, social goals.[202]

There could be two reasons why incorporating privacy-as-quality is not straightforward. Firstly, to consider privacy as a part of a digital service or product's quality, consumers have to emphasise privacy protection relative to other product attributes, including price.[203] Simultaneously, such consumers have to be able to evaluate digital firms' privacy policies. This reasoning assumes that consumers have a limited ability to choose products and services that correspond with their privacy preferences. If information asymmetries limit

[201] *Asnef-Equifax* (n 89) para 177.

[202] *Google/DoubleClick* (Case COMP/M.4731) Commission Decision [2008] OJ C184/10

[203] Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' [2016] J Econ Lit 422, 476; Y Himeur, S Saquib Sohail and F Bensaali, 'Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives' [2022] Computers & Secuty 1; Avi Goldfarb and Verina F Que, 'The Economics of Digital Privacy' [2023] Annu Rev Econ 15.

consumer choice of products and services that align with their privacy preferences, this could in turn reduce privacy-based competition. Swire argued that privacy harms reduce consumer welfare.[204] His research reasoned that it would be illogical to "count the harms to consumers from higher prices while excluding the harms from privacy invasions – both sorts of harms reduce consumer surplus and consumer welfare in the relevant market."[205] It transpires that users care about their personal data being collected and processed. Tsai indicated that consumers where likely to take more radical privacy choices when choosing 'discrete' products.[206] However, if consumers were to choose daily products, they demonstrated no requirement for a greater privacy protection. In this respect, Swire added that "[f]or these individuals, their consumer preferences are subject to harm if standard online surfing shifts to a less privacy-protective structure due to a merger or dominant firm behaviour."[207] Secondly, increased collection of personal data does not directly increase digital firms' profits. Instead, the data must be processed into something of value, creating benefits at least for consumers. In this respect, there could be other issues associated with reducing privacy quality, such as exploitative terms and conditions offered. As discussed in this thesis, all these considerations might suggest a normative link between digital firms' market power and users' privacy protection.

Regardless of its acceptance, the measurement of privacy-related competitive effect is likely to introduce practical challenges. At all stages, competition law analysis applies price-centric methodology and tools.[208] Price remains the cornerstone for competition modelling and analysis, and guided competition assessment from market power analysis to competitive effects of conducts and mergers.[209] The application of non-price considerations has been

---

[204] Peter Swire, 'Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall' (18 Oct 2007) <www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf> accessed 12 June 2020.

[205] ibid.

[206] Janice Tsai, Serge Egelman, Laurie Cranor and Alessandro Acquisti, 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study' [2011] Information System Research 234.

[207] ibid.

[208] I Lianos, 'Competition Law for the Digital Era: A Complex Systems Perspective' (2019) CLES Research Paper Series 3, 15–31; L Coppi and M Walker, 'Substantial Convergence or Parallel Paths? - Similarities and Differences in the Economic Analysis of Horizontal Mergers in the US and EU Competition Law' (2004) 49(1) Antitrust Bulletin 101.

[209] See for example, Case 26/76 *Metro SB-Großmärkte* v *Commission* [1977] ECR 1875, para 20.

recognised as a challenge for competition analysis.[210] For instance, in the *Microsoft/LinkedIn* merger, the Commission indicated that privacy might be acknowledged in the competitive assessment when the consumer sees it as "a significant factor of quality."[211] This indicated that data privacy was, arguably, an important parameter of competition that can be negatively affected by the merger.

Accordingly, if reduction of a product's quality is actionable under competition law and consumers see privacy as an aspect of quality, then reduction of privacy could arguably be seen as consumer harm in any competition assessment. Following the approach of privacy reduction as reduction of product's quality, the EU authorities noted that any privacy-related harms correspond to elements of a product or service quality. For example, in *Facebook/ WhatsApp* merger case, the Commission considered the parameter of privacy as a key quality-based element of a mobile communication apps' quality.[212] The greater protection of user privacy offered by WhatsApp allowed the Commission to conclude that the parties were not close to being competitors. As I note later, the discussion of privacy protection offered by the platforms was crucial. The Commission noted that with the high level of privacy protection offered by WhatsApp, Facebook was unlikely to retract WhatsApp's end-to-end encryption and introduce the element of targeted advertising on WhatsApp. In addition, in *Microsoft/LinkedIn,* the Commission further added that privacy was an important element of competition amongst professional social networks.[213] It was noted that transactions could indirectly impact privacy. Such reasoning was based on the consideration that LinkedIn could have been promoted on Microsoft's operation system. Microsoft could foreclose and marginalise any professional social network competitor, including such networks offering the highest level of privacy protection. Therefore, Microsoft offered remedies that allayed the foreclosure concerns and precluded any effects on privacy. Cognitive bias, information asymmetry and limited choice could make consumers unwilling or unable to switch to different services or products.

---

[210] C-439/09 *Pierre Fabre Dermo-Cosmétique* EU:C:2011:649, paras 39–40.

[211] European Commission, 'Press release, Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (2016) < https://www.europeansources.info/record/mergers-commission-approves-acquisition-of-linkedin-by-microsoft-subject-to-conditions/> accessed 10 September 2021; *Microsoft/LinkedIn* (n 90).

[212] *Facebook/WhatsApp* (n 90).

[213] *Microsoft/LinkedIn* (n 90).

The lack of established analytical tools is a significant barrier to any potential integration of privacy and any assessment of potential privacy-related harms in the realm of competition law. The common analytical tool to assess the hypothetical monopolist paradigm is the price effect assessment, which considers a fictional monopolist imposing a small but significant non-transitory increase in the price test (SSNIP test) of its services and products.[214] For the purposes of this chapter, the point is that the application of the hypothetical monopolist's test in a zero-price market is inappropriate. Consumers do not pay a/any monetary fee for the services or products; only non-price factors drive their product choice. This point could be further demonstrated in the *Google (Search) Shopping* case.[215] Google offers its search engine platform for free, and accumulates its revenues with advertising modes, exploiting the indirect network effect. In Google Search (Shopping), the zero-priced side of the market cannot be analysed with a traditional SSNIP-test which is based on price.[216] As Google offer its search engine service at no cost, it remains difficult to conduct a traditional price-centric model of consumer welfare harm. Usually, any consumer welfare harm might be assessed using the SSNIP test which bases its understanding on the price-element to measure potential abuse. However, in the digital economy, price is an unsuitable concept, as most products/services are offered ostensibly free for consumers. In this consideration, antitrust analysis might apply a small but Significant Non-Transitory Decrease in Quality (SSNDQ) test to define relevant markets.[217] At the time of writing this thesis, there have been no instances where this analytical approach has been applied to define markets, specifically on the basis of privacy protection or quality. According to Lande: "a merger which significantly reduces the intensity of competition in any information-based market must be examined for its potential effects on all dimensions of competition – including privacy – rather than just for its price effects."[218] The Cremer Report on EU competition policy observed that the SSNDQ

---

[214] European Commission, 'Notice on the definition of relevant market for the purposes of Community competition law' 97/C 372/03 [1997] OJ C372/5.

[215] *Google Search (Shopping)* (n 192).

[216] Council Regulation (EC) of 5 February 2004 on Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2004/C 31/03) [2004] OJ C 31/5, chapter 4.1; *Google Search (Shopping)* (n 192).

[217] Aleksandra Gebicka and Andreas Heinemann, 'Social Media & Competition Law' [2014] World Competition 149, 158.

[218] ibid.

test application is challenging: "[the] idea is probably more useful as a loose conceptual guide than as a precise tool that courts and competition authorities should actually attempt to apply."[219]

The precise measurement of effects on privacy quality could be challenging. This could include heterogeneity of consumer privacy preferences or tradeoffs between privacy and different product features. Essentially, antitrust analysis is sufficiently resilient to adapt to the technological changes and zero-priced markets. For example, Germany introduced legislation to clarify that zero-priced services and products do not preclude findings which relate to antitrust markets.[220] However, it remains unclear how to apply price-focused tools to evaluate the effects of privacy distortion on competition. The lack of established tools to evaluate privacy effects act as a significant barrier to the integration of privacy into antitrust analysis.

2.3. From theory to practice: pluralism of Article 102 TFEU

Competition could be driven by different factors other than data in a particular market. This thesis does not argue that complementarity is an inaccurate description of the interface being argued, just that it is incomplete. The prevailing view remains that the two areas of law can complement each other. Although the two regimes have different areas of application, it is recognised that privacy can be recognised as part of quality-based competition. To this end, possible value pluralism efforts that provide a framework for striking a balance between competition law and data protection can help courts and competition authorities make decision-making based on evidence, principles, and context. In practice, this does not mean that competition law will be a panacea for all privacy problems. Instead, within the framework of value pluralism, the evaluation of competition law should include values such as economic freedom, consumer welfare, fairness, and legal certainty.

This section analyses Article 102 TFEU in relation to the aforementioned approaches. The analysis involves two main aspects: (1) it scrutinises the Court and competition authorities' objective in deterring whether a single objective of Article 102 TFEU motivates the

[219] Cremer Report (n 1).

[220] Act Against Restraints of Competition 2013, as last amended by Article 10 of the Act of 12 July 2018

judgements; (2) it reconsiders Article 102 TFEU to assess a possible degree of adaptability in acknowledging detriments about privacy.

2.3.1. Article 102 TFEU and the value pluralism: preliminary observations

Both integrationist and separatist views cannot wholly explain whether Article 102 TFEU could acknowledge relevant privacy-related harms. Value pluralistic theory is supported by the conclusion that it is possible to endorse a plethora of goals concerning Article 102 TFEU, as it does not claim to be a complete normative theory. Instead, it is based on the consideration that there is no need for strict prioritisation of competition law objectives.

Over the years, EU competition law has relied on the economic parameters which allow to demonstrate consumer harm, such as by monitoring prices or possible reduction in input, quality and/or innovation.[221] Article 102 TFEU hinges on the concept of abuse which is "recourse to methods different from those which condition normal competition,"[222] but also indicates that a dominant undertaking's conduct may "impair genuine, undistorted competition."[223] It should be first noted that there is no general contradiction between public interest concerns and the objective to protect competition. For example, the CJEU has held that the concept of abuse might be examined regarding other areas of law.[224] Arguably, safeguarding competition would also lead to achieving public policy objectives, especially where consumers expect such outcomes.[225] Hence, there may be a possible complimentarily between competition law and non-competition public interest objectives, such as data privacy. The 'pure' privacy harms, not related to the effects on competition, are not generally viewed as a cognisable competition law issue. Except for the privacy-related harms, this question has already been dealt with by NCAs regarding whether environmental

---

[221] C-107/82 *AEG-Telefunken* v *Commission* ECLI:EU:C:1983:293, para 33; N Averitt and R Lande, 'Consumer Choice: The Practical Reason for Both Antitrust and Consumer Protection Law' (1998) 10(1) Loyola Consumer Law Review 44; Ioannis Lianos, 'Competition law in the European Union after the Treaty of Lisbon' in Diamond Ashiagbor, Nicola Countouris, Ioannis Lianos (eds), The European Union after the Treaty of Lisbon (CUP 2012). Roger Van den Bergh and Peter Camesasca, *European Competition Law and Economics: A Comparative Perspective* (2nd edn, Sweet & Maxwell 2006) 16-53.

[222] *Hoffmann-La Roche* (n 196) 91.

[223] Case C-413/14 P, *Intel v. Comm'n*, EU: C:2017:632, para 135.

[224] *AstraZeneca* (n 99).

[225] M Vestager, 'A Principles Based approach to Competition Policy' (Keynote at the Competition Law Tuesdays, 22 October 2022)

concerns might be considered to the prohibition of anticompetitive agreements per Article 101 TFEU.

One of the examples has been dealt by the Netherlands competition authority (ACM) which reviewed the 'Chicken of Tomorrow' initiative.[226] In 2013, several Dutch organisations and businesses from the poultry industry, and Dutch supermarket chains began discussion about more sustainable production of chicken meat. The aim of these conversations was to establish an industry-wide baseline that goes beyond the legally mandated conditions for producing chicken meat, eventually leading to a signed declaration of intense tot product more sustainable poultry.

ACM reviewed the reached agreement between Dutch organisations and businesses from the poultry industry, and Dutch supermarket chains, concluding that such an initiative introduced competitive restraints under Article 101(1) TFEU.[227] In the view of ACM, the initiative restricted competition on the chicken meat retail market, as 'regularly' produced poultry will no longer be available for purchase in Dutch supermarkets once the initiative takes effect, leading to a decreased variety of choices for consumers. According to ACM's opinion, it was not possible to except the initiative based on Article 101(3) TFEU as well. Hence, ACM analysed the consumers' willingness to pay. The assessment demonstrated that the "Chicken of Tomorrow" initiative could possibly be exempted from its anticompetitive conduct if the initiative resulted in a higher consumer surplus. The latter was to be determined based on the consumers' willingness to pay for the product in question, which was eventually not enough to justify the expected increase in consumer price and reduced choice.

Similarly, the BKartA dealt with the sustainability initiative — the animal welfare initiative (ITW). Within the framework of the proposed ITW initiative, the key element was the animal welfare fee rewarded to farmers for implementing animal welfare measures. The initiative

---

[226] For a detailed summary of the initiative and ACM's assessment see G Monti and J Mulder, 'Escaping the Clutches of EU Competition Law: Pathways to Assess Private Sustainability Initiatives' (2017) 42 European Law Review 635.

[227] ACM, 'ACM's Analysis of the Sustainability Arrangements Concerning the 'Chicken of Tomorrow'' (26 January 2015) <https://www.acm.nl/en/publications/publication/13761/Industry-wide-arrangements-for-the-so-called-Chicken-of-Tomorrow-restrict-competition.> accessed 20 July 2023.

was reviewed by the BKartA on its effect on competition law, based on the exchange of information between the market levels involved and the business on the relevant market.[228] In any form of competitive assessment, it is evident that substantive antitrust assessment focuses on competition problem that arises from firms' behaviour.[229] In order words, to establish abuse, it is necessary to find a deviation from competition on the merits.[230]

The idea behind this approach originates from the understanding that dominant firms are subjected to increased responsibility to ensure that their activities do not distort competition.[231] Beyond any doubts, the concept of economic efficiency holds a central position in the reasoning of Article 102 TFEU. The concept of 'dominance' is defined as 'a position of economic strength which enables an undertaking to prevent effective competition'.[232] In addition, any possible reference to public interest would include a economic efficiency standard. Any restrictions of competition might steam from abusive practices that undermine the public interest of the EU.[233] It can be deduced that the EU Courts emphasise that the specific responsibility of a dominant undertaking prevents its actions from negatively affecting fair and unbiased competition.[234] If the reason behind the special responsibility was to address anti-competitive outcomes, then all companies that hold significant market influence would be obligated to uphold this responsibility.[235] Potentially, economic freedom, consumer welfare, fairness and legal certainty have triggered the recognition of such a responsibility. In *British Airways*, AG Kokott emphasised that Article

---

[228] Bundeskartellamt, '2013/2014 Activity Report, German Bundestag – 18th legislative period, printed paper 18/5210, 53-54, <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Taetigkeitsberichte/Bundeskartellamt%20-%20T%C3%A4tigkeitsbericht%202014.pdf?__blob=publicationFile&v=2> accessed 4 August 2023.

[229] Case C-95/04 *British Airways plc v Commission* [2007] ECR 1-2331, para 86

[230] *Google Search (Shopping)* (n 192).

[231] Joined Cases C-501/06 P, C-513/06 P, C-515/06 P and C-519/06 P, *GlaxoSmithKline Services and Others v Commission and Others* ECLI:EU:C:2009:610.

[232] *United Brands* (n 195) para 65.

[233] Case C-52/09, *Konkurrenverket v TeliaSonera Sverige AB* ECLI:EU:C:2011:83, paras 21-24.

[234] Case C-322/81 *NV Nederlandsche Banden Industrie Michelin v Commission* [1983] ECR I-3461, para 57; *British Airways* (n 229) para 23.

[235] Ioannis Lianos, 'Categorical Thinking in Competition Law and the 'Effects-based' Approach in Article 82 EC' in Ariel Ezrachi (ed), *Article 82 EC – Reflections on its recent evolution* (Hart 2009) 35-37; Stavros Makris, 'Applying Normative Theories in EU Competition Law: Exploring Article 102 TFEU' (2014) UCL Journal of Law & Jurisprudence 30, 46.

102 TFEU: "is not designed only or primarily to protect the immediate interests of individual competitors or consumers, but to protect the structure of the market and thus competition as such."[236]

However, the question arises if such an assessment might consider external to competition policy. EU competition law does not exist within a regulatory vacuum and non-competition public interest concerns are considered within competition law realms to a greater or lesser extension within the broader framework that underpins the internal market. In other words, competition authorities might take into account non-competition public policy considerations in determination of whether a particular behaviour hampers competition and as a proxy to ensure fair competition and consumer welfare. Consequently, both general values on the maximisation of consumer welfare and social and political priorities, that shape enforcement, could be part of the competition law parameter, if they introduce a competitive restrains on a relevant market. For example, sustainable development has a strong legal position amongst the objectives of the EU, as the codification of the environmental integration rule can be found in Article 11 TFEU. Generally, the EU policies would be implemented by considering social protection,[237] consumer protection,[238] public health,[239] equality considerations,[240] regional development, investment[241] and environmental protection.[242] On the same note, it is generally accepted that human rights protection is guaranteed by EU competition law.[243] For example, in *Front Polisario,* it was held that the EU institutions must consider the impact of fundamental rights even where it is not evident that the rights are engaged.[244]

---

[236] *British Airways* (n 229) para 68.

[237] TFEU (n 5), article 9 refers to: 'the promotion of a high level of employment, the guarantee of adequate social protection, the fight against social exclusion, and a high level of education, training and protection of human health.'

[238] TFEU (n 5) article 12; Charter (n 46) article 38.

[239] TFEU (n 5), article 168(1); Charter (n 46) article 35.

[240] TFEU (n 5), article 8.

[241] *Ford/Volkswagen* (n 187) para 36.

[242] TFEU (n 5) article 11; Charter (n 15) article 37; see also: Julian Nowag, *Environmental Integration in Competition and Free-Movement Laws* (Oxford University Press 2016)

[243] R O'Donoghue and J Padilla, *The Law and Economics of Article 102 TFEU* (Hart Publishing 2020) 43.

[244] Case T-512/12 *Front Polisario*, ECLI:EU:T:2015:953.

In several cases, the Court emphasised that Article 102 TFEU should seek to persevere the undistorted competition in the market as to increase the social welfare.[245] In *GlaxoSmithKline*, the concepts of end consumers and their choices to limit a dominant company's competitive freedom was applied.[246] This helped connect limitations on parallel trade to negative impacts on competition. In fact, Advocate General Kokott emphasised that protection of the market structures also indirectly protects consumers as any damage to the competition flow also impacts on consumers,[247] with the EU courts establishing that competition law aims at practises both damaging consumers and the structures of effective competition.[248] The case of *TeliaSonera* recognised a significance of preserving competition from possible distortion with a negative effect on public interests, individual undertakings and consumer, thereby, ensuring the EU wellbeing.[249] The starting point in showing anticompetitive conduct is to clearly demonstrate a credible mechanism explaining the reasons for the conduct can introduce anticompetitive effects and describe what these anticompetitive effects are. Such an approach is consistent with the CJEU's and the Commission's practice.[250] From this perspective, the conduct of a dominant understanding that falls outside competition on the merits and disrupts or hinders the competitive process should not be allowed.

2.3.2. Re-thinking Article 102 TFEU for the digital economy

Article 102 TFEU stipulates that dominant undertakings' unilateral practices are deemed abusive if they constitute a restriction of competition. The courts and competition authorities approach to Article 102 TFEU can be summarised as taking two principal approaches: (1) establishing if the undertaking in question is dominant; (2) the assessment

---

[245] Case T-321/05 A*straZeneca AB and AstraZeneca plc v European Commission* [2010] ECR II-2805, para 804; *GlaxoSmithKline* (n 231) para 118; Joined Cases T-213/01 and T-214/01 *Österreichische Postsparkasse AG and Bank für Arbeit und Wirtschaft AG v Commission* [2006] ECR II-1601, para 115.

[246] *GlaxoSmithKline* (n 231).

[247] *T-Mobile Netherlands* (n 146) Opinion of AG Kokott, para 71

[248] Case 6-72 *Europemballage Corporation and Continental Can Company Inc. v Commission* [1973] ECR-215, para 26; *British Airways* (n 229) para 106.

[249] *TeliaSonera Sverige* (n 233) para 22.

[250] *Intel* (n 223).

of the conduct and its possible anticompetitive effects.[251] Under this approach, a dominant undertaking can be condemned due to its superior efficiency and market position, irrespective of the impact of its behaviour.[252] This approach could be criticised for protecting competitors rather than the competitive process. As discussed above, EU competition law has not been designed to pursue a narrowly defined economic goal. Article 102 TFEU, arguably, cannot be separated from other provisions of the EU treaties and the Charter. In *Servizio Elettrico Nazionale,* the Court emphasise that Article 102 TFEU:[253]

> "part of a set of rules, the function of which is to prevent competition from being distorted to the detriment of the public interest, individual undertakings and consumers, which ensure well-being in the European Union"

At this point, it might be already noted that the Court does not reduce Article 102 TFEU to only protecting consumer welfare, recognising its possible plurality of pursued goals, with the maintenance of the prevailing level of market competition or the promotion of its growth as the key objective.[254]

The question that remains under Article 102 TFEU is how to establish between competition on merits and abusive conduct. It remains difficult to classify what goal has been primarily adopted by the competition authorities and the courts to consider. The Commission aims to focus on these types of conduct that are most harmful to consumers, with the key concern being to achieve greater efficiency through competitive pressure. [255] Such an approach has been summarised as "from fairness to welfare".[256] In fact, the Commission has never limited itself to a narrow consumer welfare criterion,[257] which arguably indicates that any possible categorisation under Article 102 TFEU should be rejected as formalistic.[258] Institutional

---

[251] Gunnar Niels, Helen Jenkins and James Kavanagh, *Economics for Competition Lawyers* (OUP 2011) 180.

[252] See, Case T-201/04 *Microsoft Corpn v Commission* [2007] ECR II-3601, para 846.

[253] *Servizio Elettrico Nazionale* (n 143).

[254] *British Airways,* Opinion AG Kokott (n 229); *Nederlandsche Banden Industrie Michelin NV* (n 234) para 57.

[255] Václav Šmejkal, 'Abuse of Dominance and the DMA – Differing Objectives or Prevailing Continuity?' [2023] Acta Universitatis Caroliniae – Iuridica 33, 37.

[256] ibid.

[257] V Daskalova, "Consumer Welfare in EU Competition Law: What Is It (Not) About?" (2015) 11(1) The Competition Law Review 133.

[258] See, Pinar Akman, 'Searching for the Long-Lost Soul of Article 82 EC' (2009) 29 2 OJLS 267.

practice has confirmed that EU competition law in essence is not monotheistic but pursues a multitude of different goals.[259] In addition to prioritising efficiency, other objectives have also defined the boundaries of the effects-based approach and underscored the importance of thinking in terms of categories. EU competition law has been interpreted within a framework that encompasses various goals, rather than relying exclusively on a solitary objective or ideological perspective.

In 2009, the publication of Commission's Guidance on the Commission's Enforcement Priorities in Applying Article [102] EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings (Guidance) reflected on the enforcement priories of the Commission.[260] It was a manifestation of a political matter for the Commission to decide.[261] In fact, the Guidance set out the methodological approach how to deal with cases under Article 102 TFEU, identifying the approach as "more economic approach". The Guidance slowly became a useful point of reference summarising previous jurisprudence and paved the way for a more economic-based consideration. Both the Court and the Commission, in many cases, scrutinised the approach, requiring proof of anticompetitive effects of the abusive practice in question.[262] Practically, the Guidance deviated with the economic reasoning due to difficulties in accommodating the 'more economic approach'.[263] Such notion has backfired heavily with the *Intel* case, that implemented the enforcement priorities as an actual methodology.[264]

---

[259] See K Stylianou and M Iacovides, "The Goals of EU Competition Law: a Comprehensive Empirical Investigation" (2022) 42 Legal Studies 620

[260] Guidance on the Commission's Enforcement Priorities in Applying Article 82 (n 87) para 3.

[261] Or Brook and Katalin J. Cseres, 'Priority setting in EU and national competition law enforcement' (2021) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3930189> accessed 14 August 2023.

[262] *Wanadoo España v Telefónica* (COMP/38.784) Commission Decision 4 July 2007; *Intel* (n 223); Case C-280/08 P *Deutsche Telekom AG v Commission* [2010] ECR I-09555; *TeliaSonera* (n 233).

[263] R Podszun and T Rohner, 'Making Article 102 TFEU Future-Proof – Learnings from the Past' (2023) <https://ssrn.com/abstract=4428170> accessed 30 August 2023.

[264] *Intel* (n 223).

The current review of the Guidance appears necessary to adapt to the digital economic changes, which has brought new problems for competition policy.[265] A set of workable interpretative guidance would be a positive development. Yet, the 2009 Guidance and the current proposed guidelines are listed to exclusionary abuses only, leaving exploitative abuses out of the scope of the discussion. Traditionally, the Commission seldom investigated exploitative abuses due to the high burden of proof and concerns over the risk of market regulation.[266] This scenario has progressively changed over the recent years when several National Competition Authorities (NCA) sanctioned exploitative conducts in the energy and pharmaceutical sectors.[267] Finally, the BKartA decision in Facebook's case represents the first instance of exploitative conduct sanctioned in the digital economy. However, there is a peculiar: 'exclusionary' abuses refer more to practices of dominant undertakings which harm the competitors or exclude them from the market. On the other hand, exploitative abuses are seen as an attempt by a dominant undertaking to use its market position to harm consumers directly. With the general emphasis on consumer welfare, one is expected to include an assessment of exploitative abuses since they immediately harm consumers. The call to include exploitative abuses in the Guidelines has been during the review process.[268]

2.3.2.1 Exploitative vs exclusionary theory of harm

Exploitative theories of harm are the crux of this thesis, as privacy-related harms are likely to directly harm consumers. This has been proved by BKartA's case against Facebook, which

---

[265] T Rohner, 'Ideas for Sustainable Control of Abusive Practices' (D'Kart, 11.8.2022), <https://www.d- kart.de/en/blog/2022/08/11/agenda-2025-ideen-fur-eine-nachhaltige-missbrauchsaufsicht/> accessed 15 August 2023; See in general: European Commission, 'Application of Article 102 TFEU' < https://competition-policy.ec.europa.eu/antitrust/legislation/application-article-102-tfeu_en> accessed 31 August 2023.

[266] See for example, MS Gal, 'Monopoly Pricing as an Antitrust Offense in the U.S. and the EC: Two Systems of Belief about Monopoly?' (2004) 49:1–2 Antitrust Bulletin 343.

[267] R Karova and M Botta, 'Sanctioning Excessive Energy Prices as Abuse of Dominance: Are the EU Commission and the National Competition Authorities on the Same Frequency?' in PL Parcu, G Monti and M Botta (eds), *Abuse of Dominance in EU Competition Law: Emerging Trends* (Edward Elgar 2017) 169–84; M Colangelo and C Desogus, 'Antitrust Scrutiny of Excessive Prices in the Pharmaceutical Sector: A Comparative Study of the Italian and UK Experiences' (2018) 41:2 World Competition 225.

[268] See for example, Anne Witt, 'Feedback On The Proposed Guidelines On Exclusionary Abuses By Dominant Undertakings' (EU Commission, 2023) 5 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-EU-competition-law-guidelines-on-exclusionary-abuses-by-dominant-undertakings/F3406999_en> accessed 13 August 2023.

calls for a broader discussion on whether and to what extent Article 102 TFEU could be relied on to sanction exploitative abuses in the digital economy.[269]

Exploitative abuses directly harm customers, while exclusionary abuse might indirectly harm consumers. This particular interpretation of the term 'exploit' is directly applicable to the fundamental query regarding the definition of 'exploitative abuse' as outlined in Article 102 TFEU. The situation becomes complex when the actions of a company take advantage of its customers rather than fully utilising its available resources. Additionally, the specific aspects of 'exploitation' are not well-defined. This includes uncertainties about whether exploitation pertains to factors like price, quality, choice, or a combination of these elements.[270] Determining when these attributes cross the threshold of being considered as 'exploitative' remains uncertain. Addressing these inquiries necessitates evaluating a hypothetical scenario, and this alternative scenario is not straightforward either. It is not clear which alternative competitive state should be used as a basis for comparison to ascertain whether customers are being 'exploited' by a dominant undertaking. A working definition of exploitative abuse under Article 102 TFEU is seen as directly causing harm to the consumers of a dominant undertaking. The concept of direct harm to consumers is the crux of an exploitative theory of harm.[271]

Both the 2009 Guidance and the reform of Guidance Paper are limited to exclusionary abuses and excludes exploitative abuses. The 2009 Guidance introduced the effect-based approach concerning the application of Article 102 TFEU, aiming to provide a solid economic foundation to not solely rely on the nature of the dominant undertaking's conduct.[272] The effect-based approach to Article 102 TFEU has arguably combined both consequentialist and deontological thinking,[273] demanding a detailed economic analysis of the conduct in

[269] The analysis of the Facebook case is presented in Chapters 3 and 4. In Chapter 3, I discuss the crux of the case, discussing its implication on the relationship between competition law and data protection law, and its institutional impact on NCAs ability to acknowledge privacy-related harms. In Chapter 4, I use this case to explain exploitative theories of harm.

[270] Pinar Akman, 'Exploitative Abuse in Article 82EC: Back to Basics?' (2009) ESRC Centre for Competition Policy CCP Working Paper No 09-1.

[271] Akman (2009) (n 258) 8.

[272] Lianos (2019) (n 208) 35-37.

[273] ibid.

question. The CJEU has confirmed the main elements of an effect-based approach to exclusionary conduct in several judgements.[274] However, in the CJEU's approach, it seems more difficult to characterise certain types of abuses under Article 102 TFEU. When a dominant undertaking submits evidence that the investigated conduct has not resulted in an anticompetitive effect, then the Commission has to assess the effect of the conduct. To find an abuse, the Commission is required to find that the dominant undertaking's conduct has introduced "at least potential – anti-competitive effects in the relevant market".[275] This approach, attributed to the CJEU, provides useful guidance about new and old categories of abuse. Firstly, it is certain that practices are deemed harmful only when they cause anticompetitive consequences within the specific economic and legal framework that applies.[276] Secondly, For Article 102 TFEU to be relevant, there should be a clear connection between the practice and the real or potential adverse impact it has on competition.[277] In other words, there must be a cause-and-effect relationship between the practice and its impact on healthy competition. In such cases, if the detrimental consequences would have occurred regardless of the specific behaviour or can be traced to other factors, such as regulatory conditions or the undertaking's inevitable failure due to its inefficiency, then the behaviour in question would not be subject to prohibition. For example, if a dominant undertaking maintains prices above their costs and effectively excludes competitors, it might not be the result of its strategy but rather its inherent inefficiency.

Correspondingly, even if one assumes that the exclusionary abuses are the key concern as introducing the effect on competitors, the effect on the consumer should not be left excluded, especially in the digital economy. For example, in *Slovak Telekom*, the Commission assessed whether a practice representing a fair competition or introducing real or potential anticompetitive consequences become intertwined and essentially the same matter.[278] This is especially important in the review of large digital undertaking's conduct which introducing harms associated with personal data exploitation, and possible reduction of privacy. At first sight, it might seem strange to question why competition authorities should take

[274] *Intel* (n 223); Case T-235/18, *Qualcomm Inc v Commission*, 15 June 2022.

[275] Case T-612/17, Google v Commission (Google Shopping), 10 November 2021, para 459.

[276] Case T-219/99 *British Airways plc v Commission*, EU:T:2003:343; and *British Airways* (n 229).

[277] Case C-209/10 *Post Danmark A/S v Konkurrencerådet*, EU:C:2012:172

[278] Case C-165/19 P, *Slovak Telekom* [2021] ECLI:EU:C:2021:239, paras 1046-1048.

enforcement against exploitative conduct, especially since Article 102 TFEU aims to protect consumer welfare. For example, in *Intel*, the Commission applied reduced choice as a criterion of the assessment.[279] On the same note, in the *Telekomunikacja Polska* case, consumer harm was mentioned as infringing competition in a relevant market.[280] Also, in the *Google Search (Shopping)* case, the Commission investigated consumer harm through the higher prices and less innovation.[281] Although such cases considered exclusionary theories of harm, the element of consumers' exploitation demonstrated the paradox of exclusion of exploitative abuse.[282] It emphasises that the Commission and the CJEU put the priority on exclusionary abuse due to practical difficulties in intervening in exploitative conduct.

In March 2023, the Commission launched an initiative, which would result in the adoption of the new set of Guidelines on exclusionary abuses.[283] The purpose of the revision is to liberate the Commission and the CJEU from the 'more economics-based' approach which the Commission has injected its own administrate practice.[284] Especially, decisions such as *British Airways* embraced that the approach was difficult to predict, making it complicated for companies to escape the prohibition once conduct was labelled as abusive.[285] Above all, the 2008 Guidelines were criticised for not paying attention to the actual or potential effects on competition before taking action. In addition, the growing body of case law demonstrated several enforcement challenges from substantive to practical consequences. For instance, in *Intel,*[286] *and Servizio Elettrico Nazionale,*[287] the Commission

---

[279] *Intel* (n 223).

[280] *Telekomunikacja Polska* (n 131) paras 703, 706.

[281] *Google Search (Shopping)* (n 192)

[282] Mario Siragusa, 'Excessive Prices in Energy Markets: Some Unorthodox Thoughts' (2007) < https://www.eui.eu/Documents/RSCAS/Research/Competition/2007ws/200709-COMPed-Siragusa.pdf> accessed 30 July 2023.

[283] European Commission, 'Antitrust: Commission announces Guidelines on exclusionary abuses and amends Guidance on enforcement priorities' IP/23/1911 (Brussels, 27 March 2023).

[284] Pablo Ibáñez Colomo, "The (Second) Modernisation of Article 102 TFEU: Reconciling Effective Enforcement, Legal Certainty and Meaningful Judicial Review" (SSRN, 2023) 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4598161> accessed 22 October 2023.

[285] *Virgin/British Airways* (Case IV/D-2/34.780) Commission Decision of 14 July 1999.

[286] *Intel* (n 223).

[287] *Servizio Elettrico Nazionale* (n 143); Case C-680/20 *Unilever Italia Mkt. Operations Srl v Autorità Garante della Concorrenza e del Mercato*, EU:C:2023:33.

was required to consider the actual or potential consequences of anticompetitive actions, and the challenge of demonstrating these consequences, appear to pose a greater obstacle. Nevertheless, there remains a significant lack of clarity when it comes to evaluating these actions. Establishing an abuse to meet the necessary legal criteria might be a more laborious task than before, but the extent of this increased difficulty is still uncertain.

Over the years, the CJEU has adopted an interpretation of Article 102 TFEU that hinges on a meticulous and situation-dependent evaluation of the real or possible consequences of practices that could be harmful to competition.[288] Nevertheless, there are lingering uncertainties regarding the precise stringency of the effects analysis.[289] In fact, the very definition of what constitutes "effects" has never been explicitly clarified up to this point. This context provides the backdrop for understanding the Commission's actions concerning exclusionary abuses. In the call for the Guidances reform, the Commission asked for evidence to assess the learning that can be drawn from the latest case law of the Court and the Commission under Article 102 TFEU in the hope of assisting effort to align its policy with the current judicial development and enforcement experience. The submissions received by the Commission concerned primarily the economic approach and its paradigm change.[290] In fact, the Court has not rejected the consumer welfare standard and the Court has not been required to prove consumer harm when assessing abusive practice.[291] This approach has been reflected in multiple rulings where the focus is on highlighting that causing a negative impact on competition alone is enough, and there is no need for explicit proof of direct

[288] Pablo Ibáñez Colomo, 'Beyond the 'more economics-based approach': a legal perspective on Article 102 TFEU case law' [2016] CMLR 709.

[289] Pablo Ibáñez Colomo, 'Anticompetitive Effects in EU Competition Law' [2021] Journal of Competition Law & Economics 309.

[290] See for example, Witt (n 268); N Petit, 'Towards Guidelines On Article 102 Tfeu How Much Leeway Within The Case-Law?' (EU Commission, 2023) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-Prawo-konkurencji-UE-wytyczne-dotyczace-naduzyc-wykluczajacych-popełnianych-przez-przedsiebiorstwa-dominujace/F3407407_pl> accessed 28 July 2023; Google, 'Proposed Adoption By The European Commission Of Article 102 TFEU Guidelines On Exclusionary Abuses: Google Response To The European Commission's Call For Evidence' (EU Commission, 2023) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-Prawo-konkurencji-UE-wytyczne-dotyczace-naduzyc-wykluczajacych-popełnianych-przez-przedsiebiorstwa-dominujace/F3407381_pl> accessed 28 July 2023; Thibault Schrepel, 'Re: Call for evidence regarding the guidelines on exclusionary abuses by dominant undertakings' (EU Commission, 2023) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-Prawo-konkurencji-UE-wytyczne-dotyczace-naduzyc-wykluczajacych-popełnianych-przez-przedsiebiorstwa-dominujace/F3405651_pl> accessed 28 July 2023.

[291] Podszun and Rohner (n 263) 7.

harm to consumers.[292] Even if one assume that the effective competition structure is the sole goal of Article 102 TFEU,[293] exploitative harms needs to be acknowledged when considering harms introduced by large online undertakings, as they broaden the scope of understanding the potential negative impacts of privacy violations.

As the Commission focused on the exploitative theories of harm, the concept of consumer welfare was generally seen as being narrowly defined. Recently, the Court in *Servizio Elettrico Nazionale* emphasised that Article 102 TFEU aims to protect "maintenance of the degree of competition existing in the market or the growth of that competition,"[294] and Article 102 TFEU intervenes in conducts "undermining an effective structure of competition"[295] In fact, the dominant undertaking is required to engage in competition on the merits, which unquestionably includes not only end consumers but sees consumer as the ultimate objective.[296] Consumer welfare seems unavoidable as the ultimate goal, and consumer well-being seems to be a broader concept than merely economic consideration. Arguably, the notion of consumer well-being, as referred in the *Servizio Elettrico Nazionale* would include values such as price, choice, innovation, and quality.[297] The language and the statement suggested indicates that the consumer welfare objective is broader than anticipated and should include exploitative theories of harm. In fact, despite the deontological approach attracting in this context, the EU competition enforcement should be oriented on contributing to a fairer society,[298] as the objective of market integration,[299] which is a key element of the EU foundation, accounts consumer welfare too. The notion of consumer welfare could provide a workable benchmark for intervention in digital markets, allowing to address any exploitative and/or exclusionary practices with the objective to restrict competition.

---

[292] GlaxoSmithKline (n 231); Case C-202/07 P, *France Télécom v Commission* ECLI:EU:C:2009:214, para 105; *TeliaSonera* (n 233) para 24.

[293] *Servizio Elettrico Nazionale* (n 143) para 44.

[294] ibid.

[295] ibid.

[296] ibid, para 46.

[297] ibid, para 47.

[298] A Lamadrid, 'Competition law as Fairness' [2017] JIPLP 147, 147-148.

[299] Case C-468/06 *Sot. Lélos Kai Sia v. GlaxoSmithKline* [2008] ECR I-7139

On the broader assessment of the consumer welfare standard, a fusion of exploitative abuse is important in the digital economy cases, especially for cases involving a direct infringement on users' privacy. Within the digital economy, the concept of consumer welfare might be used to tackle the effect of welfare on numerous groups of consumers. It can be effective in addressing multi-sided markets, which undoubtedly characterise digital markets. The Commission acknowledged that the notion of 'consumers' covered all direct and indirect, covered by an agreement, product users, incorporating producers, retailers, wholesalers, and final consumers.[300] The term consumer welfare is fully in line with the competition law jurisprudence and should reflect on the exploitative cases that have been actively used to pursue new types of conduct, especially in the digital platform economy. While the BKartA's *Facebook case* centred on domestic regulations relating to the abuse of a dominant position, it is important to acknowledge that the idea of exploitative abuse has experienced a resurgence in Europe as of late.[301] Arguably, this might indicate that consumer welfare as the ultimate goal of Article 102 is much broader and includes a normative dimension. The term consumer welfare has attached a narrow understanding of consumer harm, which should be expanded to consider the ability of consumers, as well as all participants in the market, to make decisions independently when it comes to economic matters. This perspective aligns well with the CJEU's well-established legal principles, which emphasise the need for decision-making independence from economic entities.[302]

2.4 Conclusions

This chapter demonstrated that the relationship between competition law and privacy remains still at the early stage of judicial and practical developments. Due to an unprecedented level of personal data collection and processing activities, large digital undertakings have superior access to data, which they could use for competitive advantage. Therefore, by recognising the aggregation of personal data as a potential source of market power, competition law enforcement might provide recourse where companies use their

[300] Ariel Ezrachi, 'EU Competition Law Goals and The Digital Economy' (2018) Oxford Legal Studies Research Paper No 17/2018, 6.

[301] Marco Botta, 'Exploitative abuses: recent trends and comparative perspectives' in Pınar Akman, Or Brook, and Konstantinos Stylianou (eds) Research Handbook on Abuse of Dominance and Monopolisation (Elgar 2023)

[302] R Podszun, 'Digital ecosystems, decision-making, competition and consumers – On the value of autonomy for competition' (2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3420692> accessed 14 August 2023

market power to inflict harm that degrades privacy. Present theories have either ceased to view privacy or rejected privacy entirely as an antitrust element, treating privacy as a separate legal entity. However, both these views demonstrate the existence of a mutuality between competition law and privacy and a potential way to explain privacy as complementary with competition law. Essentially, competition law and privacy could share a multi-modal interface with both legal orders trying to mitigate unfairness via introducing and imposing obligations on those with information or market power — there is an apparent complementarity and tension. Focusing on one complementarity might result in more complex situations being left unexamined when privacy is traded at the margins of data-driven competition. Particularly, discussed theories overlook the role of privacy as a distinct legal doctrine, which pursues different competition law interests. Possible value pluralism attempts to provide a framework for balancing between competition law and data protection may assist the courts and competition authorities in reaching a context-specific and principled decision. In fact, this is not to suggest that competition law would be a panacea for every privacy concern. Instead, under value pluralism, the competition law assessment should comprise values such as economic freedom, consumer welfare, fairness, and legal certainty.

The Commission maintains its position that when assessing competition, factors such as data protection cannot be taken into account directly. It is important to realise that EU competition law is not an isolated law, but part of a larger framework of the TFEU. This means that competition authorities can tailor general principles to each particular case they deal with. This chapter emphasises that competition can be influenced by many factors beyond mere data in a particular market. Interestingly, the most complex cases for courts and competition agencies stem from a potential link between competition law and data privacy law, rather than a simple association between them. The search for the objectives outlined in Article 102 TFEU reveals that the concept of consumer welfare is broad enough to encompass theories of harm that involve exploitation. This underscores the comprehensive nature of the EU's approach to competition law.

Chapter 3: Article 102 TFEU and Privacy Violations: on the way to regulatory hybrid?

3.1. Introduction

This chapter analyses the situation in which a dominant undertaking faced legal action or enforcement measures due to its mishandling of users' data under Article 102 TFEU.[303] Although data protection principles have begun to influence competition authorities, the protection of individuals' rights as consumers and market participants is already protected by data protection and consumer protection authorities. Yet, the implementation of the large digital platforms' commercial practice depends on existing regulation, which includes competition, data protection law and consumer protection law, that forms family tie.[304] Arguably, they could exert internal and external constraints on one another.[305]

Empirically, through EU legal practice one can identify different methodological phases in the development of the intersection between competition law and data protection. Firstly, the chapter briefly discusses the institutional jurisprudence between competition authorities and data protection authorities (section 3.1). This overview serves as a foundation to later assess the protocol for competition authorities to consider privacy-related harms. Secondly, the chapter provides a historical narrative of how the approach of the Commission and the CJEU was changing towards privacy-related harms. This narrative is used to demonstrate that competition law is designated to protect consumer welfare through the protection of competition as a process: such a semantic statement demonstrates the need to recognise a broader scope of potential abuses not just those categories by economic methods of assessment. In this respect, competition law is used to discuss the event it plays a relevant role in solving the market failure. The narrative indicates that large digital undertaking's practice, resulting from exploitative data collection, might directly or indirectly harm consumers through its impact on competition.[306] However, as the discussion demonstrates, the CJEU and the Commission have lacked possible methodologies while asserting possible privacy-related harms through balancing as infringing competition

---

[303] See for example *Facebook case* (n 2); D Condorelli and J Padilla, 'Harnessing Platform Envelopment in the Digital World' [2020] Journal of Competition Law & Economics 1.

[304] Costa-Cabral and Lynskey (n 152)

[305] ibid.

[306] *Post Danmark* (n 277).

law. Primarily, the CJEU, in *Asnef-Equifax,* rejected the interplay between these areas of law, stressing that protection of data privacy law remained outside the scope of competition law (section 3.2).[307] Over the years, the interface between competition law and privacy has started to be acknowledged (section 3.3). The major step in recognising the intersection between competition law and privacy was demonstrated by Member State practice (section 3.4).[308] This section of the thesis uses BKartA's *Facebook cas*e as the quintessential example of an attempt to narrow the legal gap between competition law and data protection.[309] In the *Facebook case*, BKartA held that the requirement of giving consent to combine personal data from various sources was prohibited as an exploitative abuse by a dominant undertaking. The section also briefly discusses the decision of the Düsseldorf Appeal Court, suspending the execution of the Facebook decision in the interim legal proceeding.[310] The *Facebook case* has been referred to the CJEU for a preliminary reference by the Higher Regional Court Düsseldorf;[311] final remarks refer to the Opinion of AG Rantos and the CJEU's reasoning concerning this case (section 3.5.).[312] This chapter concludes that the approach adopted by BKartA could encourage a more adaptable interpretation of the limits of competition law.[313] This could be key to effective competition law enforcement in privacy-related cases. However, this approach should not act to expand existing competition law tools, it should only advance an understanding between competition law and privacy.

---

[307] *Asnef-Equifax* (n 89) para 177.

[308] see notably: Cremer Report (n 1); Furman Report (n 1); 'Online Platforms and Digital Advertising Market Study' (n 1) *Facebook case* (n 2); CMA, 'Algorithms: How they can Reduce Competition and Harm Consumers' (CMA, 2021) < https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers> accessed 9 May 2023. (Hereinafter: 'CMA 'Algorithms').

[309] *Facebook case* (n 2).

[310] *Case VI-Kart 1/19* (n 2).

[311] Case C-252/21, *Request for a preliminary ruling, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* 22/04/2021

[312] *Meta Platforms, Opinion of AG Rantos* (n 85).

[313] Ezrachi (2016) (n 174).

3.2. Institutional jurisprudence: overview

3.2.1. Competition authorities

The multilevel governance of competition law in the EU leads to the frequent interaction between EU competition law and national competition law:[314] the Commission serves as the central competition authority, while each Member states have their own national-level authorities in place. Regulation 1/2003 sets the framework for enforcing competition rules as enacted by Articles 101 and 102 TFEU.[315]

Article 3 of Regulation 1/2003 defines a relationship between the Commission and the NCAs competencies to the conduct falling within the scope of EU competition law, and the possible consequences of non-respect of this provision.[316] Article 3 of Regulation 1/2003 enables the EU Council to regulate the relationship between Articles 101 and 102 TFEU and national law. According to Recital 8 of Regulation 1/2003 the purpose is to ensure "the effective enforcement of the competition rules and the proper functioning of the cooperation mechanisms contained in [Regulation 1/2003]".[317] Correspondingly, the cooperation mechanism provides that the Commission and the NCAs apply Article 102 TFEU in close cooperation. Such an incentive has been expanded by the ECN+ Directive.[318] This Directive ensure that NCAs should have the authority to establish their priorities, including the discretion to determine which cases to pursue and which to close. Member States, at a minimum, must ensure that NCA personnel remain free from external influences, while still adhering to general policy guidelines.[319]

Secondly, Article 3(2) of Regulation 1/2003 concerns a "convergence rule": regarding Article 102 TFEU, Member States are allowed to enact and enforce more stricter national competition laws on their own territory, which can forbid unilateral actions that are not

---

[314] F Cenzig, *Antitrust Federalism in the EU and the US* (Routledge 2013)

[315] Regulation 1/2003 (n 54) article 3.

[316] ibid.

[317] ibid, recital 8.

[318] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (Text with EEA relevance.) PE/42/2018/REV/1

[319] ibid, article 4.

prohibited by Article 102 TFEU.[320] Essentially, if an anticompetitive practice affects market in multiple member states, the Commission will decide which authority is the most suitable to launch an investigation. If there is no singular NCA equipped to handle a situation due to the significant impact on competition primarily at the national level, simultaneous actions are initiated. A lead authority is appointed to oversee and coordinate the investigations across relevant jurisdictions. The Commission will deal with the case if more than three member states are affected, especially in the instances where the Commission should develop a competition policy particularly when a new competition issue arises.[321]

In relation to the merger proceedings, the EU Merger Regulation establishes the guidelines for the distribution of cases between the Commission and the NCAs.[322] In essence, the Commission holds an exclusive jurisdiction over mergers that possess a 'Community dimension.'[323] In such instance, NCAs are predated from enforcing their respective national merger control regulations.[324] If a merger with a 'Community dimension' could substantially impact competition in a specific market within a member state, it may be reasoned to that member state. Correspondingly, if a merger lacking a 'Community dimension' is eligible to be reviewed under the national law of at least three member states, it can be transferred to the Commission for examination.

3.2.2. Data protection authorities

The enforcement of data protection law relies mostly on national authorities,[325] with each member state having its authority in respect of enforcing GDPR.[326] The GDPR assigns supervisory authorities the duty of enforcing its provisions, including promoting public and controller awareness of their rights and responsibilities, monitoring developments that impact the protection of personal data (especially within the domains of information and

---

[320] Regulation 1/2003 (n 54), article 3(2)

[321] European Commission, 'Commission Notice on cooperation within the Network of Competition Authorities' (2004/C 101/03), para. 15.

[322] Merger Regulation (n 190).

[323] ibid, article 1.

[324] ibid, article 21(4)

[325] GDPR (n 57) articles 51(1), 58 and 83

[326] ibid, article 55.

communication technologies and commercial practices), and undertaking enforcement actions.[327]

In instances where data processing activity impacts several member states, the supervisory authority of the primary or sole establishment of the controller or processor is authored to act as the leading supervisory authority for overseeing cross-border processing activities.[328] In this respect, when it comes to global players active in the EU, the exclusive authority to initiate investigations against them lies with the lead supervisory authority, even if the conduct in question raises concerns in several member states.[329] The possible issue with this one-stop-shop mechanism is that there is a high concentration of large digital undertakings European headquarters in a particular member state, such as in Ireland.[330] In such instances, the national authorities could face difficulties in investigating every possible GDPR infringement. Yet, the Commission deems the procedural framework of GDPR as "not yet satisfactory."[331]

If the leading data protection supervisory authority neglects to investigate an apparent GDPR breach, there is a risk that the conduct may be unchecked, as other data protection authorities are precluded from initiating cases against these undertakings. This signifies a limitation in the GDPR's mechanism for assigning supervisory roles. GDPR has been particularly challenging for a country like Ireland, which has been criticised over its lax attitude towards data protection practices concerning Facebook's sharing of data with

[327] GDPR (n 57) article 57.

[328] ibid, article 56.

[329] ibid, recital 127.

[330] Irish Legal News, 'Ireland remains 'enforcement bottleneck' for GDPR' (2023) <https://www.irishlegal.com/articles/ireland-remains-enforcement-bottleneck-for-gdpr> accessed 23 November 2023; Madhumita Murgia and Javier Espinoza, 'Ireland is 'worst bottleneck' for enforcing EU data privacy law – ICCL' (*The Irish Times,* 2023) < https://www.irishtimes.com/business/technology/ireland-is-worst-bottleneck-for-enforcing-eu-data-privacy-law-iccl-1.4672480> accessed 23 November 2023.

[331] European Commission, 'Communication from the Commission to the European Parliament and the Council: 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' (2020) 3 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN> accessed 17 October 2021.

WhatsApp.[332] In this instance, a German court indicated that Facebook and WhatsApp were sharing data about German users and, subsequently, prohibited this behaviour. However, the enforcement of this ban was ineffective with the GDPR implementation, designating Ireland as the lead supervisory authority. German authorities indicated that the data sharing has recommenced, urging Ireland to take corrective action.[333]

The proposed procedural changes to GDPR demonstrate an overall dissatisfaction with the procedural application.[334] The proposed system is said to introduce a harmonised resolution of the GDPR-related claims.[335] Under the proposed system, the European Data Protection Supervisor would also gain enhanced authority to direct the parameters of investigations in cross-border data protection cases. In addition, the Commission aims to modification of the one-stop-shop mechanism to ensure that data protection authorities, not serving as the lead supervisory authority in a cross-border case, have the chance to receive a summary of crucial information about those cases at the earliest possible stage. At the time of writing this thesis, the Commission has been working on the procedural adjustment of GDPR.[336]

3.2.3. Competition authorities' role in investigating privacy-related harms: the act of balancing

One needs to balance what is the desirable role of competition authorities when investigating privacy-related harms.[337] According to the case law, the EU Commission enjoys broad discretion to select cases, that deal with Article 102 TFEU.[338] Under Recital 9 of Regulation 1/2003, NCAs could apply national rules that regardless of whether specific

---

[332] See Nicholas Vinocur, 'Millions of Americans rely on Europe's tough new privacy rules to safeguard their data, but the law's chief enforcer – Ireland – is in bed with the companies it regulates' (*Politico*, 24 April 2019) <https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/> 23 November 2023.

[333] ibid (271).

[334] Proposal for laying down additional procedural rules relating to the enforcement GDPR (n 82).

[335] European Commission, 'Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases' (2023) < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609> accessed 23 November 2023.

[336] ibid.

[337] There is no discussion on how to distinguish between national competition law and other laws within the meaning of Articles 3(2) and (3) Regulation 1/2003 (n 54). Or Brook and Magali Eben, 'Article 3 of Regulation 1/2003: A Historical and Empirical Account of an Unworkable Compromise' (SSRN, 2022) <https://ssrn.com/abstract=4237413 or http://dx.doi.org/10.2139/ssrn.4237413> accessed 29 October 2023.

[338] See a discussion in section 2.2.2 in Chapter 2, where I discussed the theory of value pluralism.

actions are known to or believed to impact market competition should fall under the domain of competition law.[339] The fundamental reasoning is that when a competition authority exercises its power, it has to evaluate whether the conduct in question involves the use of methods that deviate from competition on the merits. In this process, a competition authority has to consider the legal and economic environment in which harm occurs. Therefore, determining whether the behaviour conforms or deviates from the GDPR provisions, not in isolation but by taking into account all the relevant circumstances, can serve as a crucial indicator of whether the conduct employs methods that run counter to the principles of fair competition. It is prudent to consider including not only the other facets of competition law but also areas that could potentially become part of the system following the introduction of the ECN+ or areas that stand to benefit from similar considerations.[340] This is particularly true about tackling the data-related harms within the remits of competition law.

The interplay between competition law and data protection law can be possibly guided by two distinct dynamics. Firstly, the CJEU and/or the Commission can incorporate the concepts of one area of law when interpreting the rules of the area it is authorised to enforce.[341] It can involve adopting the rules and values of a different area of law in the process of competition law enforcement.[342] Secondly, the CJEU and/or the Commission could indicate an enforcement action by relying on the existence of various bases for each of the areas of law for each of these cases.[343] Here, an investigation that conduct can simultaneously involve unfair processing, anticompetitive behaviour, or unfair conduct, all within the

---

[339] For example, in *VAG*, the CJEU assumed that German law on unfair competition was not considered as part of national competition law, it was not included in the statutes related to competition law. On the same note, using the objective of national statues as a benchmark informing Article 3 of Regulation 1/2003 (n 54) as an analysis introduces an advantage offering predictability, which could result in a higher degree of harmonisation of NCAs approaches. C-41/96 - *VAG-Händlerbeirat eV v SYD-Consult* 1997 I-03123, para 12-14.

[340] Costa-Cabral and Lynskey (n 152); see also N Heilberger, F Zuiderveen, Borgesius and A Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) CMLRev 1427.

[341] I discussed this concept in Chapter 2, see particularly the discussion in section 2.2.2.

[342] *Meta Platforms, Opinion of AG Rantos* (n 85).

[343] *Servizio Elettrico Nazionale* (n 143); GDF Suez Décision n° 14-MC-02 du 9.9.2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité) (2014) <https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9-september-2014-gas-market> accessed 23 November 2023.

boundaries of its competence or the primary legal basis of the action. In such cases, there is not a true "interaction" among the three areas of law, as their enforcement proceeds along separate and parallel paths. Crucially, merely not complying with GDPR does not, by itself, determine the legality of a practice under Articles 102 TFEU. A situation where data processing adheres to GDPR may still violate competition regulations, while a failure to comply with GDPR does not guarantee a violation of competition rules. The next sections focus on such intersection, guiding possible competition law interference into privacy-related conducts.

3.3. Competition law and privacy: two separate regimes

The first case at the EU-level focusing on the intersection between competition law and privacy is *Asnef-Equifax.*[344] In 2006, the CJEU delivered a preliminary ruling on the potential anticompetitive effect of a Spanish database operated by financial institutions and considered a possible exemption under Article 101(3) TFEU. The CJEU opined that the database did not restrict competition, as it improved the credit supply functioning. Furthermore, the Court viewed the database as not restricting competition if: (i) the register did not reveal the lenders' identity; (ii) the relevant market was not highly concentrated; and (iii) the data basis was accessible on a non-discriminatory basis to different financial institution in that market. Essentially, if the case considered the anticompetitive effect of the gathered database, the CJEU observed that consumers would receive a fair share of the benefits of the restrictive agreement. In *Asnef-Equifax*, the CJEU rejected the interplay between competition law and data protection rules by stressing that data protection law was outside the scope of competition law.[345] The ECJ found 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.”[346] In other words, the Court stressed that privacy concerns had no recognisable connection with competition law.

[344] *Asnef-Equifax* (n 89) para 177.

[345] Ibid.

[346] ibid, para 56.

With developments of the digital economy, subsequent enforcement abandoned isolation of data protection principles in anticompetitive assessments.[347] In 2007, the Commission cleared the Google and DoubleClick merger.[348] Google obtained the most popular free search engine, which attracted a high number of daily users. DoubleClick was a US entity, selling ad serving and reporting technology to website publishers, advertisers, and advertising agencies. In this proceeding, the Commission was concerned with the potential foreclosure effect on the online advertising market. Nonetheless, the merger was approved, as the switching costs for providers of the online advertising platforms were not cost-prohibitive to consumers. In relation to the privacy of the users, the Commission, adopting the *Asnef-Equifax* ratio, concluded the case:

> "[W]ithout prejudice to the obligations imposed onto the parties by Community legislation concerning the protection of individuals and the protection of privacy about the processing of personal data."[349]

Again, the Commission had not addressed the relationship between competition law and privacy.[350] The Commission considered the case by applying well-established competition law principles and cleared the merger. The Commission was conscious that the acquisition of users' data might result in targeted advertising and restrictions of privacy rules. The potential anticompetitive conduct concerned exploitative and exclusionary abuse, diminishing consumer experience and lessening competition in a relevant market. Essentially, both *Asnef-Equifax,* and *Google/DoubleClick* mergers represent competition law reaching out to assess non-competition concerns through the lens of competition law enforcement.[351] These cases are almost laying the groundwork for a similar interchange

---

[347] *TomTom/Tele Atlas*, Case No COMP/M.4854, Decision of 14.5.2008; The vertical merger of *TeleAtlas/ TomTom* did not raise any data issues and kept a prudent approach in excluding data protection arguments in its assessment. Once again, the Commission did not provide any guidance on the relationship between competition law and data protection.

[348] *Google/DoubleClick* (n 202).

[349] ibid, para 368.

[350] For a similar point see the FTC decision, FTC, 'Statement of FTC Concerning Google/DoubleClick' FTC File No. 071-0170, 2–3 (Dec. 20, 2007) <https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf> accessed 20 October 2021. The merger between Google and Doubleclick was cleared. Pamela Jones Harbour, the FTC Commissioner, remained the only objector of the merger, as the relationship between competition law and data privacy was not adequately expressed.

[351] See also Apple/Shazam merger where the Commission also reiterated that the GDPR matters are: ""[w]ithout prejudice to the assessment of the matter by the competent data protection authorities […]". Case M.8788, *Apple/Shazam* 6 February 2018*.,* para. 231

between data protection law and competition law. Both cases emphasise an important parameter — privacy protection was viewed as not falling within the scope of competition law, but within the scope of EU data protection rules.

3.3.1. Google/Fitbit merger: no direct link between infringement of privacy and competition

The Commission continued to treat privacy-related harms as outside the scope of the EU competition law as consistent with the *Asnef-Equifax* decision. Recently, the Commission investigated the *Google/Fitbit* merger case, which involved the acquisition of Fitbit by Google.[352] Both businesses were based on the monetisation of personal data. Before the merger, Google had already access to collect and analyse large amounts of personal data, with unique data-generating assets in most areas of users' lives. The Commission approved the merger. Yet, the decision has been subjected to criticism, due to dire consequences for competition and privacy.[353]

The Commission recognised that the combination of Google and Fitbit's data could introduce possible competitive restraints.[354] Yet, in the view of the Commission, Google and Fitbit were not active in the same market, making the theory of harm seen as horizontal — the harm arose from the combination of Google and Fitbit's data input. Fitbit collects a vast amount of health-related personal data,[355] as well as users' email addresses, gender, birthdate, height and weight, which users are required to add to ensure their device works properly. Fitbit did not use the collected data for advertising purposes, and Google has promised not to do that too. Yet, Google did not convince the Commission, which predicted that Google would combine its data with Fitbit's data, giving Google a greater ability to

[352] *Google/Fitbit* (n 155).

[353] Tommaso Valletti and Cristina Caffarra, 'Google/Fitbit review: Privacy IS a competition issue' (Cepr 2020) < https://cepr.org/voxeu/blogs-and-reviews/googlefitbit-review-privacy-competition-issue> accessed 1 August 2023.

[354] *Google/Fitbit* (n 155) para 399.

[355] ibid, para 415

engage in targeted advertising.[356] Correspondingly, that would strengthen Google's position in online advertising, which model is based on the use or exploitation of personal data.[357]

The merger has a key implication on the data, as both Google and Fitbit directly offer consumer-facing digital products and services. Arguably, the *Google/Fitbit* merger makes it difficult for consumers to negotiate, leaving them in a "take it or leave it" position. Google and Fitbit indicated that Fitbit has not sold personal data and its health data would not be used for Google targeted advertising. Yet, it needs to be noted that only Google ads are mentioned in the Google's remedy statement, not any other Google services which might captivate the data. There is no clear definition available as to what constitutes Fitbit's health data, making it difficult to assume what kind of data might be used by Google. The wording of Google's remedies suggest that only Fitbit's health data would not be exploited by Google, making it possible for Google to use non-health data for their analytical purposes. The Commission was more concerned that the merged entity could restrict access to Fitbit's application programming interface, harming competition in various digital healthcare market.[358] Eventually, this theory of harm was also rejected, as the Commission considered Fitbit's data as clearly not the centre of Google's rationale for this acquisition, indicating that such data is easily replicable with many competitors being active in the digital healthcare sector.[359]

Importantly, the Commission had not raised any concern about users' privacy, rejecting any possible privacy-related arguments.[360] The Commission based its stance on the consideration that the combination of Google's and Fitbit's data would not directly harm the users. Instead, the harm would occur on the side of advertisers, who would have to pay higher prices. The decision indicted that Fitbit's users would not be harmed by any deviation in offered privacy level. The decision came as a surprise, as this merger is occurring amid growing concerns about declining privacy standards, as the competition among data

[356] “Google has more data, of more types, from more sources than anyone else” 'Online Platforms and Digital Advertising' (n 1) para 50.

[357] See Case AT.40099 – *Google Android,* Commission decision of July 18, 2018, para 674, where Google was found to be a dominant undertaking in general search service in the EEA.

[358] *Google/Fitbit* (n 155) para 475.

[359] ibid, para 488.

[360] ibid, para 452.

collectors has decreased, and user attention is increasingly concentrated in a small number of dominant "attention brokers." At the time of the merger, privacy has been recognised as "very much a competition concern".[361] This argument would be considered in the next section (section 3.4.), here I offer considerations of the missed opportunity for the Commission to recognise degradation of privacy as influencing possible deviation of competition.

The Commission's orthodox approach to privacy in this merger control has come in for criticism. For example, Valletti and Caffarra emphasised that any possible degradation of consumer data might result in a dominant position of a large dominant undertaking and might lead to the detriment of consumer welfare.[362] In their opinion, Google's collecting practices should not be disregarded because of the amount of data collected, but of the multimodality of collected data post-Fitbit merger. Perhaps, the Commission's assessment of possible exploitation and discrimination of users was less directly addressed after Google announced no plans to integrate Fitbit's data into Google's digital healthcare initiatives.[363] It is also unclear why the Commission has not followed a similar approach as adopted in the merger of *Facebook/WhatsApp* where privacy was recognised as a parameter of quality. Instead, the Commission indicated that users still have several various choices other than Fitbit, such as Huawei, Apple, and Xiaomi.[364]

The Commission bypassed the debate on users' privacy due to a lack of tools or methodology to merge privacy and competition law, as it has been insisted that anticompetitive conducts should be classified into "a known category of abuse,"[365] establishing a direct link between conduct and its likely effect by analysing a counterfactual scenario to assess the state of competition if the conduct has not existed. The decision taken by the Commission in the merger dovetail the one taken in *Facebook/WhatsApp*, where the Commission indicated that: “any privacy-related concerns flowing from the increased

[361] Furman report (n 1); Cremer report (n 1).

[362] Valletti and Caffarra (n 353).

[363] *Google/Fitbit* (n 155) para 490.

[364] Simon Vande Walle, 'The European Commission’s Approval of Google/ Fitbit – A Case Note and Comment' (2021). Concurrences Competition Law Review Nr. 3-2021

[365] see, *Google Search (Shopping)* (n 192); *Slovak Telecom* (n 278).

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 EU data protection rules"[366] As the *Facebook/WhatsApp* merger was conducted in 2016, the optic and priorities and perception of Big Tech were very different. Google's strategy has been driven by collecting and processing more data about various aspects of users' lives. Arguably, Google's crucial objective could be to maximise the value of data, which would include linking multiple pieces of information about its users.[367] Google is capable of exploiting users' data as the power comes from ability to obtain and analyse collected from, and linking together, incredibly large datasets. Potentially, the *Google/Fitbit* merger created the opportunity to combine unique sets of personal data with other sets of personal data about the same user, generating more robust signals that can be explored from various dimensions, and possible exploitation of users. Although I agree with this presumption, privacy protection has been recognised as a quality element of an offered product or service. Some online users value the privacy protection offered by digital platforms. Privacy protection can only impact competition law when privacy is a key parameter of competition and is not the case for consumer communication apps where price, user base, popularity or reliability are important factors. I argue that it is important to not lose sight of the fundamental principle that what is relevant in a competition assessment involving privacy concerns are market-driven privacy standards.

3.4. Privacy as 'not the main' but one of the 'important' parameters in competition

Despite the analytical challenges in measuring privacy, competition law analysis has suggested some early effects in measuring privacy, which might serve as recognising privacy as a component of a competition law assessment. The Commission faced the question of whether existing competition law rules were fit for the challenges created by the technology revolution.[368]

---

[366] *Facebook/WhatsApp* (n 90) para 164.

[367] *Google/Fitbit* (n 155).

[368] See *Telefónica UK/Vodafone UK/Everything Everywhere/JV,* No COMP/M.6314, 4 September 2012; In *Telefonica UK/ Vodafone UK/Everything Everywhere*, a decision on joint venture creation, the Commission mentioned that personal data acted as a commodity, as consumers tended to surrender their data to market players.

In 2014, the Commission conducted a review of the merger of Facebook and WhatsApp.[369] The Commission reviewed the possible loss of competition in the social media market,[370] the communication app market[371] and the online adverting market.[372] The merger was approved by the Commission without conditions.[373] The Commission considered if the merger could create a concentration of commercially valuable data[374] and reviewed the potential privacy concerns, despite the Commission general approach that privacy concerns should be reviewed by the data protection authorities, as consistent with the *Asnef-Equifax* decision.[375] The review found that:

> "Regardless of whether the merged entity will start using WhatsApp user data to improve targeted advertising on Facebook's social network, there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control."[376]

The Commission extensively considered the role of privacy as an element of the competition law review. In its consideration, the Commission recognised that: "contrary to WhatsApp, Facebook Messenger enables Facebook to collect data regarding its users that it uses for … its advertising activities."[377] Essentially, the WhatsApp strategy remained to maintain its business with little knowledge about its users.[378] Importantly, during the merger review, the Commission noted the increased importance of a privacy parameter, especially as an element of a service offered by consumer communication apps.[379]

---

[369] *Facebook/WhatsApp* (n 58).

[370] ibid, para 143-63.

[371] ibid, para 84-142.

[372] ibid, para 164-190.

[373] ibid, para 191.

[374] ibid, para 164.

[375] ibid.

[376] ibid, para 189.

[377] ibid, para 102.

[378] ibid, para 169: "WhatsApp does not allow ads because it believes that they would disturb the experience that it wants to deliver to its users."

[379] ibid, para 87.

Although the importance of personal data privacy varies amongst the digital users,[380] the Commission made cross-references to two other messaging services, Threema and Telegram. The services were more protective of privacy than Facebook Messenger.[381] The review further proved that privacy concerns made several German users switch from WhatsApp to Threema, following the announcement of the merger.[382]

Once again, the Commission's approach to privacy impact appears to be incomplete. A considerable part of the merger review focused on different privacy practices in the market. Still, the Commission remained silent on the importance of these practices in relation to competition between the merging platforms.[383] Even if such differences were the differentiating factor amongst the merging entities, the Commission concluded that privacy was not the driving competition factor, nor the basis for consumer choice. In general, the reasoning of the Commission emphasised that the main drivers of competitive interactions were: (1) the underlying network; and (2) the functionalities offered by the platforms.[384] Hence, competition between these entitles consisted of the communication functionalities and the network size.[385]

The Commission concluded that privacy was not the *main* driver of competition in the consumer communication market.[386] Moreover, the Commission concluded that the merger did not impede competition in that market.[387] The proposed transaction increased the merged company's market share to 40%, with the remaining spread among smaller providers.[388] Essentially, the Commission found a substantial overlap between Facebook and WhatsApp's user bases. Facebook Messenger and WhatsApp were seen rather as offering

---

[380] Pasquale (n 163) 1012.

[381] *Facebook/WhatsApp* (n 58) paras 90, 129.

[382] ibid, para 174.

[383] ibid, para 87.

[384] ibid, para 86.

[385] See, Ariel Ezrachi and Maurice Stucke, *Virtual Competition* (Harvard University Press 2016); Stucke and Grunes (n 8), for a discussion on the network size.

[386] *Facebook/WhatsApp* (n 90) para 86.

[387] ibid, para 142.

[388] ibid, para 96.

complementary services than operating as competitors.[389] Furthermore, there were several alternative providers after the mergers,[390] in addition to there being barriers to entry.[391] Network effects would not seriously hinder competition, even if Facebook merged Messenger with WhatsApp.[392] In this respect, the merger was seen as not diminishing existing competition.

The Commission's approach in the *Facebook/WhatsApp* merger did not elaborate extensively on the relationship between competition law and privacy. The Commission concluded that the merger introduced no changes for users in that respect.[393] Later Facebook announced that WhatsApp would join Instagram, Messenger, and Facebook as an app that advertisers accessed to reach their intended audience.[394] Hence, WhatsApp's pro-privacy practices were replaced with the less protective, but legal, data collection practices typical for the Facebook product family. At the time, privacy protection was not a crucial, competitive element. This consensus seems reasonable even today. Functionality and the user base remained the key elements of competition.

However, the subsequent merger of *Microsoft/LinkedIn* offered a more nuanced approach to data privacy within EU competition law.[395] The Commission, at first, determined that the merger posed a risk of competitive harm on the professional social networks, as the data acquired in the merger has a long durability and could constitute a barrier to entry into the social network market. Yet, the merger was cleared after Microsoft's proposal on LinkedIn's integration with different Microsoft's products.[396] The Commission relied on the user privacy

---

[389] *Facebook/WhatsApp* (n 90) para 101-107.

[390] ibid, para 109.

[391] ibid, para 117.

[392] ibid, para 135.

[393] WhatsApp, 'WhatsApp Blog' (2014) <https://blog.whatsapp.com/499/Facebook?> accessed 14 June 2020

[394] Mike Isaac, 'Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger' *(The New York Times,* 25 January 2019) < https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html> accessed 23 October 2022.

[395] *Microsoft/LinkedIn* (n 90).

[396] ibid, para 470.

protection to assume the impact of combining the two companies' databases.[397] The Commission concluded that:

> "The combinational of their respective datasets does not appear to result in raising the barriers to entry/expansion for other players in this space, as there will continue to be a large amount of internet user data that are valuable for advertising purposes .. not within Microsoft's exclusive control."[398]

It was concluded that the merger would not negatively influence the competition for personal data. During the review of the competition for personal data, the Commission devoted its attention to considering the intersection between competition law and privacy. The approach was different, and more nuanced to that adopted in *Facebook/WhatsApp* merger:

> "Privacy related concerns as such do not fall within the scope of EU Competition law but can be taken into account in the competition assessment to the event that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor. In this instance, the Commission concluded that data privacy was an important parameter of competition between professional social network on the market which could have been negatively affected by the transition."[399]

In order words, the Commission still emphasised the *Asnef/Equitax* ratio and demonstrated that competition law and privacy protection were not mutually inclusive. However, the Commission, for the first time, considered the role of personal data privacy as an element of quality, guiding the preference of online users in choosing social network services. The Commission continued:

> "Privacy is an *important* parameter of competition and driver of customer choice in the market for (professional social network) services."[400]

The privacy parameter was mentioned as a potential competition problem with the merger.[401] The Commission was concerned that Microsoft could adopt certain integration and pre-instalment practices to foreclose competition in the market for professional social

---

[397] *Microsoft/LinkedIn* (n 90).

[398] ibid, para 180.

[399] 'Mergers: Commission approves acquisition of LinkedIn by Microsoft' (n 211).

[400] *Microsoft/LinkedIn* (n 90) para 330.

[401] ibid, para 350.

networks.[402] It would prevent consumers from choosing the professional social network with the best privacy protection. In this respect, the Commission claimed that the foreclosure effects would result in the marginalisation of existing competition. The transaction could have restricted the choice of consumers about the privacy parameter when choosing a professional social network.[403] However, the merger was cleared based on accepted commitments from Microsoft, restricting their connection and integration with LinkedIn.

In the assessment, the Commission offered an analysis of the professional social network services market, distinguishing it from personal social networks and specialised professional social networks. The essential functionality of a competing professional social network is to create CVs, and search for jobs. The Commission did not disclose its privacy parameters as one of the essential functionalities. It remains unclear how to account for privacy as 'an important parameter' in the professional social network market competition. This lack of details raises several questions. If privacy counted as a major factor, the Commission did not list a privacy policy as one of the essential functionalities of any professional social network. The main consideration of the Commission fluctuated around the perception that privacy was not seen as a major element of competition for consumers.[404]

It remains difficult to interpret the Commission's approach to privacy competition in *Microsoft/LinkedIn*. The findings in *Microsoft/LinkedIn* dovetail with those from the *Facebook/WhatsApp* merger decision. In both instances, the Commission's merger analysis focused on the data-related competition. In order words, the Commission assessed if the proposed merger between Facebook and WhatsApp, and Microsoft and LinkedIn could introduce exploitative or exclusionary effects for market participants. Even though the analysis focused on exclusionary and exploitative data-related harms, privacy was considered as a potential parameter of quality, guiding the preferences of online users in choosing the service or product offered in question. For example, the WhatsApp decision emphasised that Facebook Messenger and WhatsApp were seen as close competitors. Their communication functionalities determined that privacy was not seen as the *main* driver of

[402] *Microsoft/LinkedIn* (n 90)

[403] ibid.

[404] 'Mergers: Commission approves acquisition of LinkedIn by Microsoft' (n 211).

competition.[405] To compare this decision with the *Microsoft/LinkedIn*, the Commission, in the *Facebook/WhatsApp* merger decision, found that privacy was an *important* factor of competition. So, accordingly, the Commission went to extraordinary lengths to make their disparate conclusions consistent in both *Facebook/WhatsApp* and *Microsoft/LinkedIn* merger review decisions. It is unclear why the Commission focused on privacy as a parameter of quality, which guides users in choosing digital services or products. It is reasonable to conclude from the Commission's practice in *Facebook/WhatsApp* and *Microsoft/LinkedIn* merger review decisions that privacy might be seen as an important driver of competition. Hence, one does not need to impose a consistency between these two proceedings. In any case, the privacy parameter was not a determinant of the Commission's conclusion in these mergers. The Commission's remedy did not address the loss of privacy competition, revealing no optimal method of evaluating privacy as a competitive parameter.

3.4.1. Facebook/Giphy merger: privacy-related harms as a demonstrable phenomenon

In both merger cases, discussed above, the Commission asserted that data protection law did not apply to competition law analysis. However, the Commission's avoidance should not be viewed as its indifference. The Commission bypassed this debate due to a lack of tools or methodology to merge privacy and competition law. In neither case did the Commission clearly assert whether competition law was suitable to consider privacy-related harms as a part of the competition law paradigm. Instead, the Commission based its investigation of the specific market contexts involved in both *Facebook/WhatsApp* and *Microsoft/LinkedIn* merger review decisions. The *Facebook/WhatsApp* merger case analysis provided more detail in respect to key market participants. In contrast, the *Microsoft/LinkedIn* merger decision provided a less detailed reference to underlying market participants, as compared with F*acebook/WhatsApp* merger decision, and offered no assessment of factors driving competition. The same approach has been shared in the *Google/Fitbit* merger case, which did not provide any analysis of the privacy-related theories of harm. Instead, the Commission maintained its separatist approach and has not established a direct link between possible data privacy breaches as a competition concern.

[405] *Facebook/WhatsApp* (n 90) para 103.

Privacy concerns are a demonstrable phenomenon that can be observed and potentially quantified. The problem lies in objectively assessing which factor plays a crucial role in the decisions of consumers.[406] Yet, these merger reviews were conducted in 2014 and 2016, when data-driven competition was on the increase. In addition, the merger reviews focused on mostly on exclusionary theories of harm, rather than on possible exploitation of digital users. With the development of the digital economy and a high reliance on the zero-priced and data-fuelled digital services and platforms, consideration of privacy-related harms could be more nuanced. Arguably, this approach has been recently shared in the CMA's *Facebook/ Giphy* merger case.[407]

In *Facebook/Giphy* merger case, the CMA blocked the acquisition of Giphy by Facebook.[408] The CMA deemed the commitments offered by Facebook as not acceptable in connection with the risks posed by the merger within the UK advertising market. As opposed to Facebook's market dominance in the social media and messaging services market, Giphy is a leading provider of GIFs through search engines. Both Giphy and Facebook operate at different levels of the supply chain, with Giphy being an input for social media platforms. The CMA found possible lessening of competition on two bases: (1) vertical effects on competition in the supply of social media; (2) horizontal effects resulting from the loss of potential competition in the advertising market.[409] Hence, the considered theories of harm in this proceeding were not new, as the CMA indicated that the merger might result in a loss of competition and innovation based on the dynamic characteristic of digital markets. Facebook could have potentially changed the terms of access, requiring users and other platforms provides to share more data to access and use Giphy GIFs. Notably, the CMA indirectly considered exploitative theories of harm concerning data mishandling and user

[406] *Google/Fitbit* (n 155) emphasised that consumer choice is crucial.

[407] CMA, 'Completed acquisition by Facebook, Inc (now Meta Platforms, Inc) of Giphy, Inc. Final report on the case remitted to the CMA by the Competition Appeal Tribunal' (2022) < https://assets.publishing.service.gov.uk/media/635017428fa8f53463dcb9f2/Final_Report_Meta.GIPHY.pdf> accessed 1 July 2023.

[408] CMA, 'Completed acquisition by Facebook, Inc (now Meta Platforms, Inc) of Giphy, Inc.Summary of Remittal Final Report' (2021) < https://assets.publishing.service.gov.uk/media/634e6ce58fa8f53465d13a35/Facebook_GIPHY_-_Remittal_Summary_.pdf> accessed 1 July 2023. (hereinafter: 'Completed acquisition by Facebook: Final Report')

[409] ibid, para 14.

privacy abuses.[410] Arguably, consumer privacy measures were considered as a response to digital monopolies offering free services, funded by the utilisation and sale of personal data to advertisers and businesses. In fact, consumer data-driven algorithm discrimination could exploit consumers' ignorance for advertisements. As a result of personalisation, predictive consumer data analytics and behavioural insights have experienced remarkable advancements.[411]

Examining the personal data combinations, the CMA placed a significant value on the possibility to sell users' data for higher prices, especially for targeted advertisement.[412] Similarly, in the *Facebook/Kustomer* case, the CMA noted that advertisers are particularly interested in consumer-specific characteristics such as location, language, and culture.[413] The CMA noted that the possible risk of negative publicity resulting from the muses of consumer data and privacy harms represented a good metric of quality reduction in the absence of significant customer transition away from the leading platform Although users appear immune to potential privacy degradation, this is caused by their misunderstanding about how privacy loss could lead to potentially higher prices. Since the CMA predicted that the merger could lead to a substantial lessening of competition, the CMA ordered Facebook to sell Giphy. Any possible algorithmic discrimination resulting from an increased data acquisition of merging databases has risen considerations whether privacy and data protection infringement might result in distortion of competition.

3.5. The Facebook case saga: on the way to regulatory hybrid?

The German Facebook case remains an example of a competition authority diminishing the boundaries between competition law and data protection law. Germany has been the most active in integrating privacy into competition law. Its unique perspective has provided the most innovative approach to acknowledging privacy concerns into exploitative competition law. The exploitative theory of abuse concentrates on the extraction of excessive rents from

---

[410] 'Completed acquisition by Facebook: Final Report' (n 408) para 5.118.

[411] Filippo Lancieri and Patricia Morita Sakowski, 'Competition in Digital Markets: A Review of Expert Reports' (2021) 26 Stanford J of Law, Bus & Finance 84

[412] 'Completed acquisition by Facebook: Final Report' (n 408) para 5.118.

[413] CMA, 'Anticipated acquisition by Facebook, Inc. of Kustomer, Inc. Decision on relevant merger situation and substantial lessening of competition' (2021) ME/6920/20 < https://assets.publishing.service.gov.uk/media/618a6328d3bf7f56059042d5/Facebook.Kustomer_-_Phase_1_Decision_.pdf> accessed 10 November 2023

businesses or consumers. In other words, they have related to fairness rather than efficiency-based competition law violations. This section discusses the potential extension of the existing competition law rules to establish a hybrid between competition law and data protection.

It is important to note that the BKartA found Facebook's abuse of market position under §19 GWB.[414] Such an approach has been criticised by several authors, as the BKartA focused on national law provision, rather than EU competition law.[415] NCAs do not possess the authority to determine the legal foundation for an antitrust inquiry. Under Article 3(1) of Regulation 1/2003, NCAs are obliged to apply Articles 101 and 102 TFEU when the anticompetitive conduct introduces constraints on the 'intra-community trade'. Arguably, this provision is applicable in this case,[416] due to the cross-border nature of Facebook operation. Under Article 3(2) of Regulation 1/2003, NCAs could apply their own national competition law rules if they are stricter. Yet, this is not the case for §19 GWB, as the wording of this provision is almost identical to Article 102 TFEU. The BKartA possibly opted for national competition law as its legal foundation to avoid setting a precedent at the EU level and to leverage the established German case law instead of that of the CJEU.[417] However, these reasons may not sufficiently justify the selection of the legal basis. The CJEU has already addressed unfair trading practices enforced by dominant firms on their customers in its jurisprudence on Article 102(a) TFEU.[418]

3.5.1. BKartA's Facebook case

The BKartA thoroughly examined Facebook's terms and conditions during the investigation and concluded that some of the terms were unfair to its users. The BKartA found that

[414] Bundeskartellamt, 'Amendment of the German Act against Restraints of Competition' (2021) < https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB Novelle.html?nn=3591568> 14 August 2023.

[415] See notably, 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 Antitrust Bulletin 426

[416] Marco Botta, Alexandr Svetlicinii and Maciej Bernatt, 'The Assessment of the Effect on Trade by the National Competition Authorities of the "New" Member States: Another Legal Partition of the Internal Market?' [2015] Common Mkt L Rev 1247.

[417] Botta and Wiedemann (n 415).

[418] In Chapter 4, I offer a discussion on the privacy-related exploitative theories of harm. In section 4.2.2, I cover unfair trading conditions and practices.

Facebook's actions were a clear manifestation of market dominance, as per the §19(1) GWB,[419] the national equivalent to Article 102 TFEU.[420] The BKartA's assessment showed Facebook's strong market position and the likelihood that users would remain loyal to the platform, resulting in a lock-in effect. Due to Facebook's position, the platform was able to collect and analyse data from its family of products,[421] and data collected from any apps or websites that make use of "Facebook Business Tools." This was evidenced by the low level of competition in this market and the lack of viable social networks.[422] Additionally, Facebook's dominant position was influenced by the user behaviour factors. Users of this platform were reluctant to switch to other providers if their friends and family were also not using them. Based on the broad assessment, the BKartA concluded that Facebook was dominant due to its network effect and the absence of any competitors in the national market for social networks.[423]

The BKartA was concerned with two antitrust issues: 1) the accumulation of the data allowed Facebook to entrench the dominant position; and 2) the single catch-all consent of Facebook users to be unfair under Art 102(a) TFEU. Such an approach might be viewed as dividing the theories of harm into two spectrums: exploitative and exclusionary theories of harm. Although the BKartA based its decision relying on German law, I consider the wider EU competition law implications.

Considering the exploitative theories of harm, the BKartA assessed that:

> "[I]mplementing Facebook's data policy, which allows Facebook to collect user and device-related data from sources outside of Facebook and to merge it with data collected on Facebook, constitutes an abuse of a dominant position [...] in the form of exploitative business terms."[424]

---

[419] GWB (n 414).

[420] *Facebook case* (n 2) 5.

[421] They include WhatsApp, Instagram, Oculus and Masquerade.

[422] Due to Google+ being shut down, there has not been an alternative social platform available that permits a valid comparison with Facebook.

[423] *Facebook case* (n 2) 5.

[424] ibid, 7.

According to the BKartA, the collection of users- and device-related data, the data combination practice and the subsequent use of the information collection was a processing of personal data as per Article 4 GDPR. Also, Facebook collected data outside the social network thought the use of Facebook Business Tools and cookies, which were correspondingly linked to the personal data of users already registered. The data processing component was contractually imposed by Facebook. The exploitative abuse in question amounted to Facebook manifesting its market power and implementing abusive terms and conditions.

Generally, under EU law, exploitative abuses are prohibited under Article 102 TFEU. The exploitative abuses include a prohibition of unfair trading conditions, unfair pricing, or predatory pricing.[425] It remains accepted that price or trading terms might be unfair as to its effect on competitors. Yet, the case law affirmed that excessive trading conditions and/or prices could amount to abuse of dominance due to its effects on consumer welfare.[426]

It is nevertheless acknowledged that a pricing or set of commercial terms may be unfair to competitors. However, the case law confirmed that because of its consequences on consumer welfare, excessive trading conditions and/or pricing could amount to abuse of power.[427] Therein, the case of exploitative trading condition *BRT v SABAM,*[428] points to the 'fairness' of the clause requiring an assessment of all relevant interests. This is necessary to achieve proportionate assessment and ensuring a balance. Furthermore, in *Tetra Pak II*, the Commission raised an interesting point on the applicability of the proportionality test in exploitative abuse assessments.[429] According to the Commission, such clauses imposed "additional obligations which have no connection with the purpose of the contract and

---

[425] *United Brands* (n 195); Case C-333/94P *Tetra Pak International SA v. Commission* (Tetra Pak II), [1996] ECR I-5951; Case 395/87 *Ministère public v. Jean-Louis Tournier*, [1989] ECR 2521.

[426] *United Brands* (n 195) para 248.

[427] R Nazzini, 'Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision' (CPI, 2019) <https://www. competitionpolicyinternational.com/wp-content/uploads/2019/03/EU-News-Column-March-2019-4- Full.pdf> 23 June 2021; J Luzak, 'Preserving Consumers' Choice Online: Competition Law to the Rescue!' [2021] Tijdschrift voor Consumentenrecht en handelspraktijken 1.

[428] Case **C**-127/73 *BRT v SABAM;* ECLI:EU:C:1974:25, 27/03/1974

[429] *Tetra Pak II* (n 425) para 106.

which deprive the purchaser of certain aspects of his property rights."[430] In comparison to Facebook's case, the BKartA concluded that Facebook's privacy policy was not necessary to serve the social network to digital consumers and monetise the network through targeted advertising.[431] In addition, the BKartA performed an extensive proportionality test to weigh all relevant benefits.[432] From the BKartA perspective, the GDPR is based on a uniform level of fundamental rights to data protection, which makes it suitable for assessment under competition law.[433]

Arguably, GDPR violations can undoubtedly be grounds for exploitative abuse.[434] This approach requires case-by-case analysis, as mere violations of the GDPR do not amount to exploitative abuse. According to Article 7(4) GDPR, contractual performance is considered when evaluating voluntary consent. This shows that consent to the processing of data is of paramount importance. Performance of the contract is conditional regardless of whether the data controller holds a dominant position. The BKartA has taken care to justify appeals to the GDPR to prove violations of competition laws.[435] The BKartA stated that Facebook could not rely on the voluntary consent of users as per Articles 6 and 9 GDPR. Facebook's user consent could not have been seen as freely given if it is a precondition for the performance of a service and relates to the processing of data which is not necessary for the perforce of the contract. The BKartA provided that Facebook's dominant position and its direct network effect established a clear imbalance between Facebook and its users which deprived their consent of free nature. The data processing was seen as not necessary for the performance of a Facebook contract, as a dominant understanding cannot establish necessity by defining non-negotiate interests of its business models, which included personalisation. Processing of data would therefore be seen as only necessary if Facebook objectively indicated the need to engage in this processing for the preference of the contract. Without any viable negotiating mechanism, and clear indication of the data collecting practices, Facebook's users suffer from a serious intrusion into their privacy.

---

[430] *Tetra Pak II* (n 425) para 107.

[431] *Facebook case* (n 2) 10.

[432] ibid, 8.

[433] ibid, 10.

[434] This argument would be considered in detail in chapter 4.

[435] *Facebook case* (n 2).

Although the general position of EU competition law is to consider data protection-related damages outside the scope of EU competition law, the BKartA continued to rely on the case law of the Federal Court of Justice. The case showed that the protection of constitutional rights could be justified through the application of competition rules. This was based on the presumption that a dominant position provided for special unlawful privileges to abolish users' contractual autonomy.[436] GDPR violations themselves are not considered competitive harms, as not all privacy-related harms are considered competition-affecting. However, the BKartA noted that the GDPR violations are related to competition law. Facebook's market position was important given the circumstances surrounding corporate infringement. The BKartA therefore chose a cumulative approach and viewed the breach of the GDPR as a strong indication of abuse of a dominant position within the meaning of Article 19(1) of the GWB and Article 102 TFEU.

Moreover, the title of the Facebook's case summary, "Facebook, Exploitative business terms pursuant to §19(1) GWB for inadequate data processing"[437] BKartA could be deceived into thinking it was solely for exploitative abuse. However, the section of the case summary, titled "Manifestation of market power" points out that Facebook's behaviour is also likely to fall under the concept of exclusionary abuse.[438] The BKartA claimed that Facebook's conduct:

> "[I]mpedes competitors because Facebook gains access to a large number of further sources by its inappropriate processing of data and their combination with Facebook accounts. It has [...] gained a competitive edge over its competitors in an unlawful way and increased market entry barriers […]."[439]

The summary of the Facebook case may not explicitly mention exclusionary abuses, but it is still worthwhile to bring up the concept in relation to Article 102 TFEU. Based on the precedent set by *Post Danmark I*, Facebook's behaviour could be classified as exclusionary. In fact, Facebook's conduct amounted "to the detriment of consumers, of customers hindering the maintenance of the degree of competition existing in the market or the

---

[436] *Facebook case* (n 2), 9.

[437] ibid.

[438] ibid, 11.

[439] ibid.

growth of that competition."[440] In order to have a fair and healthy competition on the merits, any firm seeking data must obtain it through voluntary consent in compliance with GDPR regulations. If a dominant undertaking were to engage in unlawful behaviour, it would negatively impact both consumers and competition, and could be considered abusive. This could lead to a restriction of the competitive process, causing consumer harm and blocking competitors from the social media and online advertising markets. Therefore, Facebook's infringement of GDPR regulations is significant in terms of competition. While poor privacy protection could lead to lower quality, higher prices, or reduced innovation, the competitive impact of Facebook's conduct would be more focused on foreclosure, rather than just the GDPR infringement itself. Additionally, Facebook's GDPR breach could impact competitive processes. This is based on the *AstraZeneca* case,[441] where the infringement of other legal principles could amount to exclusionary practices. Generally, to determine the anticompetitive effects of GDPR infringement, it is usually necessary to identify the elements of abuse of dominant position. In some cases, it may be deemed acceptable that the unlawful acquisition of data can create barriers to entry that are difficult or even impossible to overcome. The 'data asymmetry' could affect in hindering competitive growth. Thus, to some extent, privacy concerns and competition principles may have distinct areas of authority. Nevertheless, this could only be useful as an additional factor in identifying competitive abuse.

Essentially, the Facebook case is the first antitrust assessment of unfair digital trading conditions and their corresponding effects on user privacy. It is an instance where the authority attempted to interpret both competition law and data privacy law uniformly, creating a normative framework enabling the application of both areas of law. The Facebook case had a pending appeal at the Higher Regional Court, Düsseldorf as its previous preliminary decision found serious doubts about the BKartA's analysis, being overruled by the German Supreme Court.[442] In 2020, The German Supreme Court reached a similar to the BKartA decision, indicating that the collection of data outside facebook.com was not seen as decisive for the performance of the contract.[443] The German Supreme Court confirmed that

[440] *Post Danmark* (n 277) para 24.

[441] *AstraZeneca* (n 99).

[442] *Case KVZ 90/20* (n 2)

[443] ibid.

Facebook abused its dominant position on the German social networks market to the detriment of users, overruling the decision of the Düsseldorf Court of Appeal from 2019.[444] Users were seen as locked-in to unfair trading terms with Facebook, depriving private users a choice as to whether they agree to more personalisation, with Facebook having, arguably, unlimited access to characteristics of any internet user. The case has been referred to the CJEU for a preliminary reference.[445] In relation to the intersection between competition law and data privacy law, the Higher Regional Court asked:[446] 1) whether the consent, as per the GDPR meaning, could effectively be given to a dominant undertaking;[447] and 2) whether the BKartA was competent enough to find the GDPR infringement in their competition law investigation.[448] If the answer was negative to the second point, the CJEU should consider whether the BKartA could assess Facebook's terms and conditions and its implementation's compliance with the GDPR.[449]

3.5.2. Facebook case at the EU level: AG Rantos Opinion

In 2022, AG Rantos delivered his Opinion on the Facebook case, with his decision intending to predict how the ECJ could interpret the intersection between competition law and privacy. In this section, I turn to scrutiny AG Rantos' Opinion and the discussion centred on it. I will consider two issues: (1) can an established violation of privacy by a dominant undertaking be seen as an instance of abuse?; (2) can this infringement (even if incidentally) be established not by a data protection authority but by the competition one?

---

[444] See the overruled decision, *Case VI-Kart 1/19* (n 2).

[445] *Meta Platforms, Opinion of AG Rantos* (n 85).

[446] In the light of the questions asked, the Higher Regional Court Düsseldorf enquired about the BKartA's finding, compared with Ireland's Data Protection Commission over Facebook's conduct. Data Protection Commission, 'In the matter of Meta Platforms Ireland Limited, formerly Facebook Ireland Limited, and the "Instagram" social media network' DPC Inquiry Reference: IN-20-7-4 (2022) <https://www.dataprotection.ie/sites/default/files/uploads/2022-09/02.09.22%20Decision%20IN%2009-09-22%20Instagram.pdf> accessed 25 October 2022.

[447] *Meta Platforms, Opinion of AG Rantos* (n 85) para 5.

[448] ibid, para 1.

[449] *Meta Platforms, Request for preliminary ruling* (n 311).

(1) Facebook's violation of data privacy law as an instance of abuse

AG Rantos opined that the BKartA did not penalise the breach of the relevant data protection laws by Facebook.[450] Instead, the BKartA analysed the alleged abuse of Facebook's dominant position, through consideration of Facebook's non-compliance with the GDPR provisions. In AG Rantos' view, BKartA's application of the GDPR in the competition law assessment was incidental.[451] The failure to comply with the GDPR can be taken into account when examining the overall legal and economic situation in which the behaviour occurs, together with all other relevant factors in the case. If competition authorities were prohibited from interpreting GDPR's provision, the effective application of EU competition law would be questioned.

While the absence of GDPR compliance cannot solely determine the legality of a conduct under Articles 102 TFEU, it is essential to recognise that GDPR adherence alone does not justify or validate a conduct's conformity with competition law either. In other words, the presence of GDPR non-compliance does not automatically imply a breach of competition rules. On the other hand, a dominant undertaking's compliance with GDPR does not immediately guarantee that it will not violate competition law. Both GDPR and competition law considerations must be evaluated independently to assess the lawfulness of any given conduct. In this respect, AG Rantos' interpretation of the incidental analysis of data privacy law in competition law assessment might provide some clarity on the matter by providing clear concepts on the interaction between both legal fields.[452]

AG Rantos focused on the lawfulness of Facebook's granted consent, which is a cornerstone of the BKartA's proceeding. In the BKartA's view, the requirement of giving consent to combine personal data from Facebook and third-party sources was prohibited as an exploitative abuse by a dominant undertaking. This was a manifestation of Facebook's antitrust conduct. According to AG Rantos, Facebook users were not given free or effective consideration, as required by the GDPR.[453] AG Rantos confirmed that Facebook's users did

---

[450] *Meta Platforms, Request for preliminary ruling* (n 311) para 18.

[451] ibid, para 24.

[452] ibid, paras 21-25.

[453] *Meta Platforms, Opinion of AG Rantos* (n 85) para 75; GDPR (n 57), recital 43: "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller."

not have any bargaining power before Facebook to indicate their privacy preferences.[454] Hence, Facebook's abuse takes place through the exploitation of users.

AG Rantos assessed the opt-in and lock-in of Facebook's users, to establish if their consent is freely given.[455] AG Rantos indicated that users have not intended to share their data with the general public, as opposed to specific third parties to which they transfer their data.[456] Also, user consent for the installation of cookies or similar programs, as per Article 5(3) of the Directive on Privacy and Electronic Communications, does not include the handling of sensitive personal data or count as a publishing action under Article 9(2)(e) GDPR.[457] AG Rantos believed that whether the data processing was justified by consent depends on a case-by-case basis, with the onus being on the data controller.[458] Users are not able to freely consent if they have no free and genuine choice as to whether consent or withdraw their consent without prejudice. Consent cannot be seen as freely given if terms and conditions are not negotiable, nor if there is a clear imbalance between the parties. AG Rantos argued that Facebook's dominance might act as an element to assess whether its users have given their consent freely.[459] In other words, even if there is no clear dominance or power imbalance, it still cannot be assumed that the user has given their consent freely and genuinely. In this respect, AG Rantos assumed that unlawful consent might have strengthened the platform's dominance.

AG Rantos continued by assessing the interpretation of GDPR towards the collection, processing, and use of personal data by Facebook and its owned substitutes. In other words, when a user signs up for Facebook's service, Facebook can collect a whole range of data protected on other sources different to Facebook. AG Rantos pointed out that possible justification under Article 6(1)(b)-(f) GDPR lays on Facebook and suggests a detailed case-by-case analysis of various Facebook's terms of service in the context of the practice at issue.[460]

---

[454] *Meta Platforms, Opinion of AG Rantos* (n 85), paras 74-77.

[455] ibid, para 74.

[456] ibid, para 42.

[457] ibid, para 72.

[458] ibid, para 71.

[459] ibid, para 74.

[460] ibid, para 50.

Article 6(1)(b) GDPR requires more than just the usefulness of data processing and requires necessity in the sense that there must be no realistic alternatives, considering the expectations of the data subjects.[461] In AG Rantos' view, Facebook encompassed not just personal data provided by users during sign-up but also personal data gathered from tracking users outside of Facebook.[462] Correspondingly, Facebook could derive great value and insight from collecting and processing the personal data obtained from third parties. AG Rantos indicated that personalisation might not be necessary for providing Facebook's services, and personalisation of advertising and product improvement might be seen as a legitimate interest of data collecting in the sense of Article 6(1)(f) GDPR.[463] In the balancing of interest under Article 6(1)(f) GDPR, the referencing court would have to consider the off-Facebook nature of collected data and the degree of personalisation, the purely economic nature of such interest and users' reasonable expectations. The onus to show that data processing is necessary for achieving its legitimate interest will be on Facebook.

About Article 6 GDPR, BKartA and AG Rantos had a similar approach, carrying a multi-factor analysis of the consent validity, necessity of Facebook to data collecting and processing practices, and a resulting imbalance between the parties and users' expectations. It has been pointed out that that platform's dominance and the invalidity of consent increased the relevance of competition law intervention.[464] There are still certain variations between the BKartA's and AG Rantos' approaches. For example, BKartA consider the data processing importance under Article 6(1)(f) GDPR, while AG Rantos suggested the case-by-case analysis of the consent is required, as a proxy to demonstrate Facebook's dominance.[465] AG Rantos seemed to propose a requirement to balance all relevant circumstances in the case. AG Rantos approach might be seen as quite challenging not because he considers Facebook's burden of proof for the necessity of data processing practices, but also because of his openness of legal analysis which has not been yet tested in courts. With respect to the given imbalance between Facebook and its users, the courts should demonstrate that such

[461] *Meta Platforms, Opinion of AG Rantos* (n 85) para 53.

[462] ibid, para 44.

[463] ibid, para 58.

[464] I Graef and S Van Berlo, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility' [2020] European Journal of Risk Regulation 674.

[465] *Meta Platforms, Opinion of AG Rantos* (n 85) para 76.

imbalance does not necessarily prevent valid consent but might be an indicator that users' consent was not given freely. AG Rantos' consideration of the appropriateness parameter for a given consent might contribute to rendering a user's consent valid in certain specific instances.

Facebook T&Cs were seen by both AG Rantos, BKartA and a refereeing German court as unfair. The BKartA considered that offered business terms to be abusive under §19(1) GWB, requiring merely a normative causality between Facebook's dominance and the antitrust effect of its conduct.[466] In other words, due to the dominance of Facebook in the market, Facebook's terms of service must result in an anticompetitive effect. In fact, normative causality exists between Facebook's dominance and its anticompetitive conduct, resulting in an imbalance between the parties and Facebook data collecting and processing practices, which exploited users. AG Rantos has not considered the causality between Facebook's dominance and its exploitative abuse. Form a perspective of EU competition law, AG Rantos might have opted for a requirement closer to causality as addressed by BKartA. A stance taken by AG Rantos on causality would have likely consumed that his assessment brings Facebook's case to the BKartA's assessment. AG Rantos Opinion indicates that market power could not render GDPR parameters irrelevant, especially while considering the validity of a given consent and data processing and collection practices which have given a clear link between a large undertaking's dominant position and anticompetitive practices.[467] Accordingly, the prohibition of handling sensitive personal information could also encompass indirect methods of processing, such as combining datasets containing proprietary information from online users and creating profiles for economic gain. Competition law allows for the inclusion of incidental factors in its considerations of privacy-related infringements. It can be implemented within the broader context of the legal and economic environment in which the conduct takes place. This is done to determine whether the conduct involves utilising alternative methods that differ from competition based on merit.

(2) Competition authorities' competence to apply data privacy breaches

For the BKartA's finding of Facebook's abuse, the stipulation and implementation of Facebook's terms must infringe GDPR principles. Hence, for finding a competition law

[466] *Facebook case* (n 2).

[467] See *Tetra Pak II* (n 425).

infringement from the violation of provisions outside competition law,[468] BKartA considered German case law which indicated that inappropriate contractual terms and conditions offered by a dominant undertaking can amount to an abuse in the competition law sense.[469] BKartA adopted such consideration and indicated that GDPR indeed could serve as a suitable parameter for whether offered terms and conditions are appropriate, especially because GDPR pursues the goal to counter imbalances between companies and private individuals.[470]

Procedurally, the BKartA considered itself as being competed to assess Facebook terms' compliance with GDPR: although competition authority does not have an explicit competence to enforce the GDPR, it can assess GDPR compliance as a part of the enforcement of competition law.[471] In fact, Article 60 GDPR aims to ensure cooperation of consistency and does not provide any restrictions on such an approach. The question of a NCA's mandate to consider GDPR was referred to the CJEU.

AG Rantos Opinion concluded that the BKartA did not penalise the breach of the relevant data protection laws by Facebook.[472] Instead, the BKartA analysed the alleged abuse of Facebook's dominant position, through consideration of Facebook's non-compliance with the GDPR provisions. Consequently, AG Rantos Opinion deemed irrelevant the question on the BKartA's competence to establish a breach of the data privacy law.[473]

In AG Rantos' view, the BKartA's application of the GDPR in the competition law assessment was incidental.[474] AG Rantos underlined that a national competition authority should scrutinise if an undertaking resort influence a merit-based competition.[475] Hence, GDPR compliance of a conduct in question could be a vital clue in the fact-based assessment of an individual case. Simultaneously, AG Rantos remained cautions that Article 102 TFEU violation

---

[468] see Van Rompuy (n 181) 227.

[469] For example, BGH, 07.06.2016, KZR 6/15, *Pechstein/International Skating Union*, para 48.

[470] *Meta Platforms, Opinion of AG Rantos* (n 85) para 53.

[471] ibid.

[472] ibid, para 18.

[473] ibid, para 19.

[474] ibid, para 24.

[475] ibid, para 26.

was not apparent from a lack compliance with the GDPR. The GDPR breach on its own cannot be seen as unlawful under Article 102 TFEU. Instead, an incidental consideration of privacy-related harms could guide the assessment of data-related anticompetitive harms. In order words, without the GDPR infringement, conduct that harmed competition would not exist at all.

Additionally, AG Rantos acknowledged that if the conduct in question did not comply with the GDPR provision, then it could be considered in a broader manner of the legal and economic context, and other relevant circumstances of the case. Even an incidental consideration of GDPR rules by an NCA could potentially undermine a consistent application of GDPR, as NCAs would interpret GDPR principles differently than a data protection authority. In the absence of specific EU rules on the cooperation between NCAs and data protection authorities, the general duty of good faith of Article 4(3) TEU and the principle of sound administration applies, which are based on extensive duty of diligence on the part of national authorities.[476] AG Rantos assumed the duty of competition authorities to cooperate with data protection authorities excited. Such cooperation needs to comply with national procedural law and the EU rules on effectiveness and equivalence. Although AG Rantos concluded that competition law and GDPR pursued different objectives, his decision emphasised the possibility of competition law incidentally considering privacy-related harms without triggering the ne bis in idem principle, if a data protection authority decided over the same case.[477]

Competition authorities should be able to take into considerations violation of legal provisions beyond competition law as an ancillary aspect during their examination of abusive practices. However, a mere violation of legal provisions beyond competition law does not directly lead to identifying anticompetitive behaviour. Even the incidental consideration of GDPR rules could conflict, with the outcome and the measures undertaken to reach it. In other words, NCAs which sanction an antitrust violation of the GDPR, could factually also add the position of the GDPR enforcer. Based on such consideration, AG Rantos pointed this out so clearly and calls for coordination between authorities.[478]

---

[476] *Meta Platforms, Opinion of AG Rantos* (n 85) para 29.

[477] ibid, para 28.

[478] ibid, para 29.

AG Rantos' consideration of the legal basis and modalities of such cooperation are possibly the most remarkable part of his opinion. AG Rantos derived from the duty of cooperation in good faith and sound administration to the novel regime interaction of NCA and data protection authorities.[479] AG Rantos emphasised a lack of context-explicit mechanisms for inter-authority coordination in several parts of secondary EU law.[480] However, the rationale for inter-authority coordination could be traced broadly to the need to ensure consistency between the actions of competition law and non-competition law authorities, reducing possible duplication and enabling them to achieve their objectives.[481] For instance, competition authorities should only cooperate with a focus on a GDPR violation. While NCAs might impose behavioural remedies that address competition concerns, data protection authorities might only address privacy-related concerns. In AG Rantos' consideration, the NCA should at the very least inform and cooperate with data protection authorities to protect competition.[482] Privacy in competition cases implies privacy considerations. Given the fact that competition authorities are not equipped with specific resources for enforcing legislation beyond competition law, the non-competition authorities should be ready to continue the investigation cases having a focus on their respective competence area.

3.5.3 The CJEU decision: incidental privacy-related harms as a competitive theory of harm

In July 2023, the CJEU provided a further discussion on the dilemma about the possible interaction between competition law and data privacy law.[483] Importantly, the judgement provided by the CJEU is especially directly to German competition authority and should not be seen as providing guidance in the context of Article 102 TFEU interpretation. In other words, the judgement focused on taking into account GDPR concerning the specific and unique implementation of §19(1) GWB. In this section, I analyse the decision in the light of: (1) acknowledging privacy-related harms as a possible parameter of competition law; (2) the mandate of competition law authorities to consider data protection infringements.

---

[479] *Meta Platforms, Opinion of AG Rantos* (n 85) para 32.

[480] ibid, paras 27, 29 and 32.

[481] Stucke and Grunes (n 8) 325- 334.

[482] *Meta Platforms, Opinion of AG Rantos* (n 85) para 32.

[483] *Meta Platforms* (n 41)

(1) Processing of personal data as a parameter of competition law

The CJEU demonstrated that Facebook's digital operations are subsidised via online advertising: users registering with Facebook accept its offered terms of series and consequently its data and cookies policies.[484] According to offered by Facebook's terms of service, Facebook collects data about its users' activities on and off the social network and links the data with the Facebook account of the users concerned. The collected data serve to create personalised advertising for Facebook users. The CJEU continued to establish that Facebook's business model and online advertising are possible, in technical terms, by the production of users' profiles and the online services offered by the Facebook group. In other words, the CJEU considered that the utilisation of personal data by Facebook is influenced by technical limitations rather than deliberate economic or strategic choices that drive Facebook's exploitation of user data.

While assessing Facebook's data collecting and processing practices, the CJEU agreed with AG Rantos Opinion and indicated that BKartA has not found that a breach of GDPR led to anti-competitive harm.[485] Instead, the Court determined that the BKartA's examination of Facebook's data processing activities aimed to assess their alignment with the fundamental principles of the GDPR.[486] Importantly, the way the case is portrayed demonstrates a subtle yet significant difference: the outcome would have been different if the CJEU believed that the BKartA had directly applied the GDPR to the case (even considering the unique procedural differences) which is explicitly prohibited from occurring**.** Instead, the incidental consideration of GDPR is possible in the context of larger economic conduct surrounding anticompetitive conduct. Such a practice is crucial in balancing interest in decisions under competition law.[487] Importantly, the BKartA's comprehensive analysis has not involved a substantial interpretation of the GDPR beyond its competencies. Instead, the BKartA only focused on examining each legal requirement under the GDPR to determine whether there was a breach of competition law. The aim was to assess whether Facebook's data processing activities were performed in conformity with the GDPR and ensured consistency in Facebook's analytical and collecting practices of user data.

---

[484] *Meta Platforms* (n 41) para 50.

[485] ibid, para 62.

[486] ibid, para 30.

[487] ibid, para 147.

The CJEU addressed whether Facebook's processing activities were lawful under GDPR: Articles 6(1)(a) and 9(2)(a) GDPR were of a particular interest as they related to the nexus between market power, imbalance in the sense of GDPR and exploitative conducts.[488] Here, the ruling did not appear to engage in a process of balancing between competition law and data privacy law. Instead, it offered more direct conclusions. The CJEU established that processing of Facebook's data was unlawful under Article 9(2) GDPR, mirroring the approach taken by AG Rantos — Facebook has been involved in the processing of specific categories of personal data without the consent and clear understanding of the implications for individuals who registered on the social network.[489]

However, it is important to note that the CJEU discussed the idea of embracing GDPR from a broader antitrust perspective.[490] The CJEU went further to acknowledge the significance of personal data collection and utilisation in the digital economy, without involving fundamental user rights.[491] This is particularly relevant for business models that fund themselves through personalised advertising like the Facebook group. Correspondingly, the CJEU argued that the ability to access personal data, along with the processing of this data by Facebook (after aggregating and connecting them into extensive datasets), could be regarded as a competitive factor among companies in the digital economy.

The market dominance of the data controller did not exclude users' valid consent, but it might affect the freedom of users' consent.[492] The CJEU discussed Facebook's capacity to justify its processing activities in the context of the consent under Article 6(1)(a) GDPR, although having a dominant position does not inherently ban users of a social network from giving their valid consent.[493] Facebook's dominance might create imbalances preventing valid consent. However, the CJEU indicated that the responsibility falls upon the German court to evaluate whether users were unformatted to grant their consent freely when using

[488] *Meta Platforms* (n 41) para 154.

[489] ibid, paras 147-154.

[490] ibid, para 62.

[491] ibid, para 117.

[492] ibid, para 147.

[493] ibid, paras 140-147.

the Facebook buttons on external websites. The CJEU emphasised that the assessment of Facebook's justification for processing user personal data within their services, apps, and on third-party websites is grounded in Articles 6(1)(b)-(e) of the GDPR, leaving a narrow space for the referring court to interpret broadly in favour of Facebook regarding the legitimacy of their data processing actions.[494] Here, the CJEU discussed that Facebook's current approach to generating revenue involves supporting its services through online advertising, the company is indeed capable of developing alternative solutions to offer its products online, where extensive processing activities are either minimised or absent.[495] Crucially, this strategy did not constitute a complete ban of the possibility of Facebook justifying contracts involve both network access and extensive data processing through consent. Instead, this could entail users potentially needing to pay a suitable fee to account for the value of the service for collection of possible non-necessary data,[496] and including a clause within a contract emphasising on a possible non-necessary processing activity.

In fact, such a formula should not be seen as adding novelty to the competition law regime, as the EU Commission termed privacy as a parameter of competition in *Microsoft/LinkedIn* or *Facebook/WhatsApp*.[497] With the CJEU labelling access to and the ability to process personal data as a competitive factor, the CJEU refrained from expressing a judgement that favours business models prioritising privacy (where more privacy is seen as preferable for consumers). Instead, the CJEU emphasised that the level of access and processing capacities carries importance in competitive dynamics, regardless of their connection to the GDPR.[498] It becomes apparent that a digital platform's activities can be a vital clue in assessing the platform's deviation from normal competition. However, this perspective does not appear to be applicable when it comes to interpreting the GDPR in relation to the platform's dominance.[499] Instead, the CJEU claimed that dominance could play a crucial role in deterring whether user consent is freely given for the data controller's processing

[494] *Meta Platforms* (n 41) para 154.

[495] ibid, para 148.

[496] ibid, para 150.

[497] See section 3.4 above for a detailed discussion.

[498] *Meta Platforms* (n 41).

[499] ibid, para 151.

activities.[500] Consequently, the interaction between these legal domains takes into account the potentially exploitative nature of a large digital undertaking's behaviour. Yet, the idea of this exploitation might not be inherently regarded as a prominent factor in determining whether a platform can lawfully engage in processing personal data.

The CJEU approach affirmed the AG Rantos' Option with some adjustments. The exploitative abuse should be an indirect matter of the GDPR assessment, especially regarding consent validity. The CJEU clarified that a GDPR violation does not automatically constitute an abuse, particularly not without regard to balancing a genuine competition law interest and consideration. However, the line of CJEU's argument, together with its emphasis on the data controller bearing the burden of proving valid consent, makes it highly improbable to establish a successful consent justification.[501] The CJEU discussed the notion of consent in detail, increasing legal certainty compared with the approach provided by AG Rantos: a dominant data controller has to determine if the data processing activity is essential for its primary service to its users within a contract. Yet, the CJEU has not engaged in establishing the casualty requirement whether: (i) there is a causal link between Facebook's action and its anticompetitive effect resulting from its dominance; (ii) it is essential to prove that Facebook can enforce its exploitative terms due to its market dominance. Against this background, the CJEU steers the consideration that a large digital undertaking's access to personal data should be seen as a parameter of competition law and a GDPR violation resulting from a lack of consent constitutes a vital clue for finding an abuse within Article 102 TFEU in the digital economy. However, this should not be seen as a goal or an indicator that should be applied across the board into EU competition law.

(2) Competition authority's necessity to apply data protection regulation

Although the CJEU ruling might be read as proving leeway for the incorporation of data privacy law considerations into the competition law analysis, the CJEU provided limitations at the institutional level to narrow down the NCA's capacity to produce its findings based on the GDPR rules. The view adopted by the CJEU reflects on the arguments presented by AG

[500] *Meta Platforms* (n 41) para 154.

[501] ibid, para 152.

Rantos and emphasises the need for the duty of sincere cooperation under Article 4(3) TEU.[502]

In practice, the duty of sincere cooperation frames a whole set of scenarios which in principle defines potential coordination between NCA and data protection authorities. In principle, NCAs are required to consult with the national data protection authority to observe their respective competencies.[503] Hence, even if there is no risk of divergence, NCAs are obliged to consult a competence data protection authority to resolve an issue in question.

In the instance of a possible risk of interpreting GDPR rules in a divergent manner, then the principle of necessity steps in.[504] The CJEU has not provided clear guidance on what the necessity means in this contact. Instead, the CJEU emphasised that by excluding the GDPR consideration by the NCA could result in ineffectiveness of competition law within the EU.[505] Hence, it is deducible that the NCA's capacity to interpret the GDPR provision in the antitrust conduct is circumscribed to those occasions where consideration of data protection rules is necessary to establish a competitive infringement.[506] In the context of a wider duty to cooperate, NCAs cannot fully depart from privacy-related infringements and cooperation with a competent data protection authority. At the enforcement and advocacy level, different measures ordered by various authorities to assess GDPR violations might conflict with each other.[507] Competition and data protection authorities need to be careful to not overextend their competencies. In the case of enforcing competition law and data protection law together, the French *GDF Suez* case[508] serves as an interesting example where the ordered competition law remedy arguably introduced privacy issues.

---

[502] *Meta Platforms, AG Rantos Opinion* (n 53) para 28.

[503] *Meta Platforms* (n 41) para 54.

[504] ibid, paras 55–56.

[505] ibid, para 51.

[506] ibid, para 48

[507] Reyna (2023) (n 152).

[508] Autorité de la Concurrence, 'Press release, 9 September 2014: Gas Market' (2014) <https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9-september-2014-gas-market> accessed 2 August 2023.

In the *GDF Suez* case, the former gas monopoly used its database on regulated tariffs for personalised offers on gas and electricity to its consumers. In this case, GDF Suez's competitors were disadvantaged as they could not replicate the database. Correspondingly, Autorité de la Concurrence ordered GDF Suez to grant its competitors access to its historical files, containing consumer and consumption data. In response, the French data protection authority issued an opinion that Autorité de la Concurrence should ensure that competition remedy complies with data protection law.[509] The competition remedy allows for a possible opt-out option to share data, if consumers explicitly opposed to data-sharing within 30 days. There is doubt regarding whether such a competition remedy safeguards privacy. Theoretically, in this context, the GDF Suez uses' actual choice might be different from their preferred choice. Instead, users could consent to their desired choice with an opt-in mechanism than an opt-out option. The French *GDF Suez* case might illustrate a possible dilemma between competition law and data privacy law, as the protection of competitive process might introduce adverse effects on the protection of users' privacy. However, it is not to suggest that competition law remedy would inevitably breach data privacy law. Instead, the purpose of competition law and data privacy law is to protect consumers in a B2C relationship against harmful behaviour that could make users worse off.[510]

To mitigate the possible risks of divergences in the interpretation of the GDPR rules, the CJEU hinted that the Facebook case illustrates how to possibly solve the dilemma between competition law and data privacy. Arguably, the CJEU approach introduced a nuanced and hierarchal, integration grid.[511] NCAs are required to ascertain if the behaviour in question has already been addressed in a decision made by the relevant GDPR authority or the CJEU.[512] In this respect, a competition authority cannot depart from such a decision, but it remains free to draw its conductions from a competition law perspective. This consideration departs from AG Rantos' approach who underlined that the competition authority would have had to consult and reach consent with the GDPR authority, in the case of 'doubts' over

[509] Autorité de la Concurrence, Décision N° 14-MC-02 du 9 Septembre 2014 Relative à une Demande de Mesures Conservatoires Présentée par la Société Direct Energie dans les Secteurs du Gaz et de l'électricité, September 9, 2014, para. 289.

[510] Pasquale (n 163).

[511] *Meta Platforms* (n 41) para 54.

[512] ibid, paras 49 and 56.

the GDPR authority interpretation.[513] The CJEU preferred to favour an approach where the GDPR authority enjoys an interpretational primary, while the competition authority can independently determine whether conduct does or does not violate the GDPR according to the GDPR authority's interpretation. This is particularly relevant in the context of assessing potential abuses. In other words, an assessment under Article 102 TFEU might demonstrate that privacy-related conduct distorted competition on the merits, whereas the GDPR authority might have considered it as lawful under Article 6 GDPR. Future cases will demonstrate how this rationale plays out in practice. The absence of a consensus requirement will make it easier to enforce competition law based on the GDPR, and in this regard, evaluating the lawfulness of conduct under different sets of rules, even outside of competition law, is not a particularly new or unique concept. For example, claims based on intellectual property rights might be unlawful from the perspective of intellectual property law, whereas competition authorities can consider them as introducing antitrust effects.[514]

In this respect, the CJEU indicated that the principle of cooperation matters, but also emphasises on the effectiveness of competition law enforcement. In this consideration, the CJEU still requires competition authorities to consult the GDPR authority when: (i) it is not clear whether a prior decision from a GDPR authority applies to a specific case in question; (ii) there is no existing decision, but similar conduct is reviewed by a GDPR authority; (iii) there is no decision or an ongoing investigation and a competition authority believes that the conduct in question infringed GDPR.

Considering the limited resources available to GDPR authorities, it is possible that granting precedence waivers may become more common in the future.[515] In instances where asserting precedence does not appear to be essential from the perspective of the GDPR, but could cause significant delays in competition law enforcement,[516] the duty of cooperation should even require the GDPR authority to waive precedence. GDPR-compliance assessments conducted by competition authorities have no binding effect on GDPR

[513] *Meta Platforms, AG Rantos Opinion* (n 53) para 30.

[514] Case T-172/21 *Valve Corporation v Commission*. Luxembourg, 27 September 2023.

[515] *Meta Platforms* (n 41) para 60.

[516] GDPR (n 57) article 78.

authorities[517] but could influence examination of the same conduct by these authorities. Correspondingly, competition authorities can contribute to GDPR enforcement. There should be an opportunity for the GDPR and competition law authorities to maintain ongoing contact, which is not limited to a single interaction but should be available through the assessment process. Such a point has not been mentioned by the CJEU, but Article 4(3) TFEU offers the necessary flexibility for this and further elaboration of the CJEU's fundamental framework. This would be especially useful for discussing and refining the competition authority's preliminary position on whether the conduct complies with GDPR.

3.6. Conclusions

This chapter examines the scenario in which a dominant company is subject to legal action or enforcement measures because of its mismanagement of user data under Article 102 TFEU. I note that competition law and data protection law are two different and separate legal orders. However, data protection (and privacy protection) and competition policy share foundational concerns and similar remedial approaches: how to mitigate unfairness by introducing and imposing obligations on those with information or market power. Essentially, the goal is to prevent power imbalances arising between individuals and powerful companies. However, not every breach of privacy might be relevant to competition law analysis.

The Commission practice demonstrates that they can detect market power and abuse in cases involving digital companies. Data protection legislation offers only a partial response to the exploitation of personal data: Data protection law does not recognise the long-term harms to the platform users, including the special responsibility that could ensure the position of power of some digital platforms. Competition law and its theories of exploitation and exclusion might complement data protection law in this context. I assume that that the intersection between competition law and data privacy law requires a further, more nuanced analysis of the tradeoffs and policy choices between competition law and privacy. Privacy protection can only impact competition law when privacy is a key parameter of competition and is not the case for consumer communication apps where price, user base, popularity or reliability are important factors. I argue that it is important to not lose sight of

[517] *Meta Platforms* (n 41) para 49.

the fundamental principle that what is relevant in a competition assessment involving privacy concerns are market-driven privacy standards.

It has been also suggested that competition authorities can act in tandem with data protection enforcement at both the national and European levels, simultaneously pursuing distinct goal and preserving market competitiveness. With AG Rantos and the CJEU opinions, privacy-related harms could potentially be seen as incidentally influencing competition law assessment. Both AG Rantos' and the CJEU's approaches could become the reference for how competition authorities could accommodate conducts designated for the GDPR assessments. It could also function as an instructive model for similar situations with shared jurisdiction, such as those involving GDPR authorities and competition law enforcers. By contextualising the issues raised by the *Facebook* case and previous data-related competition law assessments, this chapter explored what ways market power needs to be taking into account privacy as a parameter in competition law. However, as demonstrated, competition law should be applied in pursuit of its goals, with reflection that privacy matters. This raises an important consideration when developing well-sustained understanding of whether privacy harms might be accounted as a competitive theory of harm. This issue is considered in the next chapter.

Chapter 4: Effectiveness of competition law in dealing with privacy-related harms

4.1 Introduction

The previous chapters have shown that there is not a comprehensive regulatory framework addressing all facets of privacy-related harms, emphasising the need to address the problem through various regulatory systems from different angle. The discussion has indicated that Article 102 TFEU can be inherently open-ended, and the appropriate competition authority might take an external-to-competition policy as a proxy to find an antitrust conduct. Given that data protection rules are explicitly designed to address the concerns of individuals having insufficient control over their personal data, it serves as the primary route of redress when remediating privacy-related harms. GDPR inherently aims to solve possible challenge of information and power imbalances and safeguards individuals' fundamental right to determine the extent of data collection and its processing. On the other hand, competition authorities can only investigate conducts that are detrimental to the competition on the merits. Privacy-related harms have not been considered as a directly amounting to competitive theories of harm but were considered as influencing the investigation to find the abuse in a broader context. It is still questionable how to bring possible privacy-related harms within the scope of competition law, which aims at safeguarding competitive prices and prompting users' choice how much data they are willing to discuss under what conditions.

Based on the findings from the previous sections, this chapter focuses on an examination of assumptions of the theories of harm underlying privacy analysis in competition law. There has been an argument that competition law possesses a versatile toolkit for evaluating market power and dominance, particularly in cases involving digital companies. In this respect, I demonstrate that competition law account could be joined into a more holistic or pluralistic approach. I argue that it is preferable to adopt value pluralistic approach to creating a framework that accommodates privacy-related harms, which appears objectively justified. This is especially the case of large digital undertaking's business model, based on exploitative data collection and processing. This chapter analyses potential exploitative theories of harm in the context of user privacy breaches. The focus is on privacy-related theories of harm in the context of digital markets and the appropriate welfare standard. In

fact, the theories of harm could involve a 'citizen perspective', which is not confined to a narrow economic rationale, but is based on aspects of democracy or fairness. This emphasises on the open-ended nature of Article 102 TFEU. With the rise of Big Data acquisition and analytics, one question becomes pressing: to what extent (if any) could privacy breaches serve as an element of competition assessment? The question is based on the consideration of whether the relationship between competition law and data privacy law could lead to positive effects of competition on privacy. In other words, the rationale of Article 102 TFEU appears to not be endorsed to a certain ultimate goal, but its reasoning involves deontological and consequentialist approaches.

With this consideration in mind, section 4.2 discusses the effectiveness of competition law in dealing with privacy-related harm. As this section explains, most data-related anticompetitive investigations are not expressly focused on the individual's data privacy. However, competition law agencies have recently paid attention to novel instances of digital market-based abuses of dominance and have focused their attention on the role of data in competition assessment. With the findings from section 4.2, section 4.3 focuses on analysing to what extent undertakings could rely on improvements of privacy to avoid anticompetitive liability within the context of Article 102 TFEU. Though this theory is at an early stage, competition law agencies have begun to question whether increased protection for individuals' data privacy could justify otherwise anticompetitive conduct and avoid possible exploitation of users through an increased data collection. This is one of the most nascent interactions on the horizon between competition law and data privacy law. To scrutinise the findings, recent developments introduced by Google and Apple are discussed.

4.1.1 Reason to focus on exploitative abuses only

It is beyond the scope of this thesis to consider all potential privacy-related theories of harm. I delimit the scope of the examination of the assessment to focus on exploitative theories of harm: the conducts allowing large digital undertakings to exploit their market position to the detriment individual undertakings and consumers. Exclusionary conduct as the behaviour of a dominant undertaking might introduce foreclosure effects on the relevant market, ultimately harming consumers. The Commission includes the harms to consumer welfare in enforcement priorities regarding exclusionary conduct. Yet, there is nothing to suggest that the Commission thinks there is only one type of abuse: there is instead an

emphasis on the separation of 'exploitation' from 'exclusion', leaving exclusionary abuses without any guidance on its substantive assessments. Elaboration on 'exploitative' abuse is crucial in the application of Article 102 TFEU if the objective is to be on consumer welfare. The business models of zero-priced online platforms rely on the acquisition and processing of consumer data. In fact, this relates more to potential users' exploitation rather than exclusion, in ways that have not previously been considered. Here are my preliminary observations:

1. The emerging digital economy has raised concerns regarding the interaction between competition law and privacy and the need for a more articulate approach between these areas of law, as they both aim to avoid the exploitation of consumer's personal data and privacy.

2. Article 102(a) TFEU is broad enough to cover various types of exploitative conducts. Excessive data acquisition could be captured as a form of unfair trading conditions within the meaning of Article 102(a) TFEU.

3. As digital platforms have begun to offer subscription-based models, where digital platforms seek alternative revenue streams and/or where users prefer ad-free experiences, users could be subjected to abuses of excessive pricing due to unfairly imposed prices to accept free-ads versions. In fact, such a scenario of exploitative harm is hypothetical.

4. While Google's and Apple's efforts to improve users' privacy are significant, they could potentially create a false sense of security among consumers. Google's and Apple's pro-user and pro-privacy advancement could advance consumer fallacy and act as a proxy to further data collection of digital giants and exploit users.

The discussion below focuses on these concepts and tests its legal credibility.

4.2: Exploitative abuse and privacy: analysis

4.2.1 Conceptualising exploitative abuse and privacy infringement

Over decades, the concept of abuses under Article 102 TFEU has expanded to capture novel forms of abuse conduct. This process has opened the prospect of dealing with non-exhaustive forms of unique categorisation of abuse of a dominant position. Such judicial formalism has prevailed in an overarching approach towards preventing market distortions for 'the detriment of the public interest, individual undertakings, and consumers' with a notable addition of consumer 'well-being'.[518] Hence, the outcomes of the individual investigation are based on a case-by-case consideration, which has not signalled a major enforcement change.

Large digital companies[519] are capable of collecting and processing extensive amount of personal data, which could allow them to exploit their position in their relevant market.[520] Existing theories of harm might be used by the Commission on their investigations against large digital firms. From a competition law perspective, data collection might amount to exploitative abuse, taking the form of excessive price, or unfair terms and conditions. As per the CJEU's wording, excessive pricing is prohibited as a monopolist, relying on its monopoly position, "reap trading benefits that [he] would not have reaped if there had been normal and sufficiently effective competition."[521] Such cases demonstrated the difficulty in establishing the 'excessiveness' of a price.[522] Potentially qualifying excessive data acquisition as an excessive pricing abuse could imply that data collection transfers into a quantifiable price.[523] It is, however, beyond the scope and methodology of this thesis to reproduce a multifaceted debate on the monetary value of data. For the purposes of this research, it is noted that the views on the monetary value of data differs amongst market participants.

---

[518] See, Case T-399/16 *CK Telecoms UK Investments Ltd v EC* [2020] ECLI:EU:T:2020:217, para 93.

[519] For the purposes of this research, I refer to example of GAFAM practices.

[520] Gebicka and Heinemann (n 217) 165.

[521] *United Brands* (n 195) para 250. However, for a similar considerations see also *BRT v SABAM* (n 428); Case C-179/90 *Merci Convenzionali Porto di Genova SpA v Siderurgica Gabrielli* [1991] EU:C:1991:464; M Gal, 'Abuse of Dominance - Exploitative Abuses' in I Lianos and D Geradin (eds), *Handbook on European Competition Law* (Edward Elgar 2013) 385–422.

[522] V Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2020) 57 (1) Common Market L Rev 161, 169.

[523] Ioannis Lianos and Evgenia Motchenkova, 'Market Dominance and Search Quality in the Search Engine Market' [2013] JCL&E 419; Kerber (2016) (n 83) 860.

Clearly, the value of data varies by the type of data,[524] individuals,[525] and non-monetary values such as morality and privacy.

In fact, excessive data acquisition could take the form of unfair trading conditions within the meaning of Article 102(a) TFEU. Users accept qualifying trading conditions before accessing digital platforms without understanding such conditions. This is uncontroversial, given the role data plays in such agreements.[526] Such trading conditions might be seen as unfair if imposed obligations are not necessary for the agreement object, or if the agreement is deemed disproportionate.[527] It could be seen as exploitative if online users access a service that does not reflect the value their data represents to such a platform. In this section, the potential exploitative theories of harm in the context of user privacy breaches are addressed.

4.2.2. 'Take it or leave it' scenario: unfair trading conditions and practices

The assessment of unfair trading conditions is carried out in the consideration of B2C contracts, which reflects the nature of the GDPR enforcement. This is a deviation from the previous case law that instinctively focused on business-to-business contracts.[528] This thesis will offer some conceptualisation of this potential approach, which focuses on the reduction of quality of concerning services, or other exploitative effects.

In the *Google Search (Shopping* case),[529] the monetary considerations of consumer data were recognised, while the *Google Android* case recognised that the combination of consumer data can be derived from multiple applications for different purposes, such as

---

[524] Kerber (2022) (n 158); Stucke (n 26).

[525] Tsai, Egelman, Cranor, and Acquisti (n 206); G Skoumu and L Leonard, 'On-line Behavioural Tracking: What may change after the Legal Reform on Personal Data Protection' in S Gutwirth, R Leenes, P de Hert (eds) *Reforming European Data Protection Law* (Springer 2015) 45; Costa Cabral and Lynskey (n 152) 21-22.

[526] G Schneider, 'Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's Investigation against Facebook' (2018) 9 JECLAP 213, 220

[527] *BRT v SABAM* (n 428) para 15; Commission decision IV/29.971 of 4 December 1981, *GEMA II*, OJ 1982 L 94/12, para 36.

[528] *Deutsche Post AG* (Case COMP/C-1/36.915) Commission Decision 2001/892/EC [2001] OJ L331/40; Pinar Akman, *The Concept of Abuse in EU Competition law: Law and Economic Approach* (Hart Publishing 2012).

[529] *Google Search (Shopping)* (n 192).

Gmail for location data, Chrome for search data and/or YouTube for experience data.[530] The CJEU affirmed that the Android-operated devices collected valuable consumer data, such as location or usage data extracted from advertising.[531] Also, in the CMA's investigation into Google's Privacy Sandbox, the CMA illustrated an increased consumer awareness of their data privacy when accepting Google's commitments, such as non-disclosure of consumer data collected from Chrome analytics, browsing history and third-party cookies for targeted advertising, business secrets, algorithm, non-discrimination and non-tracking.[532]

Competition law and data privacy authorities focus their attention to terms and conditions offered by digital platforms, where consumers grant consent to data collection and processing of their data in return for accessing a service.[533] Digital products and services require consent to use data as a condition for accessing their service.[534] Individuals are faced with a choice: they need to accept the said terms otherwise they are not able to use the service. Such conditioning of service access has been referred to as a 'take it or leave it' scenario, which could be indicative of an imbalance in bargaining power between gatekeepers and consumers.[535] Under Article 102(a) TFEU, unfair trading conditions could be accounted as an abuse of a dominant position.[536] The content of unfair trading conditions is unquestionably broad: competition authorities are equipped with a high degree of discretion with policy, while the courts rely on a high degree of appreciation to frame the scope of a certain legal category seen as appropriate.[537] Unfair trading conditions are often cast as consumer protection issues. The CMA linked unfair digital trading conditions as a competition law issue, articulating that:

---

[530] Case T-604/18 *Google & Alphabet v EC* (*Google Android)* [2022] ECLI:EU:T:2022:541

[531] ibid, para 610

[532] CMA, Case 50972 *Google Privacy Sandbox* Commitments (4 February 2022) paras 25-27.

[533] See for example, *Facebook case* (n 2); Furman Report (n 1); Cremer Report (n 1).

[534] 'Online Platforms and Digital Advertising Market Study' (n 1) 13; *Facebook case* (n 2); GDPR (n 57) article 6.

[535] Condorelli and Padilla (n 303).

[536] TFEU (n 5), article 102(a) provides as an example of abuse "directly or indirectly imposing [. . .] unfair trading conditions."

[537] Economides and Lianos (n 24) 816.

> "[L]imited choice and competition … 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. … [T]his means they have to provide more personal data to platforms than they would like."[538]

The 'take it or leave it' approach raises a question about the potential power imbalance and legitimacy of data processing.[539] Under the GDPR, consent for personal data processing needs to be given freely with an "unambiguous indication of the data subject's agreement to the processing of personal data…"[540] The interpretation of the 'freely' is broad, with the European guidelines suggesting that there has to be a genuine choice as whether to accept the terms or not.[541] In the scope of competition law, this thesis questions: (i) what provisions constitute an unfair contractual provision?;[542] and (ii) how to adequately capture privacy-related harms as unfair trading conditions?

Case law does not provide a clear definition of unfair trading conditions. The CJEU approach suggests that a contract of an 'inequitable nature' constitutes abuse, taking into account the combined and intrinsic individual effects of such clauses.[543] Alternatively, the CJEU finds that unfair practices should not be derived directly from the contract in question.[544] The Commission's definition of unfair trading conditions relates to practices that "materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed."[545] In other words, the CJEU assessed unfair trading practices as relying on a legalistic approach. If a contractual

---

[538] 'Online Platforms and Digital Advertising Market Study' (n 1) 8.

[539] GDPR (n 57) article 1(74); Cremer Report (n 1) 80.

[540] ibid, Recital 32.

[541] EDPB Consent Guidelines (n 61) 5.

[542] Economides and Lianos (n 24) 817.

[543] *BRT v SABAM* (n 428) para 12-13.

[544] *AAMS* (n 552) para 76; Case T-83/91 *Tetra Pak International SA v Commission* [1994] ECR II-755, para 140, which was upheld in *Tetra Pak II* (n 425).

[545] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), article 5(2).

clause was challenged as falling within unfair trading conditions outlined by the Court it was automatically deemed as unlawful. The CJEU has never evaluated how the unfair trading conditions imposed by a dominant company distort downstream competition among its customers. Equally, the Commission refers to the diminished added value for a weaker party involved in the contract, indicating an imbalance in power bargaining,[546] or restricted customers' use of its product without any valid reason.[547] In the BKartA's *Facebook case*, Article 102(a) TFEU was instrumental in finding consumers' weaker bargaining power.[548] By giving consumers the ability to make a choice, their preference for economic privacy might take preference over personalised experience, especially among consumers who place no value on personalised services. Also, in the *Epic Games* case, a legal action has been initiated wherein a group of consumers under Chapter II prohibition in §18 of the UK Competition Act 1998 against Apple for imposing exploitative terms and conditions on app developers, unfair prices on app distributed via the App Store, and removal of the Fortnite app from the App Store.[549] Equally, in the *Facebook* case, the CJEU also allowed for a consumer class action for infringement of personal data protection based on national law on unfair competition or consumer law, which included unfair terms and conditions.[550] Finally, the CJEU considered objective justifications for the imposition of unfair trading conditions. For example, in *United Brands,* the CJEU indicated that a dominant firm has the right to protect its commercial interests, but only in a proportional manner.[551] During the writing of this thesis, neither undertaking was successful rebutted the determination of abuse by presenting valid justifications.[552]

---

[546] Unfair Commercial Practices Directive (n 545) article 6(1).

[547] United Brands (n 195) paras 130–62.

[548] *Facebook case* (n 2)

[549] See Joined Cases 1377/5/7/20 and 1378/5/7/20, Epic Games Inc, Epic Games International SARL and Epic Games UK Ltd v Apple Inc and Apple (UK) Ltd; Epic Games Inc and Epic Games International SARL v Alphabet Inc, Google LLC, Google Ireland Ltd, Google Commerce Ltd, Google Payment Ltd (UK CAT, 22 February 2021, Roth LJ), paras 49 and 50 (b).

[550] See Case C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen and Verbraucherverbände – Verbraucherzentrale Bundesverband eV* (28 April 2022) ECLI:EU:C:2022:322, para 83.

[551] *United Brands* (n 195)

[552] Case T-139/98 *Amministrazione Autonoma dei Monopoli di Stato (AAMS) v Commission* ECLI:EU:T:2001:272, para 79.

(1) The German Facebook Case: an attempt to extend Article 102 TFEU

In essence, competition authorities have rarely used Article 102(a) TFEU to forbid unfair trading conditions.[553] The lack of enforcement in this area might be attributed to two factors. Firstly, unfair trading conditions might be prohibited under consumer law as unfair commercial practices.[554] Secondly, the CJEU has not established a comprehensive test akin to the *United Brands* test for evaluating unfair trading conditions.[555] However, such non-enforcing trend is currently shifting, particularly in the digital economy landscape. In the cases such as *Facebook case, Google Ads Rules*[556] and *Google News*[557], both BKartA and the Autorité de la Concurrence penalised several unfair training conditions imposed by large digital undertakings on their uses as abuses of dominant positions. Here, a discussion is provided considering B2C unfair commercial practices as a proxy to cover the exploration of personal data as an abuse of dominant position under Article 102 TFEU.

The BKartA's Facebook case is an interesting example of an attempt to conceptualise unfair commercial practices in a B2C approach in the context of possible privacy-related harms. The analysis of the BKartA fluctuated around the relation of competition law and data privacy law, acknowledging that Facebook's terms and conditions violated the GDPR's values.[558] The BKartA focused on Facebook's terms and conditions, examining if Facebook's data processing practices complied with the GDPR. In the assessment, the BKartA used §19(2) GWB to assess the abusive nature of Facebook's trading practices, taking a broad approach in defining the abusive trading conditions. By doing so, the BKartA applied the broader appropriateness clause, based its assessment on constitutional values,[559] and

---

[553] Botta (n 301) 110

[554] Unfair Commercial Practices Directive (n 545).

[555] *United Brands* (n 195). It is important to note that United Brands test is applicable to price-related abuses which are not the case for any privacy-related harms. I provide reference to this case to supplement the discussion.

[556] Autorité de la Concurrence Decision 19-D-26, 19 December 2019 (*Google Ads Rules*) < https://www.autoritedelaconcurrence.fr/en/decision/regarding-practices-implemented-sector-online-search-advertising-sector> accessed 16 April 2024.

[557] Autorité de la Concurrence Decision 21-D-17, 12 July 2021 (*Google News*) <https://www.autoritedelaconcurrence.fr/fr/decision/relative-aurespect-des-injonctions-prononcees-lencontre-de-google-dans-la-decision-ndeg> accessed 16 April 2024.

[558] *Facebook case* (n 2)

[559] ibid.

preserved the constitutionally protected right to commercial freedoms, which safeguard equal bargaining power.

The BKartA raised concerns regarding data aggregation practices, suggesting they could impede competition by creating barriers to entry and enhancing lock-in effect.[560] The data collected and processed by Facebook, both from its own services and third-party sources provided the company with extensive aggregate data, allowing for highly personalised services.[561] The BKartA analysed the infringement of GDPR though competition law tools and considered the legitimate interests of the parties involved, essentially third-party access to Facebook's advertising space and user data. The focus was on safeguarding citizens' rights to self-determination, with an emphasis on the non-price element of privacy and self-determination as protected by the GDPR and the German constitution. The BKartA did not provide guidelines on the 'loss of control' as a proxy for quality reduction. Essentially, this could be linked to the lack of price preference, which would require an analysis of substitutability between informational self-determination and its violation. This implies that the BKartA avoided explaining why users had not switched to different service providers if privacy, or informational self-determination, was a proxy for quality reduction. Potentially, the BKartA omitted such an analysis as it would require balancing informational self-determination with substitutability between social networks, and the BKartA lacked the methodological tools to analyse that aspect. Instead, the analysis focused on the theory of harm relating to data protection law infringement.

The BKartA deduced that GDPR principles were infringed due to a gross imbalance between Facebook's interest and the protection of users' fundamental rights. To assess if Facebook abused its dominant position, the BKartA focused on whether infringement of the GDPR also triggered the application of relevant competition law provision.[562] There are two potential justifications for this assessment. Firstly, the BKartA focused on establishing a causal link between unfair trading conditions taking the form of unlawful and exploitative data processing and Facebook's market power. Secondly, the assessment focused on balancing competition law interests.

---

[560] *Facebook case* (n 2).

[561] ibid.

[562] ibid, GWB (n 119) Section 19(1).

Firstly, the BKartA adopted a flexible approach to discussing the causal link:

> "[T]he required link with market power is, therefore, not to be construed within the meaning of a strict causality of market power, requiring proof that data processing conditions could be formulated in such a way precisely and solely because of market power."[563]

Consequently, the BKartA considered causality from a normative outlook. Causality is assessed in relation to the conduct rather than a strict causality to determine a significant causal factor where a strict counterfactual test is applied.[564] However, this does not suggest that the BKartA merged competition together with data protection law at this stage, as it remains difficult to see practically how competition law and data protection could refer to different problems. According to Lianos and Economides, the flexible approach to causality suggested difficulties as to how competition law and data protection might interact with each other.[565] The case was decided as an issue for both competition and data protection law, suggesting an apparent correlation between data protection violations and Facebook's market power.

Secondly, the assessment considered balancing various interests with competition law. At this stage, the BKartA held that Facebook's terms and conditions were abusive due to Facebook's market power. This established an anticompetitive effects presumption, indicating that in certain instances of data protection violation, there might be a causal link between the conduct and market power. Essentially, the BKartA's need for independent balancing under competition law might be challenged by German case law, as emphasised by the Federal Court of Justice: "if an infringement (of data protection law) is the result of market power… the abusiveness can no longer be called into question by a further (competition) balancing of interests."[566] I assume that the BKartA's approach could vaguely indicate that the BKartA tried, through the presumption of illegality under competition law, to provide there was apparent evidence of causality between infringement of competition law and infringement of data protection law. In order words, there was a connection

[563] Zuboff (n 48) 873.

[564] *Post Danmark* (n 277).

[565] Economides and Lianos (n 24) 761.

[566] Zuboff (n 48) 891.

between privacy-harming conduct and abuse of market position. The latter would not have been possible without finding infringement of data protection law. On this point, Lianos and Economides argued that the BKartA balanced elements of competition law and data protection law, and how such an assessment might lead to identical outcomes.[567]

On the same note, Monti suggested that the balancing activity needs to be taken between competition law and non-competition policy considerations.[568] In the *Meca-Medina* case, the CJEU considered rules dealing with doping in sports that allegedly breached Articles 101 and 102 TFEU.[569] While conducting an assessment, the CJEU did not focus on the consideration that it was a regulated activity.[570] Instead, the CJEU focused on the agreement's objectives. In other words, the CJEU took into consideration the overall context in which the rules were adopted, and its corresponding effect on competition law. Similarly, the environmental protection considerations could be possibly applied in the broader economic and legal context of an anticompetitive investigation. For example, in *CECED,* the Commission considered the agreement among the washing machines manufactured as not energy efficient.[571] The Commission's decision gave protection of environment as significant in the balancing process, demonstrating that agreements harming environment also might introduce negative effects on Article 101 TFEU infringements. Similarly, in the 'Chicken of Tomorrow', discussed in section 2.3.1, the assessment demonstrated that the sustainable initiative had possible exploitative features of unfair trading conditions. In fact, acknowledging external to competition law policies as finding a competitive abuse is plausible; the CJEU has considered the influence of non-economic and economic goals in balancing Article 102 TFEU infringement.[572] The balancing activity involves an evaluation of the extent to which two competing interests can be harmonised. Only if these criteria are met is there an attempt to strike a balance, though this balance primarily focuses on the fairness of the harm experienced by the party at a disadvantage when compared to the benefits derived from the action or practice. In essence, the question being asked is whether

[567] Economides and Lianos (n 24) 761.

[568] Giorgio Monti, 'Balancing in Competition Law" (2022) TILEC Discussion Paper No. DP2022-007.

[569] Case T-313/02 *David Meca Medina and Igor Majcen v Commission* ECLI:EU:T:2004:282

[570] ibid, paras 42, 43 and 47.

[571] *CECED* (n 125) para. 47–57.

[572] See I Lianos, 'Polycentric Competition Law' [2018] Current Legal Problems 161.

the harm suffered by the disadvantaged party is reasonable given the advantages gained from the activity.

During the *Facebook case* saga, AG Rantos Opinion provided some clarity on the intersection between competition law and privacy-relating harms. The opinion concluded that the BKartA did not emphasise the breach of the relevant data protection laws by Facebook. Instead, the BKartA analysed the alleged abuse of Facebook's dominant position, through consideration of Facebook's non-compliance with the GDPR provisions.[573] In the terms of Opinion, the BKartA:

> "did not penalise a breach of the GDPR by Meta Platforms, but proceeded, for the sole purpose of applying competition rules, to review an alleged abuse of its dominant position while taking account, inter alia, of that undertaking's non-compliance with the provisions of the GDPR."[574]

In AG Rantos' view, the BKartA's application of the GDPR in the competition law assessment was incidental,[575] as finding the privacy-breach was not in the interest of the BKartA. In fact, it emphasised that the GDPR breach on its own cannot be seen as unlawful under Article 102 TFEU. Instead, an incidental consideration of privacy-related harms could guide the assessment of data-related anticompetitive harms. In order words, the GDPR could be balanced within a broader manner of the legal and economic context and other relevant circumstances of the case, to establish whether the conduct harmed competition on the relevant market.[576]

AG Rantos considered users' consent to have their data combined from Facebook and off-Facebook services, while balancing GDPR and competition law rules.[577] Consumers create their digital selves with limited knowledge of the offered terms and conditions.[578] An impaired understanding of terms and conditions results in users having little confidence in detecting any unfair or discriminatory conduct. Data collection occurs on a 'no question

---

[573] *Facebook case* (n 2) 5-7.

[574] ibid, para. 18.

[575] *Meta Platforms, Opinion of AG Rantos* (n 85) para 24.

[576] See chapter 3 for more details, sections 3.4.2-3.4.3.

[577] *Meta Platforms, Opinion of AG Rantos* (n 85) para 77.

[578] 'Online Platforms and Digital Advertising Market Study' (n 1) 8.

asked'[579] basis. Individuals face the choice of either accepting the terms and conditions of an online service or not using it at all. Relying on the *DSD* case, one may claim that users should have an option of either creating their social network profile, using online search platforms or accepting the significant tracking practices of a dominant service provider.[580] In the light of Article 102(a) TFEU, the BKartA's theory of harm may be demonstrated as follows: Facebook's dominance is a prerequisite for demonstrating that Facebook users could not exercise their preferences for privacy before joining Facebook. Such lack of control allows for users' exploitation, resulting in abuse of Facebook's dominance. The fact that Facebook imposed unfair terms and conditions resulted not only from its position on the market but also users' attitudes towards privacy. However, their tendency to not read terms and conditions does not relate to their laziness, but to an inability to understand terms and conditions content, and lack of choices to protect their data. Particularly, the lack of privacy choices is designed to further exploit consumer biases.[581]

AG Rantos confirmed that Facebook's users did not freely consent to using Facebook, bearing in mind the applicable data protection provisions. AG Rantos challenged BKartA's decision by emphasising the significance of opt-in and lock-in of users in determining the validity of users' consent. According to Recital 42 of the GDPR, the users' consent should not be regarded as given freely if users had no reasonable choice or could not withdraw consent without detriment. For example, in *Orange Romania,* the CJEU clarified that the users' consent appears to be more stringent, requiring a 'freely given, specific, informed and unambiguous' indication of users' desire for data collecting and processing activities.[582] The validity of users' consent, consequently, appears to be assessed on a case-by-case basis. The presence or absence of dominance can be considered when assessing whether users of a social network have granted their consent freely. Similar to his previous argument on the relationship between GDPR and competition law, AG Rantos highlighted that the absence of a dominant position did not guarantee free and effective consent.

---

[579] Economides and Lianos (n 24) 772.

[580] *DSD* (n 186) para 112. *DSD* was upheld on appeal, see Case T-151/01 *Duales System Deutschland* EU:T:2007:154.

[581] CMA 'Algorithms' (n 308).

[582] Case C-61/19, *Orange Romania* EU:C:2020:901, paras 35-36.

The CJEU's judgment mirrors remarks offered by AG Rantos, yet it draws back from the key point of the debate — defining the scope of applying data protection law in the antitrust framework. The CJEU clarified that Facebook's business model and online advertising practices rely on the automated creation of network users' profiles and the Meta group's online services. These profiles are produced on a technical level, allowing the functioning of their operations.[583] For this initial statement, the CJEU appears to believe that Facebook's exploitation of user data is primarily possible by technical limitations rather than economic and strategic choices of Facebook. In other words, the CJEU attributes Facebook's reliance on personal data to be a consequence of technical necessity rather than its intentional decision.

The CJEU's approach in bringing forward and acknowledging the tension between competition law and data protection law requires elaboration. In the view of the CJEU, Facebook has been incapable of diverting its business model in any alternative way to ensure compliance with the law. In other words, Facebook might have no feasible options to change its operating services to meet legal requirements beyond its current approach.[584] In its assessment, the CJEU emphasised that the BKartA's comprehensive analysis of the GDPR was not an instance of an unauthorised data protection regulation interpretation. Instead, the BKartA examined each of the requirements individually to determine if Facebook's data collecting and processing activities were consistent with the GDPR's obligations and whether any competition law breach had occurred. Both GDPR and Article 102 TFEU do not preclude such interaction from unravelling: it is not contrary to EU law to ascertain that the GDPR does not conflict when a national competition authority assesses its provisions within the antitrust framework. In fact, such findings should not be found as a surprise, since in line with previous case law, the conformity of conduct with specific legislation does not automatically exempt that conduct from being subject to Article 102 TFEU.[585]

The CJEU has not elaborated directly on the nature of unfair trading conditions offered by Facebook. Instead, the CJEU offered a narrow interpretation of GDPR within the wider

---

[583] ibid, para 27.

[584] Meta, 'How Meta Uses Legal Bases for Processing Ads in the EU' (2023) < https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/> accessed 1 September 2023.

[585] *AstraZeneca* (n 99) para 132.

context of GDPR and extended it to recognise that data collecting and processing activities are significant in the context of the digital economy. The latter is particularly seen as important for digital platforms' business models which revenues from personalised advertising. In this respect, the CJEU's argument goes in the following direction: the access to personal data and the ability of digital platforms to process that data, particularly when collected and linked into large datasets, can be seen as a competitive parameter in the digital economy. Ignoring this aspect would disregard the realities of digital economic advancements and could undermine the effectiveness of competition law altogether. Recognising the importance of data as a key factor in the digital market is essential for fostering fair competition and ensuring that competition law remains relevant and applicable in the evolving digital landscape.[586]

Yet, this argument brings nothing new to EU competition law, as the Commission has already recognised privacy as a parameter of competition in *Facebook/WhatsApp* and *Microsoft/ LinkedIn* mergers,[587] Arguably, in both merger proceedings, the Commission recognised that data privacy might serve as an element of competition parameter, as data privacy was valued by digital users. In the *Facebook case*, the CJEU avoided taking a normative approach that that favours privacy-enhancing business models (where more privacy is considered better for consumers), by characterising access to and the ability to process personal data as a competitive parameter. However, the CJEU recognised that the extent of access and data processing capabilities is pertinent to the competitive dynamics, separate from their implications concerning the GDPR applicability. Correspondingly, the CJEU highlighted the importance of considering data-related factors in the antitrust assessment without solely focusing on privacy concerns. The CJEU's argument suggests that a digital platform's activities can be crucial when assessing a platform's departure from normal competition. However, this consideration could not hold the same weight when it comes to determining dominance under the GDPR.[588]

---

[586] *Meta Platforms* (n 41) para 50–51

[587] *Facebook/WhatsApp* (n 90); *Microsoft/LinkedIn* (n 90). EU Commission, 'Review of the Commission Notice on the definition of relevant market for the purposes of Community competition law' (2022) < https://competition-policy.ec.europa.eu/public-consultations/2022-market-definition-notice_en> accessed 15 August 2023; para 12, where privacy has been assigned as an aspect of quality.

[588] Consequently, the CJEU ascertained, in the line of AG Rantos' Opinion, that a dominant position might be an important factor in determining if users' consent can be grated freely. *Meta Platforms* (n 41) para 151

In line with this reasoning, one shall consider if Facebook's processing activities may be a manifestation of unfair trading conditions as per Article 102(a) TFEU. The decision made by the BKartA regarding Facebook is grounded in §19 of the German Competition Act, which working is almost identical to Article 102 TFEU. The imposition of unfair trading conditions for the use of digital platforms has an influence on intra-community trade and should have been assessed under Article 102 TFEU.[589] However, this section focuses on the assessment of privacy-related unfair trading conditions and will apply Article 102 TFEU.

The CJEU sanctioned under Article 102(a) TFEU several contractual clauses imposed by dominant undertakings on their consumers. In *United Brands*, it was seen as unfair that United Brands' distributors could not send unripened bananas.[590] Also, in *Porto di Genova*, the CJEU considered unfair that the maritime companies were required to rely on the services of a firm applied by Genoa seaport, rather than being able to freely choose their own provider.[591] Generally, there are different ways to classify a contractual clause as unfair. In *SABAM,* the Court considered a clause as unfair whereby artists were requirement to transfer the management of their copyright works to SABAM once the contract was ended.[592] Particularly, the CJEU held that SABAM breached Article 102(a) TFEU by:

> "imposing 'on its members obligations which are not absolutely necessary for the attainment of its object and which thus encroach unfairly upon a member's freedom to exercise his copyright."[593]

Furthermore, in *GEMA II,* the Commission specified that the crucial aspect to consider is whether the requirements go beyond what is necessary for the effective safeguarding of intellectual property law (indispensability test) and whether they can restrict the copyright holder's control over their work only to the extent necessary (equity).[594] The Commission emphasised the importance of necessity in *Tetra Pak II*, where the CJEU concluded that the

---

[589] Regulation 1/2003 (n 54) art 3(1); see section 3.2 in chapter 3.

[590] *United Brands* (n 195) paras 130–162

[591] *Porto di Genova* (n 521) paras 8–24.

[592] *BRT v SABAM* (n 428)

[593] ibid, para. 15.

[594] *GEMA II* (n 527) para 36.

obligations in question: "have no connection with the purpose of the contract and … deprive the purchaser of certain aspects of his property rights."[595] Also, in *DSD*, the Commission decided that contract conditions were unfair because they failed to comply with the notion of proportionality: it refers to a fair balance between the price and the economic value of the service, ensuring that the two are in proportion.[596] In this respect, terms of conditions may be deemed as unfair under Article 102(a) TFEU, providing they are: (i) unnecessary to achieve the objective of a contract; (ii) the contract obligations may contribute to achieving this object; (iii) they are no alternative methods that are less harmful or abusive to achieve the intended goal; (iv) the legitimate objective object ought to outweigh the exploitative effect.[597]

The assessment of unfair trading conditions relating to non-price harms has been clarified by French NCAs. The Autorité de la Concurrence made two significant rulings penalising Google under Article 102(a) TFEU for imposing unfair trading conditions on advertisers.[598] Both of the cases are landmark decisions since they sanctioned unfair trading conditions under Article 102(a) TFEU in the context of the digital economy.

According to the Autorité de la Concurrence, a dominant undertaking could impose unfair trading conditions if it a company possesses exceptionally large market shares, its products essentially constitute the entirety (or nearly so) of what the market provides.[599] Hence, consumers seeking these products have little option but to agree to the terms dictated by the dominant company, even if they are unfair.[600] In this respect, the company needs to be 'an unavoidable trading partner' for the consumers.[601] In that case, the French NCA considered unfair trading conditions under Article 102(a) TFEU, since Google's conduct was

---

[595] *Tetra Pak II* (n 425) para 107.

[596] *DSD* (n 186).

[597] O'Donoghue and Padilla (n 243) 856.

[598] Autorité de la Concurrence, 'The Autorité de la Concurrence Hands Down a €150M Fine for Abuse of a Dominant Position' (Press release, 2019) <https://www.autoritedelaconcurrence.fr/en/press -release/autorite-de-la-/concurrence-hands-down-eu150m-fine-abuse-dominant-position> accessed 17 April 2024; *Google Ads Rules* (n 556); *Google News* (n 557)

[599] *Google Ads Rules* (n 556); *Google News* (n 557)

[600] ibid.

[601] Botta (n 301) 113; *Google Ads Rules* (n 556); *Google News* (n 577)

beyond its ostensible purpose and allowed to strengthen the company's dominant position by making consumers economically dependent on the product or service provided.[602] In *Google Ads Rules,* Google was seen as being an unavoidable partner for digital advertisers and unilaterally imposed the rules on the digital advertisers.[603] In other words, the digital advertisers had no choice but to accept the Rules because of their dependence on Google. Also, several clauses were seen as unfair, due to their uncertainty and constant modifications by Google.[604] The French NCA evaluated the possible adverse effects on competition of the rules: they heightened uncertainty for advertisers and disrupted competition among websites that sell digital services.[605]

Contrary to the *Facebook* case, the French approach referred to the CJEU case law and clarified the existing jurisprudence on Article 102(a) TFEU, by discussing the concepts of unavoidable trading partner and unfair trading conditions. The decision was later upheld by the Paris Court of Appeal in 2022. The judgement indicated that Google's dominant position in the digital advertising market emphasised a unique obligation to avoid distorting competition within that market.[606] According to the Paris Court of Appeal, Google's rules were applied in a "… non-objective, non-transparent and discriminatory way…"[607] by blocking several websites that did not comply with the rules, correspondingly limiting the choice of websites available to consumer users.[608]

Moreover, the French NCA applied Article 102(a) TFEU in the *Google News* case, where Google imposed unfair trading conditions on press agencies and publishers by decrying to negotiate and compensate for featuring copyrighted press content on its existing

[602] *Google Ads Rules* (n 556) para 370.

[603] ibid, 431

[604] ibid, 108

[605] ibid, 439–66.

[606] Paris Court of Appeal, 20/03811 Google (7 April 2022), para. 151.

[607] ibid, para. 249.

[608] ibid.

platforms.[609] The case began after the enactment of Article 15 of the EU Copyright Directive into French Law 2019/775.[610] Under the French legislation, online websites were required to acquire a licence from press publishers to present newspaper articles. Google services, including Google Search or Google News, displayed "snippets," which were brief excerpts from newspaper articles.[611] As a result of the French Law 2019/775, Google asked French press publishers for a free licence and it ceased displaying article snippets from newspapers that refused to provide a complimentary licence to Google.[612] As a result, several newspapers were affected by the ban, noting a reduced number of visitors to their websites and decreased revenue from online advertising.[613] The Autorité de la Concurrence followed similar analysis as in the *Google Ads Rules case,* concluding that Google was an unavoidable trading partner.[614] In other words, French publishers had no choice but to agree to a free license agreement, as refusing it would result in a significant decrease in their visibility and advertising revenues. Also, a requirement of a "free" licence was seen as unfair as it contradicted the intention of the Copyright Directive, which aimed to ensure fair compensation for publishers instead.[615] Lastly, Google failed to provide any objective justification for its actions:[616] there were potential anticompetitive ramifications, a newspapers excluded by Google were put at a competitive disadvantage compared to those that agreed to a free licensing arrangement with Google.[617] The French NCA penalised Google for its anticompetitive conduct of unfair trading conditions and discriminatory

---

[609] Autorité de la Concurrence, 'Droits Voisins: L'Autorité Fait Droit aux Demandes de Mesures Conservatoires Présentées par les Éditeurs de Presse et l'AFP' (Press Release, 2020) <https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/droits-voisins-lautorite-fait-droit-aux-demandes-de-mesures-conservatoires> accessed 17 April 2024.

[610] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/ EC, [2019] OJ L-130/92; Law 2019-775 tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse, 24 July 2019, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038821358> accessed 18 April 2024. Botta (n 301) 114.

[611] *Google News* (n 557) para 44.

[612] ibid, paras 90–95.

[613] ibid, paras 121–123.

[614] ibid, para 200.

[615] ibid, paras 203–208.

[616] ibid, paras 255–264.

[617] ibid, paras 218–33.

treatment in line with the framework set by the *Google Ads Rules* case, emphasising the nature of unavoidable trading partners imposing unfair trading conditions that 'went beyond their ostensible purpose and were intended to strengthen (the firm) dominant position by reinforcing its customers' economic dependence on it'.[618] As a result, Google issued a set of commitments, which include Google's desire to engage in *bona fide* negotiations with press publishers and news agencies.[619] Such negotiations will adhere to transparent, objective, and non-discriminatory criteria. In addition, Google ensured that the negotiation process did not impact on the presentation of content, nor did it affect any other economic relationship between Google, press publishers and news agencies.

Despite the limited case law on unfair trading conditions, the legal tests discussed fits features of privacy-related harms. Competition law has a flexible tool set to assess market power and dominance in cases involving digital companies.[620] While assessing Facebook's processing activities, the CJEU held that the BKartA was right to consider Facebook's activities as infringing the GDPR and exploiting its users. Firstly, the CJEU established that collecting and processing data off-Facebook was prohibited under Article 9(2) GDPR, due to lack of freely given users' consent and knowledge. Also, the CJEU directly addressed Facebook's grounds for processing users' personal data, as per Article 6 GDPR. In essence, Facebook's dominant position does not inherently invalidate users' ability to provide valid consent.[621]

Indeed, the CJEU considered that the access and processing of personal data is a competitive parameter. However, the CJEU does not designate it as a universal goal, standard, or indicator applicable to all aspects of EU competition law. Instead, it recognises data-related factors as relevant for assessing competition in the digital economy without mandating their application as a definitive measure across all cases falling under EU competition law. The

[618] G*oogle News* (n 557) para 370.

[619] Autorité de la Concurrence, 'Related rights: The Autorité accepts Google's commitments' (Press release, 2022) <https://www.autoritedelaconcurrence.fr/en/press-release/related-rights-autorite-accepts-googles-commitments> accessed 20 April 2024.

[620] Hedvig Schmidt, 'Taming the Shrew: There's no need for a new Market Power Definition for the Digital Economy' (2017) Stockholm Faculty of Law Research Paper Series No 1, 17.

[621] In this regard, the Court of Justice's findings do not differ much from the Irish Data Protection Commission's decisions against Meta for its processing of personal data, even though the Court of Justice brings forward a valuable argument as a counterfactual of sorts to Meta's current business model.

Court's approach is more context-specific, considering the significance of data access and processing in the digital market without imposing a one-size-fits-all approach in EU competition law. Privacy protection can only impact competition law when privacy is a key parameter of competition and is not the case for consumer communication apps where price, user base, popularity or reliability are important factors. I argue that it is important to not lose sight of the fundamental principle that what is relevant in a competition assessment involving privacy concerns are market-driven privacy standards. I submit that when a digital platform provider requires mandatory acceptance of terms of use of personal data for the purpose to use that online service, and/or contain misleading terms that give consumers a false perception of control over their data, then this could be seen as an unfair trading condition abuse under Article 102 TFEU. The lack of optionality arising from power imbalances between consumers and online service/product providers appears both in an exploitative abuse and privacy context, as can be argued in line with the French NCAs cases. If a person only has the option to choose one service/product provider in the digital market, then they are inevitably in a weak position to negotiate for a better quality of privacy, especially since Facebook can be deemed as being an unavoidable trading partner.[622] If that online service provider has market power, then this is unquestionably also a problem for competition law enforcement. The exploitative nature of abuse stems from the fact that a dominant online platform could not impose these terms under competitive conditions. Consumers are left with no choice but to consent to them, contrary to their privacy preferences. Such assessment will be based on case-by-case considerations, as previously demonstrated by the CJEU practice.

(2) Alternative approach for privacy protection

Both Google and Apple have taken actions to readjust their service policies towards ensuring increased consumer privacy.[623] Such products 'upgrade' could affect third parties' ability to track online users and perform adverting. The strengthening of the dominance of Apple and Google can create opportunities for potential exploitation of consumers as well as exclude

[622] *Google Ads Rules* (n 556); *Google News* (n 557)

[623] Antony Ha, 'Apple defends new ad-tracking prevention measures in Safari' (*TechCrunch*, 16 September 2017) <https://techcrunch.com/2017/09/15/apple-defends-new-ad-tracking-prevention-measures-in- safari/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACJHEOUzBdbgOV96MDbycf1YZwUlAxpibSRBek4odBvKQh-LxcYDj77NF3LpeHFch9JvM-cJbagU6HEDj9FwVzQazq8ZWvOu0EnlkKRfzUQeL9F5vXBEYoGbdIgrbWrCISsNMD67PX9PJAKtp9zkfqVAMGRkbcphVvYi8SO3V9OY> accessed 6 November 2022.

competitors. For example, Google's choice to eliminate support for third-party cookies could raise concerns about leveraging, possibly distorting competition among publishers, and/or ad tech vendors to Google's benefit.[624] It is worth noting that the assessment of privacy policies introduced by these companies may involve considerations of unfair trading conditions, even though the discussion of specific cases should be approached hypothetically given the focus on exclusionary rather than exploitative abuses by competition authorities in Europe.[625]

Both Google's Privacy Sandbox and Apple's ATT initiatives are broadly related to online advertising. To start with, Apple's ATT empowered users to decide if they consented to having their activities tracked by third-party apps.[626] The significant innovation introduced by Apple's ATT was the choice to set the default preference for cross-app collection as "opted-in/out".[627] It represented a change, as the previous iOS version only allowed to navigate through multiple settings on their devices to locate and disable cross-app tracking. In essence, Apple aimed to give users more control over their privacy by simplifying the process of opting-in for cross-app tracking. Although this pro-privacy change might be positive for the users, as Apple could be effective in addressing the market's informational asymmetry,[628] the ATT incentive carried exploitative concerns. In France, the Autorité de la Concurrence opened an investigation against Apple on the allegation of self-preferencing, as

---

[624] Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, 'Google as a de facto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective' [2021] European Competition Journal 617.

[625] For example: Bundeskartellamt, 'Bundeskartellamt reviews Apple's tracking rules for third-party apps' (14 June 2022) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemittei- lungen/2022/14_06_2022_Apple.html?nn=3591568> accessed 15 April 2024; Benjamin Seufert, 'ATT advantages Apple's ad network. Here's how to fix that.' (MobileDevMemo, 1 November 2021) <https://mobiledevmemo.com/att-advantages-apples-ad-network-heres-how-to-fix- that/> accessed 15 April 2024; Dimitrios Katsifis, 'CMA opens investigation into Google's Privacy Sandbox browser changes' (The Platform Law Blog, 8 January 2021) <https://theplatformlaw.blog/2021/01/08/cma-opens-investigation-into- googles-privacy-sandbox-browser-changes/> accessed 15 April 2024; CMA, 'CMA to investigate Google's Privacy Sandbox browser changes' (Competition and Markets Authority Press Release, 8 January 2021) <https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes> accessed 15 April 2023.

[626] Ha (n 624).

[627] 'What Is App Tracking Transparency (ATT) and How Does It Affect Mobile Marketing?' (Vungle Blog, 26 May 2021) <https://vungle.com/blog/app-tracking-transparency-att/> accessed 15 April 2023.

[628]While figures may differ, around 85% of users opt out of allowing apps to track their activities across other apps. Alex Bauer, 'ATT opt-in rates: the picture so far and the ugly truth behind why the numbers vary so widely' (AdExchanger, 10 May 2021) <https://www.adexchanger.com/data-driven-thinking/att-opt-in- rates-the-picture-so-far-and-the-ugly-truth-behind-why-the-numbers-vary-so-widely/> accessed 15 April 2024.

the ATT did not apply to Apple's advertising business.[629] It was also suggested that Apple could advantage its own ad networks, as Apple's ad revenues increased after the ATT introduction.[630] In Germany, several publishers filed a complaint with the BKartA, alleging that Apple's action could amount to abuse of dominance by excluding competition in online advertising.[631] Also, in Poland, Apple's ATT substantially diminished the capacity of third-party apps to acquire personal data on iOS for purposes of personalised advertising.[632] Broadly, as the ATT elevates the value of first-part data, collected directly from the business rather than through cookies from other apps or websites, concerns arise about the internet evolving into a landscape of "content fortresses" or "walled-gardens," marked by heightened levels of concentration and consolidation.[633]

Secondly, the Google Privacy Sandbox interface is largely in alignment with those introduced by Apple. Google aimed to eliminate third-party cookies on its browser, Chrome. Cookies allow websites to track users (with their consent) across the web, enabling the construction of detailed consumer profiles online. Cookies, in this respect, serve as the foundation of the existing online targeted advertising industry. CMA found that Google and Facebook are digital advertising 'duopolists', capturing more than half of global ad spending.[634] Possessing large quantities of data is insufficient. Indeed, without the post-ad exposure action of users, and the interests or demographics of users, any targeting is limited. To capture data as positive and meaningful, it needs to be associated with a user through identifiers such as

---

[629] Alex Barker, 'Apple hit with antitrust complaint in France over privacy controls' (Financial Times, 28 October 2020).

[630] Seufert (n 625).

[631] 'Bundeskartellamt reviews Apple's tracking rules for third-party apps' (n 625).

[632] Natasha Lomas, 'Poland latest to probe Apple's app tracking transparency shift — over self-preferencing concerns' (TechCrunch, 2021) <https://techcrunch.com/2021/12/13/poland-apple-att-antitrust-probe/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJ09573B8vwb9twnmtMW09yenxqHPZzv1e8gUlfM1eU3955osVuhlg_RILhrFz5A1Qp-1Xq1nVvaR0DdxAEqLg9zN_9m1Spes9o1cWVSeRZepl9BY9hebZb9kfKZF9gfhpoLA7Dh_dU3dG0-Yl9YrVoUUfd8maxZczFNbqzwfc6S> accessed 2 May 2024.

[633] Eric Benjamin Seufert, 'The profound, unintended consequence of ATT: content fortresses' (MobileDevMemo, 15 February 2021) <https://mobiledevmemo.com/the-profound-unintended-conse- quence-of-att-content-fortresses/> accessed 26 July 2022.

[634] 'Online Platforms and Digital Advertising Market Study' (n 1) appendix F, para 64.

cookie IDs or users' IP addresses.[635] Users' identity is a cornerstone of online advertising,[636] and without this identification, digital advertising cannot be performed.[637] For instance, Facebook requires its users to register and consent to its ambitious terms and conditions by merely providing their name, gender, date of birth and email address.[638] Users joining Facebook are assigned a unique Facebook ID connected to their profile.[639] In addition, Facebook can gather generated user data from third-party sources, with the integrated Facebook interface. Google's model works within a similar alignment, allocating internal Google ID to its users, and collecting and combining information from numerous consumer-facing services.

The advancement in advertising technology to phrase out cookies is welcomed from the perspective of privacy-oriented users, as reduced cross-website tracking is generally perceived favourably in terms of privacy.[640] Yet, the removal of the cookies could disrupt the revenue treated of the vast majority of the modern internet, introducing significant implications. The CMA decided to investigate this incentive, due to several concerns about its impact, which included the ability of publishers to generate revenue and undermine competition in digital advertising.[641] The Commission also pursued its investigation.[642]

---

[635] 'Online Platforms and Digital Advertising Market Study' (n 1) appendix G, para 16.

[636] Ha (n 624).

[637] Sam Dutton, 'Digging into the Privacy Sandbox' web.dev (8 April 2020) <https://web.dev/digging-into- the-privacy-sandbox/>. Accessed 17 October 2022; Bauer (n 628).

[638] 'Online Platforms and Digital Advertising Market Study' (n 1) appendix F, 3

[639] ibid, 10.

[640] P Akman, 'A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets' [2022] Virginia Law & Business Review 1.

[641] Erin Thomson, 'Will the DMA trigger competition in the Digital Advertising Market?' (2022) 34 Competition Forum; Dimitrios Katsifis, 'How tech platforms act as private regulators of privacy' (The Platform Law Blog, 26 October 2020) <https://theplatformlaw.blog/2020/10/26/how-tech-platforms-act-as-pri-vate-regulators-of-privacy/> accessed 10 March 2024.

[642] European Commission, 'Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector' (Press Release, 2021) <https://ec.eu- ropa.eu/commission/presscorner/detail/en/ip_21_3143> accessed 30 March 2024.

The CMA identified that Google's proposal could amount to an abuse of a dominant position if it was implemented without regulatory scrutiny.[643] The CMA followed the approach that Google Privacy Sandbox could amount to anticompetitive leveraging of its market power in the browser market to the market of online display advertising. Privacy Sandbox's impact was attributed by the CMA to two factors: (a) an information imbalance between Google and third parties concerning the development of the Privacy Sandbox proposals, particularly regarding the criteria Google will use to assess the effectiveness of various solutions, and (b) a lack of confidence among third parties in Google's intentions, given that Google's commercial interests may not necessarily align with the success of the proposals.

To start with, the CMA considered the impact of the Privacy Sandbox. On this assessment, the CMA focused on three anticompetitive concerns. Firstly, the CMA assessed unequal access to the functionality associated with tracking of users. The CMA was concerned that Google Privacy Sandbox could limit the functionality available to its rival in display advertising (both rival ad tech providers and publishers) while allowing Google to offer such functionalities unaffected. As most websites and apps are sustained by advertisements (which made them "free" for users), eliminating the means of monetarisation could lead to a subscription-dominated internet, where consumers have to pay to access content. On the other hand, third-party websites, which are not dependent on Google, could find themselves compelled to engage with it to sustain their ad-supported business models. Given Google's access to extensive first-party data from Google-owned substitutes, like Gmail and Google Maps, it stands to become a valuable source for personalised advertising. As identified by the CMA, there was a possibility of potential self-preferencing of Google's advertising products and an increased collection of users' data for its products and services.[644]

---

[643] CMA, 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (CMA, 2022) < https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf> accessed 2 August 2023. (Hereinafter: CMA: 'Decision to accept commitments offered by Google') The investigation was launched under Chapter II of the Competition Act 1998, which is the UK equivalent of Article 102 TFEU.

[644] CMA, Case 50972 - Privacy Sandbox Google Commitments Offer (2022) <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf> accessed 1 August 2023.

Secondly, the CMA considered Google's preferential treatment of its own ad technology and its own operated ads. As Chrome sets to play a pivotal role in selecting acts that are displayed to users under Privacy Sandbox,[645] the CMA demonstrated a possible conflict of interests. Google enjoyed a dual role as both a dominant player in the ad tech market, as well as a publisher selling ads. In this respect, there is a risk that Privacy Sandbox could be exploited to prioritise Google's own ad inventory and ad tech services. This might include limiting interoperability with competitors or influencing the decision-making process to favour Google's offerings.

Based on Article 102 TFEU, Google's conduct might be viewed as a type of self-preferencing, similar to the Commission's decision in the *Google (Shopping) case.* In that case, Google was found to abused its dominant position in the general search services market to favour its comparison shopping services.[646] This conduct was deemed as stifling competition and lacked objective justification. In the Google Privacy Sandbox scenario, Google might leverage its dominant position in one market, including the browser market, to expand its influence into an adjacent market, such as online display advertising. Such expansion would occur through methods distorting competition on merit and might potentially limit competition in the affected market. With the enactment of Google Privacy Sandbox, Google's treatment of Chrome as a first-party entity, akin to the user's primary destination on the web, grants it a distinct advantage in tracking users across online platforms without relying on cookies.[647] This advantage makes it virtually impossible for other publishers to replicate data unless it were possible to access the browser market and introduce similar features. According to Geradin, this concept was highly unlikely.[648] Even if one assumes that Google's position in the user-facing markets, such as search engines, was a result of fair competition rather than anti-competitive behaviour, it is crucial to recognise that Google's policy change introduced competitive concerns. Google's access to vast amounts of high-quality first-party data far surpasses that of any individual publisher operating within the open web. Failing to

---

[645] Dina Srinivasan, 'Why Google Dominates Advertising Markets' (2020, SSRN) < https://ssrn.com/abstract=3500919> accessed 27 April 2024.

[646] *Google Search (Shopping)* (n 192) paras 593. 649 and 653.

[647]Geradin, Katsifis and Karanikioti (n 624).

[648] ibid.

acknowledge such concerns could overlook the fact that Google's action effectively curtain rivals' ability to enhance their advertising offerings and compete for ad revenue.

Additionally, Google's policy change could impact competition amongst ad tech vendors. Google has held a prominent position, possibly dominant, in providing ad tech tools throughout the value chain.[649] To understand concerns raised by the Google Privacy Sandbox incentive, one has to remember Google's past self-preferencing behaviour in the ad tech ecosystem.[650] The CMA's report on online platforms and digital advertising pointed to various leveraging tactics within the ad tech ecosystem.[651] The CMA found that Google utilised its dominance in search to establish itself as a demand-side platform leveraging its extensive data and advertiser base.[652] Also, Google was found to leverage its market power across different levels of the value chain, potentially creating barriers for publishers to switch to alternative ad servers and reducing competition.[653] Google increased "the barriers publishers face in switching from Google to a different ad server, reducing competition in ad serving."[654] The CMA, while investigating the Privacy Sandbox incentive, has emphasised such findings and claimed that Privacy Sandbox would give Google the ability to favour its own ad inventory and ad tech services.[655] A corresponding decline in competition amongst ad tech providers could result in significant welfare losses, which leads to reduced innovation, diminished quality and price increases for publishers, marketers and consumers. Such effects might trickle down to users, culminating in less freely available ad-supported content online, or higher prices for goods and services.

The strengthening of Apple and Google's market power, which seems likely to take place, could indeed open the way for Google and Apple to exploit consumers. In fact, an exclusionary practice does not inherently qualify as exploitation, true exploitative practices

---

[649] Damien Geradin and Dimitrios Katsifis, “Trust me, I’m fair”: analysing Google’s latest practices in ad tech from the perspective of EU competition law" [2020] European Competition Journal 11.

[650] *Google Search (Shopping)* (n 192)

[651] 'Online Platforms and Digital Advertising Market Study' (n 1) paras 5.261-5.270.

[652] ibid, paras 5.261-5.270.

[653] ibid, para 5.272.

[654] ibid, para 5.279.

[655] CMA: 'Decision to accept commitments offered by Google' (n 643).

are those directly detrimental to consumer welfare or competition parameters. Nevertheless, this does not preclude evaluating the privacy policy implemented by these entities as a business practice entailing unfair trading conditions. Considering such policy changes in relation to privacy regulation, this thesis discusses whether this proposed tradeoff between privacy and efficiency could result in exploitation on the users' side. The discussion in this respect is elevated to a hypothetical level.

I assume that the amendments to Google's and Apple's privacy policies could raise privacy concerns. Google and Apple have had a great impact on ad tech services across the value chain,[656] having control of the most popular browsers and mobile OSs. Any amendments to Google's and Apple's privacy policies could have consequences for ecosystem participants. Arguably, this allows them to act as de facto privacy regulators.[657] Importantly, such power could extend typically beyond the GDPR and any privacy law, with them having different operational opinions, with the GDPR leading a discretion over the compliance manner.

De facto privacy regulators might decide on the trade-off between competition and privacy. They could also impose their values and judgement on the ecosystem users. Despite such broad power, large digital undertakings have not been held accountable for their decisions. From a privacy protection point of view, one could argue that Google and Apple's decision to limit the third party's ability to identify users results in a welfare gain for said users. It also remains unclear to what extent such an act could result in a service quality increase. Such a gain must be balanced against welfare losses resulting from legitimate limitation of advertising, as such a limitation could imply welfare losses for users who value personalised advertising, or ad-funded content online.

From a perspective of exploitative theories of harm, the CMA, investigating Google Privacy Sandbox, was concerned that Google would be likely to exploit its dominant position by limiting the options available to Chrome's users regarding the utilisation of their data for

[656] 'Online Platforms and Digital Advertising Market Study' (n 1) 20.

[657] Geradin, Katsifis and Karanikioti (n 624) 644.

targeted advertising.[658] This approach could reduce the level of users' choice in determining how their data is used for advertisement delivery. As such, I discuss two key elements that could bring user exploitation to the fore through the operation of Privacy Sandbox, based on the offered Google's Commitments.

Firstly, Privacy Sandbox blocks third-party cookies, but it does not limit online tracking.[659] This might result in further power imbalances between users and Google through unfair trading conditions. In other words, Google will continue to have access to a vast amount of user data, from services such as Gmail, Google Maps and Google search engine, which could become a profitable source for ad personalisation.[660] It might be suggested that banning third-party cookies from Chrome could strengthen Google's position due to their access to first-party audiences. Google would remain the only platform which stores the collected data storing all users' data on the browser itself, where it will be securely processed and analysed through Privacy Sandbox. However, it is not to suggest that enhanced privacy protection might be easily accepted as a remedy. Instead, the incentive might introduce anticompetitive discrimination against both consumers and digital rivals, which would later have to be balanced against its counterproductive result in a case-by-case consideration.

---

[658] CMA, 'Investigation into Google's 'Privacy Sandbox' browser changes' (*Press release*, 8 January 2021) < https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes> 28 February 2022., para 2.3.

[659] CMA keeps monitoring the Privacy Sandbox initiative. The recent report discussed the CMA views indicating that the CMA keeps engagement with market particulate on the development of the APIs, and continues testing and developing the framework for Google Privacy Sandbox's transparency. CMA, 'CMA update report on implementation of the Privacy Sandbox commitments' (CMA, 2023) < https://assets.publishing.service.gov.uk/media/644a82cd2f62220013a6a19b/CMA_s_Q1_2023_update_report.pdf> accessed 17 August 2023; Google, 'Privacy Sandbox Progress Report Q3 Reporting Period - July to September 2023 Prepared for the CMA, 24 October 2023' (2023) < https://assets.publishing.service.gov.uk/media/653a491d80884d000df71b70/Google_s_Q3_2023_report_.pdf> accessed 24 November 2023; CMA, 'CMA Q3 2023 update report on implementation of the Privacy Sandbox commitments' (2023) < https://assets.publishing.service.gov.uk/media/653a58e2e6c968000daa9b94/__Q3_2023_update_report____.pdf> accessed 24 November 2023.

[660] Ben Thompson, 'Digital Advertising in 2022' (*Stratechery*, 8 February 2022) <https://stratechery.com/2022/digital- advertising-in-2022/> accessed 6 November 2022; Mark Nottingham, Playing fair in the Privacy Sandbox: competition, privacy, and interoperability standards' [2021] SSRN < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891335> accessed 17 May 2022.

In this scenario, surveillance on such platforms could introduce exploitative harm to society and online users.[661] There is a possible relationship between competition in digital markets and privacy protection: the economic features of the large digital company might strengthen the market power, regardless of their willingness to consider privacy-enhancing policies. Geradin suggested that Google seemed to be indifferent to online tracking.[662] Google's emphasis on third-party tracking, which allows for the collection of data from external to the platform sources, could deflect attention from Google's tracking practices. Arguably, Google can be proactive in limiting the flow of information between different ad tech companies, as increased data collection introduces a competitive advantage over competing intermediaries.[663] Google could not demonstrate sensitivity when balancing GDPR enacted principles, particularly concerning the use of data gathered from their platforms for ad tech purposes; this could be achieved only if it obtain specific and separate consent for that use. In such instances, the companies' interests could diverge from considerations of data protection. Consumer welfare is not solely affected by prices and product availability but also by the perception of products and services as invasive of users' privacy. Such offerings may be seen as detrimental to consumer well-being.[664] Here, the interests of digital firms could diverge from data protection. While prioritising profit, Google's adoption of the purpose limitation principle, as suggested by the CMA, would signal genuine concern for user privacy.[665] However, given the profit-driven nature of Google's strategy, it is sceptical to expect it to prioritise data minimisation over potential gains from the Privacy Sandbox, which offers opportunities for expanded data collection and profitable ad personalisation.

Secondly, the Privacy Sandbox could be seen as an unfair term of a contract with Google under Article 102(a) TFEU. The CMA was particularly concerned that Google would be able to exploit its dominant position by denying users substantial choice in terms of how their

---

[661] Sally Shipman Wentworth, 'Pervasive Internet Surveillance – Policy ripples' (*Improving Technical Security,* 26 June 2014) < https://www.internetsociety.org/blog/2014/06/pervasive-internet-surveillance-policy-ripples/> accessed 6 November 2022; Glenn Fleishman, 'How the tragic death of Do Not Track ruined the web for everyone', FastCompany (17 March 2019) < https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the- web-for-everyone> accessed 17 May 2022.

[662] Geradin, Katsifis and Karanikioti (n 624) 654.

[663] 'Online Platforms and Digital Advertising Market Study' (n 1) appendix M, para 520.

[664] *Port of Genoa* (n 188).

[665] 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658).

data might be used for advertising purposes.[666] Possible phrasing out of cookies might result in furthering the asymmetry of information between Google and third parties particularly in assessing different design options for capturing users' data.[667] Google has committed to designing and developing the Privacy Sandbox interface by taking into account the criteria agreed with the CMA. Particularly, Google aims to develop the Privacy Sandbox considering users' privacy and experience, and Privacy Sandbox's impact on competition in digital advertising.[668] Yet, the CMA can open its investigation into the practices and impose interim measures in future if necessary.

Arguably, Google's pro-privacy policy amendment might have a significant effect on users, as the policy change would be ambiguous and difficult to estimate. As a response, Google offered a series of Commitments aiming to address the CMA's concerns relating to its Privacy Sandbox interface.[669] Such commitments include an increased collaboration with the CMA, aiming to develop Privacy Sandbox transparently. Also, Google committed itself to ensure an increased transparency in the use of personal data, which included an increased transparency over the use of users' data, and no self-preferencing over Google-owned products and services.[670] The CMA continues to monitor the offered Commitments, particularly in relation to data collection and processing activities.[671]

I consider Google's introduction of Privacy Sandbox incentive as being a two-faced phenomenon. On the one hand, Privacy Sandbox removes cross-site tracking, which increases the creation of privacy as a quality. This could be considered a welfare gain for

---

[666] 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658)

[667] ibid, para 2.5

[668] Google, 'The path forward with the Privacy Sandbox' (2022) <https://blog.google/around-the-globe/google-europe/path-forward-privacy-sandbox/> accessed 18 July 2023.

[669] ibid; The CMA announced in November 2021 that it secured an improved set of commitments from Google. The initial commitments consulted in June 2021 involved the key role for the CMA to monitor the design and development the interface. Especially, the updated commitments concerned an increased transparency. Furthermore, in February 2022, the CMA accepted the revised commitments from Google relating to the interface. At that time, the concern regarded again the transparency over the third-party access to data. Yet, this time CMA believed that offered commitments provided sufficient safeguard for competition law.

[670]'CMA update report on implementation of the Privacy Sandbox commitments' (n 659); 'Privacy Sandbox Progress Report Q3 Reporting Period - July to September 2023 Prepared for the CMA' (n 659).

[671] ibid, 15

consumers. On the other hand, Privacy Sandbox results in users being exposed to less relevant advertising. This unquestionably corresponds to a welfare loss for consumers valuing relevant ads.[672] Of course, Google's conduct could distort competition, however Google could tentatively attempt to justify this by privacy considerations based on the efficiency defence, relying on a positive competition effect that the third-party cookies ban might support innovation and not damage consumer choice.

4.2.3 Analogy between excessive pricing, excessive data acquisition and subscriptions fees

The crucial element of an antitrust infringement is some form of misconduct that violates competition. In other words, it is conduct that not merely involves data mistreatment, and breaches of user privacy, but the conduct must have a negative impact on competition. Here, this thesis presents how it is possible to draw an analogy between excessive pricing and excessive data acquisition as per Article 102(a) TFEU. In fact, consumers pay with more than one currency while using digital platforms and services. Consumers could pay either with (1) privacy and attention,[673] and (2) money, attention and privacy. Therefore, the assessment under Art. 102 should take into account all the elements that constitute the price paid by consumers. In this section, I focus on the ongoing data protection investigations vis-a-vis the new consent vs pay policy recently introduced by Facebook, in which users could pay with a combination of money, attention and privacy. The presented discussion is hypothetical as would consider subscription fees and data collection as excessive. Such conditions would be difficult to meet in practice.

Recently, Facebook introduced the 'pay-or-okay' model as a response to stricter regulations regarding user data collection for targeted advertising.[674] The introduction of this model was influenced by the CJEU ruling.[675] The 'pay-or-okay' model offers users two choices: (1) pay for an ad-free experience without tracking, starting at €12,99/month, or (2) agree to data

---

[672] 'Online Platforms and Digital Advertising Market Study' (n 1) appendix G, para 378.

[673] The discussion on attention and privacy payment in this thesis is considered as unfair trading condition and is explained in section. 4.2.1

[674] Meta, 'Facebook and Instagram to Offer Subscription for No Ads in Europe' (30 October 2023) <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/> accessed 19 March 2024.

[675] See, *Meta Platforms* (n 41).

processing and personalised advertising.[676] Despite being a response to legal requirements, the 'pay-or-okay' model has faced criticism, surrounding freely given consent.[677] The implementation of the 'pay-or-okay' model also prompts consideration as to whether it could effectively address competition concerns or if potential risks of anticompetitive outcomes remain.

The “pay-or-okay” model triggers the application of two legal frameworks: the GDPR and the ePrivacy Directive.[678] To adhere to both regulations, websites are required to obtain consent from consumers when tracking their behaviour for purposes beyond necessity, with advertising being one of such purposes.[679] The determination of whether consent is necessary relies on analysing the purpose of each tracker used on a given website or app. The GDPR enforcement has underscored that consent is the sole legal basis for online behavioural advertising. This stance has been also reinforced by several GDPR-related proceedings against Facebook.[680] In fact, consent must meet several criteria, such as being freely given, specific, informed, or unambiguous.[681] Particularly, the “pay-or-okay” model aims at the requirement for freely given consent.

The requirement for consent to be valid emphasises users’ voluntary decision to either allow or refuse the processing of personal data. In fact, such a decision should be made without any form or coercion to persuade users to give consent. Also, there should be no negative repercussions if users refuse consent for targeted advertising. If users feel compelled to consent, facing negative consequences including additional costs, and/or suffering detriment

---

[676] BEUC, 'Choose to lose with Meta - an assessment of Meta's new paid- subscription model from a consumer law perspective' (2023) https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-156_Annex_Legal%20assessment_Choose_to_lose_with_Meta_Legal_analysis.pdf> accessed 19 April 2024.

[677] See for example, Noyb, ‘Complaint to the Austrian DPA against Meta’ (2024) <https://noyb.eu/sites/default/files/2024-01/Meta_Withdrawal_Complaint_REDACTED_EN.pdf> accessed 19 April 2024.

[678] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201/37

[679] ibid, Article 5(3)

[680] For example, Irish Data Protection Commission, Final Decision against Meta Platforms Ireland Limited (Facebook service), DPC Inquiry Reference: IN-18-5-5, 31 December 2022 <https://www.dataprotection.ie/sites/default/files/uploads/2023- 04/Meta%20FINAL%20DECISION%20%28ADOPTED%29%2031-12-22%20-%20IN-18-5-5%20%28Redacted%29.pdf> accessed 19 April 2024.

[681] GDPR (n 57) article 4.

to consenting, then their consent will not be considered valid. [682] Making access to a website conditional on acceptance of non-essential trackers could be freedom of choice in certain instances, thereby affecting the validity of consent.[683]

In the view of EDPB, the “pay-or-okay” model was introduced in an imbalanced power dynamics, as the consent became conditional rather than specific and incompatible with Article 6 GDPR.[684] Facebook's market dominance and strong network effects also resulted in a "lock-in effect", making it challenging for users to switch to alternative platforms and reinforcing their reliance on Facebook and its own and controlled platforms. Moreover, Facebook enjoys market power over general-purpose social networks, excluding those dedicated to specific groups like LinkedIn. Such factors contribute to the imbalanced relationship, establishing a situation of subordination. In the case of Facebook, it can be assumed that consent is forced as the model makes access to the service dependent on users' consent for processing of personal data unrelated to the core services, such as for advertising purposes.[685] This conclusion stems from the precedent set by rulings indicating that advertising is not essential for providing a service to users.[686] In practice, this requires that consent for data processing has to be clearly separate from contracts or agreements, such as a paywall, which is the second option available to users, as per Article 7(4) GDPR. The EDPB claimed that "the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."[687] In this regard, connecting consent to a payment might have an effect that the fundamental right to privacy is an exchange for payment. Such an approach implies that users are not entitled to data protection, and have to purchase their fundamental rights from controllers. In fact, it remains unclear if users will continue to be tracked if they opt to pay, and if so, what specific purposes aside from advertising. Moreover, if users consent to targeted ads, the purposes for which their personal data might be processed beyond advertising are also unclear.

---

[682] EDPB Consent Guidelines (n 61)

[683] GDPR (n 57), Recital 43

[684] EDPB Consent Guidelines (n 61) para 41.

[685] EDPB (n 30), para. 39, GDPR (n 57) Article 7(4) and Recital 43.

[686] *Meta Platforms* (n 41); Article 29 Data Protection Working Party (n 72).

[687] EDPB Consent Guidelines (n 61) para. 26

Generally, the Data Protection Authorities are rather satisfied with the proposed model.[688] Yet, there is a consensus that there is a requirement for an alternative, fair and reasonable model without tracking for targeted advertising. In fact, there is also a call to ensure that an alternative assessment needs to be carried out due to a possible imbalance between Facebook and its users.[689] The EDPB has not yet issued its opinion but provided that it cannot definitively assess whether offering a paid alternative to a service involving tracking would ensure valid consent for any tracking-related processing for advertising purposes. It emphasised the need for a case-by-case analysis to determine the validity of consent for advertising purposes.[690]

The 'pay-or-okay' model operates akin to a subscription fee, where users provide personal data in exchange for access, reflecting differing assessments of its value between online users and data collectors. The content of the 'pay-or-okay' model, the informed consent requirement is deemed crucial to assess the voluntary nature of consent, including the type of information provided, its purpose and the appropriateness of the price. In other words, the price of the 'pay-or-okay' model should be reasonable, which will be only asses on the case-by-case analysis. However, if the price is unreasonable, having accounted for Facebook's dominant position, exploitative abuse of excessive pricing, as per Article 102(a) TFEU, can be applied as encompassing actions directly detrimental to consumers.[691]

The cornerstone of excessive pricing is the existence of a qualifiable monetary price. As per *General Motors*, it is possible to hold an undertaking accountable for abuse of its dominant

---

[688] See for example, Österreichische Datenschutzbehörde, Decision on Complaint Dated 25 May 2018 GZ: DSB-D122.931/0003-DSB/2018, Issued on 30 November 2018 <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf> assessed 19 April 2024.

[689] Commission Nationale de l'Informatique et des Libertés, 'Cookie walls : la CNIL publie des premiers critères d'évaluation', 16 May 2022, <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation> accessed 19 April 2024.

[690] EDPB, 'EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices –DRAFT PRINCIPLES (Ref. Ares(2023)6863760)', (2023) <https://www.edpb.europa.eu/system/files/2023-12/edpb_letter_out20230098_feedback_on_cookie_pledge_draft_principles_en.pdf> accessed 19 April 2024.

[691] *Continental Can* (n 248) para. 26

position by excessive pricing relating to the economic value provided.[692] As per the ECJ's wording, excessive pricing is prohibited as a monopolist, relying on its domination position, "reap trading benefits that [he] would not have reaped if there had been normal and sufficiently effective competition."[693] Such cases are controversial due to apparent difficulty in establishing a price's "excessiveness."[694]

The *United Brands'* two-stage test can be used to determine if price is excessive might provide support to determine if the platform's 'pay-or-okay' model is extensive regarding the economic value of the service.[695] Firstly, it needs to be assessed if the price (and possible data collection) is "unfair in itself or when compared to competing products."[696] The second step of the *United Brands* test requires an assessment of whether the price is unfair in terms. Here, a reference should be made to a benchmark to assess the extensiveness of price, pursuit of verifiable criteria, and appropriateness.[697] For example, in *Latvian Copyright Society,* the price difference needed to be persistent and significant.[698] To apply such a rationale, the assessment would require comparing various privacy policies offered by competing digital platforms engaged in data collections. In fact, such an assessment might be complicated due to the vagueness of the offered privacy policies. Hence, it could be problematic to ascertain the precise terms of legitimate data collection, the privacy of users and extensive data collection due to lack of available methodology, and this concept remains the scope of this thesis However, it is noted that online users are frequently exploited by unfair terms, where a precise limit of data collection by both service provider and third parties is unmentioned.

The assessment if the price is excessive might be only answered through a consideration of economic analysis. However, as Facebook's average revenue per user in the EU is around €6

[692] *General Motors* (n 165).

[693] *United Brands* (n 195).

[694] Robertson (n 522) 9.

[695] *United Brands* (n 195) para 252.

[696] ibid, para 252.

[697] See, Case 226/84 *British Leyland Public Limited Company v Commission of the European Communities. Cominant position - Type approval for motor vehicles* ECLI:EU:C:1986:421.

[698] Case C-177/16 *Autortiesību un komunicēšanās konsultāciju aģentūra (AKKA)/ Latvijas Autoru apvienība* (LAA) [2017] ECLI, para 55 (hereinafter: *Latvian Copyright Society)*

per month,[699] charging subscription-fee-paying-users around €12.99 for using the service, while still collecting and proceeding data might be seen as constituting the price considerably higher than market conditions would dictate. In effect, Facebook, as an unavoidable trading partner,[700] would charge a price for its service and continue to collect data from its users. Effectively, Facebook's users would end up paying twice for its service. The 'pay-or-okay' model will be legal if the price charged is fair and reasonable, and aims to collect data restricted to only what is necessary.[701] Such consideration indicates that the model is problematic for both competition law and the GDRP. GDPR could only be treated as a guideline to assess if data collection is fair and could be introduced into the wider scope of legal and economic contexts surrounding the competition assessment.[702] Facebook will, also, be able to increase the price to its consumers, especially considering any lock-in effects of social network platforms.[703] Consequently, even if Facebook was solely receiving the subscription fee, the price would still be possibly excessive. However, if one assumes continues to collect and process data, as well as display (albeit less profitable but still lucrative) ads alongside the subscription fee, the total price paid, comprising both monetary and data aspects, is more likely to be genuinely excessive.

The specific application of the 'pay-or-okay' model to cannot be fully ascertained, until it fully becomes enforced.[704] However, it has been indicated that the typical model of excessive data collection by platforms amounts to a market failure,[705] and a possible

---

[699] Alessia D'Amico, Meta's Pay-Or-Okay Model: An Analysis Under Eu Data Protection, Consumer And Competition Law' (2024) Working Paper 1-2024 08-04-2024 < https://www.uu.nl/sites/default/files/rebo-renforce-working-paper-2024-Meta's Pay-or-Okay Model - An Analysis Under EU Data Protection, Consumer, and Competition Law.pdf> accessed 10 April 2024.

[700] *Google Ads Rules* (n 556); *Google News* (n 557).

[701] Mario Martini and Christian Drews, 'Making Choice Meaningful – Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy Law' (SSRN, 2022) <https://ssrn.com/abstract=4257979> accessed 14 April 2024.

[702] *Meta Platforms, Opinion of AG Rantos* (n 85) para 23.

[703] Benjamin Krischan Schulte, *Staying the Consumption Course: Exploring the Individual Lock-in Process in Service Relationships* (Springe 2015); Marco Botta and Klaus Wiedemann, 'EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita', [2018] Max Planck Institute for Innovation and Competition Research Paper No. 18-08.

[704] *United Brands* (n 195), paras. 251-252

[705] Economides and Lianos (n 24)

exploitative pricing abuse of itself.[706] In this context, this section assumes that it is possible to expand the 'pay-or-okay' model as extending that market failure; users of Facebook, who decide to pay the subscription fee, still need to provide their data, with an option to not see personalised ads. Under the paid model, Facebook continues some data collection but also appears to be intensifying such practices. If one assumes this market failure, both with the fact that Facebook has been found to enjoy excessive profitability,[707] it is able to deduce that the market functions are difficult to be described as normal, giving rise to the price changes being seen as excessive.

4.2.3.1 Behavioural limitations

In the scope of assessment, there is an additional element of price dimensions offered and recognised on many platform markets: while consumers consent to dispose of an unknown amount of personal data, consumers also face targeted adverting while using such platforms. Hence, the price-like element might take the form of data acquisition, attention or behaviour, or money. The behavioural/attention element of pay is discussed in the next paragraph. There is a risk of under-enforcement if the competition assessment is solely focused on the market-foreclosure test performing only a conservative analysis of the barriers to market entry, without including an analysis of consumer harm from exploitation abuses. Particularly, in the non-monetary markets, large digital undertakings have a strong ability to influence users' choices. By focusing on the case studies described in this thesis, large digital undertakings make use of this ability, especially when they provide their digital products and services.[708] In this respect, there has been more emphasis attached to consumer choice and autonomy in the cases regarding online platforms.[709]

Consumer choice implies that "the consumer has the power to define his or her own wants and the ability to satisfy these wants at the competitive prices' and has even been called 'the ultimate goal of antitrust".[710] Article 6(1)(a) GDPR mandates that when consumers provide

---

[706] Botta and Wiedemann (2018) (n 703).

[707] Online Platforms and Digital Advertising Market Study' (n 1) paras 2.73-2.81.

[708] See Chapter 3, especially the discussion about the *Facebook case* (section 3.5) and the *Google/Fitbit* merger case (section 3.3.1) as well as the discussed above Google Privacy Sandbox example (section 4.2.2(2))

[709] See for example, Podszun (2019) (n 302); Friso Bostoen, *Abuse of Platform Power Leveraging Conduct in Digital Markets under EU Competition law and Beyond* (Concurrences 2023) 90-91.

[710] Robert Lande, Consumer choice as the goal antitrust (2001) 62 University of Pittsburg Law Review 503, 503.

their data to large digital companies, it should be done through a 'notice and consent' approach. In this respect, companies are required to inform their users about the data they are gathering specific reasons for which they use their data. Based on this information, individuals can then decide whether they agree to allow the processing of their data. However, the notice and consent solution might not work effectively for consumers to make meaningful decisions about the data collection and possible use of their data.[711] The *Facebook* case remains the primary example of the trend of enforcers asserting that competition law can be informed by data-protection principles, as well as data protection might be enforced outside its usual context. From the perspective of this case, end users might experience less privacy and authority over their data, resulting from excessive data collection and processing practices.[712] Indeed, from the standpoint of competition law, restriction of privacy could be a matter of abuse of dominance is itself evidence of market failure.[713] The aspects of online commercial manipulation led to an extensive scholarly debate in trying to define the online and offline contexts of exploitation.[714] The concept of behavioural market failure has been covered by Kerber and Zolna who asserted that consumers cannot effectively handle their data in a rational and informed manner.[715]

In the digital platforms' context, users either pay for money, data or their attention, or a combination of these.[716] A particularly important problem is that data-collecting undertakings can employ various tactics to influence consumers' decisions regarding consent. Here, the behavioural element supports an increased consumption of the users; consumers are likely to stay on a platform used by family and friends, often unaware of

---

[711] Giuseppe Colangelo, 'The Privacy-Antitrust Curse: Insights from GDPR Application in EU Competition Law' (2023) ICLE White Paper 2023-10-12

[712] Autorité de la Concurrence and Bundeskartellamt (n 26) 25, *Facebook case* (n 2).

[713] Economides and Lianos (n 24).

[714] ibid; Robertson (n 522); see also, D Kysar Hanson, 'Taking Behavioralism Seriously: The Problem of Market Manipulation' [1999] NYU L Rev 630.

[715] Wolfgang Kerber and Karsten Zolna, 'The German Facebook case: the law and economics of the relationship between competition and data protection law' (2022) European Journal of Law and Economics 217, 30

[716] Wolfgang Kerber and Louisa Specht-Riemenschneider, 'Synergies Between Data Protection Law and Competition Law' (2020) Bundesverband <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3977039> accessed 1 June 2022.

maintaining competitive pricing because of their increased consumption.[717] In this respect, the 'attention theft'[718] has been shown as one possible new form of exploitative conduct in the digital economy.[719] Yet, the theoretical form of behavioural exploitation of internet users has been fragmentary and little has been done to convert it into an operational standard of competition law. The digital market provides ostensibly free services for consumers, and quality forms an important parameter of competition.[720] Considering the example of the BKartA *Facebook* case, the distortion of privacy was seen as harming consumer welfare, despite the lack of price effects, and in the *Facebook* case, competition law was perceived as sufficiently flexible to consider GDPR infringements as a proxy to find competition distortion.[721] In addition, the CJEU, in the *Facebook case,* emphasised that a lack of freely given consent constitutes a viral clue in finding abuse in the sense of Article 102 TFEU.[722] The CJEU emphasised that the users' lack of clear information about the data processing activities can result in clear power imbalances between Facebook and its users.[723] Such data-rich acquisition could be self-reinforcing, as companies with superior data access might better target users, as well as improve the equality of a product. In turn, they could draw more users and generate a further amount of data — this is a lucrative feedback loop,[724] and possible bundling of users' consent. Such a feedback loop generates data-opoly's power, as more users allow more data to be captured.

Based on that, user manipulation and exploitation influence the ability to make a deliberate choice, creating the concept of a vulnerable consumer. Susser argued that such

---

[717] Arletta Gorecka, 'Is "Privacy" a Means to Protect the Competition or Advance Objectives of Innovation and Consumer Welfare?' in Maria Tzanou (ed.) *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020) 119

[718] T Wu, 'The Attention Economy and the Law' [2017] ALJ 771.

[719] Massimo Motta, 'Self- Preferencing and Foreclosure in Digital Markets: Theories of Harm for Abuse Cases' (2022) BSEWorking Paper 1374 < https://bse.eu/sites/default/files/working_paper_pdfs/1374_0.pdf> accessed 10 May 2023.

[720] Kerber and Specht-Riemenschneider (n 716); *Facebook/WhatsApp* (n 90); *Microsoft/Linkedin* (n 90); MC Wasastjerna, 'The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface' [2019] European Business Law Review 337.

[721] *Facebook case* (n 2).

[722] *Meta Platforms* (n 41) para 62.

[723] ibid, para 62 and 151.

[724] Stucke (n 26) 13.

manipulation exploits user's vulnerability by reporting that user choice has not been sufficiently engaged.[725] Posner offered that manipulation aims "to control or play upon by artful, unfair, or insidious means especially to one's own advantage."[726] Digital platforms can reach across various human experience dimensions. They are dynamic, intrusive, and interactive, which allows them to create a personalised choice architecture that steers consumer preference.[727] Hence, to state a digital service provider's practice as manipulative, it needs to be aware of online users' vulnerability. Such service providers need to have knowledge and motivation and be ready to ignore users' self-interests. In return, users need to be unaware of such tactics and/or be unaware of their effects on their behaviour.

I consider that digital service providers typically opt to not disclose the tactics and traits used to target users on an individual level. Such a concept underlies users' self-determination and digital autonomy; Calo expressed that there is a linked mediatory role of design in every aspect of the integration with consumers.[728] Essentially, data collection and analytics expand the online manipulation of digital users. There could be three issues of the digital economy manipulating practices that impact users' privacy. Firstly, there is an element of pervasive data collection, as discussed above. Secondly, users continue to access platforms such as Facebook and Google due to their high position on the relevant market and network effects, hence manipulation is an ongoing process. Thirdly, it remains difficult to capture this manipulation process, which could be both captured as a form of an unfair trading condition or excessive data collection. Cases such as the BKartA *Facebook case* are only the beginning of the fallacy, and sudden privacy-protective-polices such as Google's Sandbox might be a false proxy to offer privacy, while excluding consumer choices. It could exploit users' vulnerability to impact the extent to which their privacy is protected.

---

[725] Daniel Susser, Beate Roessler, and Helen Nissenbaum, 'Online Manipulation: Hidden Influences in a Digital World' [2020] Geo L Tech Rev 1.

[726] Eric A Posner, 'The Law, Economics, and Psychology of Manipulation' (2015) Coase-Sandor Inst for Law & Econ Working Paper No 726.

[727] Peter Behrens, 'The "Consumer Choice" Paradigm in German Ordoliberalism and its Impact upon EU Competition Law' (2014) Europa-Kolleg Hamburg Discussion Paper No. 1/14; Kerber and Specht-Riemenschneider (n 716).

[728] R Calo, 'Consumer Subject Review Boards: A Thought Experiment' [2013] Stan L Rev Online 97, 103.

Correspondingly, manipulation and attention will continue to improve sophisticated data analysis. Accordingly, such a practice can be evaluated as exploitative, as the lack of available choices for the users might undermine their autonomy to consent under Article 6 GDPR. Due to the entrenchment of lock-in effects, this limitation of choices constitutes an exploitative practice within the scope of competition law. In a genuinely competitive environment, one would anticipate a wider array of market options for social networks.[729] One could envision manipulation as involving an "intervention that changes the way an individual behaves and that but-for this intervention said individual would have behaved differently."[730] Online manipulation uses consumer behaviour and their data against their ability to make rational choices, influencing their internal decision-making process that proclaims the way they understand their choices. Therefore, online platforms could make privacy settings difficult to find or change. Frustrated consumers then opt to stay for low-privacy defaults. Therefore, it is deducible that privacy concerns might not revolutionise the competition law itself, but privacy-harms might enforce a range of, not easily quantifiable, variables impacting consumer welfare. Notably, one should remember to keep competition law and privacy harms separate, competition law would only consider the market influence, and mere privacy breaches could not qualify as being important for competition law assessment. Competition law could intervene if the consumer falls into a privacy trap where they disclose more data over time, being unable to control their privacy. In this case, complex privacy tools introduce a perception of privacy protection, while leading to a greater discourse on data. By providing some form of wider effects of the market such as manipulation, *de minimis* criterion could be set that avoids over-regulation.[731]

4.2.4. Quiet life analogy and privacy-related harms

The 'quiet life' is a type of exploitative abuse produced by the modules of neoclassical economics.[732] Here, a monopolist would not be subject to any competitive pressure to

---

[729] See, *Facebook case* (n 2), Google/DoubleClick (n 202) para 303; Colangelo (n 711).

[730] Economides and Lianos (n 24).

[731] It is beyond the scope of this thesis to focus on *de minimis* criterion. For a wider consideration on the criterion see: Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice) (OJ C 291, 30.8.2014, p. 1–4).

[732] Barry Rodger and Angus Macculloch, *Competition Law and Policy in the EU and UK* (Routledge 2021) 247.

innovate, which allows them to enjoy 'the quiet life'.[733] For example, the CJEU, in *Porto di Genova*, it was held that refusal to apply modern technology for unloading operations by a port operator was abusive, as the older method of operation was more expensive.[734] Similarly, in *ENI*, the binding commitments were abusive as underinvestment in its long-distance gas pipelines could threaten profits on other parts of their business.[735]

The 'quiet life' abuse can also be linked to exploitative practices in the context of privacy. In the digital economy, dominant players may resist adopting more secure and privacy-conscious technologies to maintain their market advantage, enjoying a 'quiet life' while avoiding competitive pressures to innovate in this area. Here, the key consideration is the lack of the monetary price we pay for accessing digital platforms. If we cannot consider the monetary payment of data, then the problem is what is the valuation of data.[736] This is a concept beyond the scope of competition law.

This thesis argues that the 'quiet life' analogy could also be applied to the large digital firms' scenario, allowing them to exploit users and impede innovation. Therefore, this thesis presents two sides of such a debate: (1) there are issues relating to the assumption that users are rationally able to determine long-term interests in sharing data; and (2) limitation of data harvesting could blindly introduce higher privacy but reduce innovation.

(1) Users are unable to rationally determine long-term interests of sharing data

It is broadly acknowledged that large digital undertakings (especially GAFAM) have been key drivers of innovation.[737] Their entrenched market position could introduce negative constraints on competition, consumer choice and innovation. For the clarity go the argument, I emphasise on practices of GAFAM companies as key digital market players. GAFAM companies have been innovative, increasing their economic power, data acquisition and capacities relating to data analytics. Such conducts allow them to increase their market power positions. GAFAM companies offer quasi-monopolistic core platform services,

[733] Rodger and Macculloch (n 732).

[734] *Porto di Genova* (n 521).

[735] Commission Decision of 29 September 2010, *ENI* (Case COMP/39.315), OJ 2010, C352/8.

[736] Kerber and Specht-Riemenschneider (n 716).

[737] See Cremer Report (n 1); Furman Report (n 1).

allowing them to use unfair and exploitative practices on their end users. This, in turn, introduces new dangers to personal privacy and their right to make rational decisions on the collection of their personal data. Reduction of privacy protection affects the form and quality of consumer choice or diminishes innovation. For example, in the *Google/Fitbit* merger case, emphases that any infringement of privacy should be a matter for data protection law rather than competition law.[738] This general approach is both shared by the Commission and the US FTC.[739]

Large digital undertakings with superior access to data can better use data to target users or improve product quality, drawing more users to their platform.[740] By capturing users' data and attention, large digital firms may manipulate users' behaviour, and reduce innovation or users' privacy. Using the example of the *Google/Fitbit* merger case — with Fitbit being a part of Google's ecosystem, Google can use Fitbit's data for advertising purposes. Increased collection of data from Fitbit wearable might straighten Google's position and lead to exploitation and discrimination of users. Google suggested that: "Fitbit data might conceivably be of some value in the future in trying to predict certain health outcomes."[741] In short, the merger may result in less control over data and less privacy for Fitbit users. Essentially, such behaviour might introduce anticompetitive constraints, which exploit digital users. In the previous sections, I explained how users are being exploited by behaviour biases and unfair trading conditions, manifested mainly by users' inability to make radical choices when providing their data. Digital platforms are better off while users are worse off under the requirement of providing data for using and accessing digital platforms.[742] Enhanced market power could be manifested in non-price terms and conditions, adversely affecting customers, with reduced product quality, product variety and diminished innovation. Here, these arguments discussed above are extend, presenting that there are concerns that users cannot rationally determine the long-term effects of sharing data.

---

[738] *Google/Fitbit* (n 155) para 164.

[739] Swire (n 204); Pamela Harbour and Tara Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' [2010] Antitrust Law Journal 769; Ezrachi (2018) (n 300).

[740]Boerman, Kruikemeier and Borgesius (n 16).

[741] *Google/Fitbit* (n 155) para 477.

[742] Economides and Lianos (n 24) 817.

Consumer harm, in the above scenario, relates to the notice-and-consent model that reflects on users' ability to bargain for higher privacy standards. The concept of fairness might provide some flexibility to the enforcement to determine broader standards. In other words, the concept of fairness could encompass the protection against exploitative abuse and its impact on innovation. This would also be in line with the *Facebook case*, which focused primarily on the exploitative nature of terms and conditions offered and their impact on informational self-determination. Including distributional goals of fairness could open the door to considering broader factors in exploitative abuses, such as privacy. As discussed above, exploitative theories of harm can centre on the extraction of excessive rents from consumers.[743] Essentially, theories of harm also involve a perspective of citizens that is not confined to a narrow economic standard.[744] For example, in *Facebook/WhatsApp*,[745] the Commission claimed that privacy polities establish a non-price parameter of competition: a degradation of private policies affect aspects of product quality, or even amount to the product price increase.[746]

Additionally, the concept of fairness is linked to innovation, as fair competition ensures a better quality of technological services and products while aiming at cost reduction, which then benefits consumers since they gain from low cost and high product quality.[747] Nonetheless, the fusion of efficiency and fairness requires a certain act of value balancing. Specifically, the undertakings should not be seen as limited to the adoption of a norm-neutral economic approach as that might result in the risk of dissolution of EU competition law from its roots and norms, which includes fairness.[748] Hence, the economic theory might act as a normative theory resolving any concerns, with non-efficiency objectives being expunged.[749] Such an approach could substitute democratic control with technocratic control.

---

[743] See chapter 4, section 4.2.3.

[744] Townley (n 159); Renato Nazzini, *The Foundations of European Union Competition Law: the Objectives and Principles of Article 102* (OUP 2009); Lianos (2018) (n 572).

[745] *Facebook/WhatsApp* (n 90).

[746] *Microsoft/LinkedIn* (n 90).

[747] Case C-42/07 *Liga Portuguesa de Futebol Profissional and Bwin International* [2009] ECR I-7633, Opinion of AG Bot, para 245; Case C-203/08 *Sporting Exchange* [2010] ECR I-4695, Opinion of AG Bot, para 58.

[748] Ezrachi (2016) (n 174)

[749] ibid.

In essence, certain large digital undertaking's conduct is presumed to be detrimental to the fairness and contestability of the market.[750] The notion of fairness has always been a part of Article 102 TFEU application, as demonstrated in the *Google Android case.*[751] In addition, the notion of fairness emphasises that there is a "special responsibility of the dominant firm not to allow its conduct to impair genuine undistorted competition on the common market", affirmed by the CJEU in several anticompetitive cases.[752] Such responsibility is recognised as an obligation not to prevent an effective competition (as per *Michelin I*),[753] and to not constrain access to the market (as per *Intel*).[754] Furthermore, the additional examples of the notion of fairness may be derived from new forms of abuse of dominant position. For example, in the *ITT Promedia case*, the CJEU held that the right to effective judicial protection and access to justice under Article 47 of the Charter might be potentially considered as an abuse of dominance in two situations: if the legal action is not a genuine effort to establish the right of the concerned undertakings, and if the action is part of a larger strategy aimed at eliminating competition.[755] The first situation concerns the notion of fairness, while the second influences the competition on the merits.[756] Furthermore, in the *AstraZeneca* case, the CJEU indicated that when an undertaking believes that it is a legitimate right, it cannot employ any methods to secure that right. In other words, employing inappropriate means would run counter to fair competition principles and the special responsibility held by dominant companies.

The role of fairness concerns also the application of Article 102 TFEU in relation to privacy-related harms. Arguably, it could allow to demonstrate a direct link between the large digital undertaking position and any possible unfair practices and competition infringement to the

---

[750] Šmejkal (n 255) 47.

[751] *Google Search (Shopping)* (n 192); *Google Android* (n 470)

[752] *Netherllandnsche Banden Industrie Michelin* (n 234) para 57.

[753] ibid, it was also recognised in *Intel* (n 223); Case T–228/97 *Irish Sugar Plc v Commission* Judgment of 7 October 1999, ECLI:EU:T:1999:246, para 112; Case T–203/01 *Manufacture française des pneumatiques Michelin v Commission* Judgment of 30 September 2003, ECLI:EU:T:2003:250, para 55; *British Airways* (n 229) para 242; *AstraZeneca* (n 99); *Google Search (Shopping)* (n 192).

[754] *Intel* (n 223)

[755] Charter (n 46) article 47.

[756] Case T- 111/96 *ITT Promedia v Commission* 17 July 1998.

detriment of price, quality, and innovation. This issue has been a prominent interest in the *Facebook case*, as well as other data-related antitrust investigations discussed in this thesis.[757] While discussing the relevance of the relationship between fairness and exploitative privacy-related harm, it is important to emphasise that finding an unfairness requires a specific evaluation of the market context and any possible influence on competition of the merits.[758] In terms of users, this amounts to an imbalance in power bargaining, and the large digital undertakings could obtain an advantage from the situation in which the services provided by large digital corporations to business users are not proportionate to the fees or charges levied on their users. It is assumed that this approach considers a distributional question between users and platforms, based on sharing of the created value. Hence, the importance of fairness could be interpreted in as:

1. In the instances of unfair and exploitative practices though the economic power of large digital undertakings could result in different negative effects,[759] and it is important to keep users protected against the negative economic power of gatekeepers.
2. Fairness could refer to transparency against misleading practices exploiting end-users, such as biased consent architecture.[760]
3. Autonomy of users and business could be impacted, influencing the choice architecture, freedom to compete and exploitation of personal data.[761]

In consideration of 'the quiet life' analogy, it is important that the fairness concept deals with market failures, especially imbalances of power and innovation and behavioural problems. Furthermore, contestability needs to be ensured. It is also important to guarantee that business users are protected against unfair platform rules and not deprived of the opportunity to innovate, which could be limited by large digital undertakings who lock-in users and introduce negative effects on competition and innovation.

---

[757] See, *Google Search (Shopping)* (n 192); *Google/Fitbit* (n 155); *Facebook case* (n 2).

[758] See, *Facebook case* (n 2)

[759] Kerber and Specht-Riemenschneider (n 716).

[760] See, *Facebook case* (n 2). Arguably, the pro-privacy interfaces might also introduce misleading practices. I offered a possible analysis based on the sources available in section 4.2.2(2).

[761] P Marsden and R Podszun, 'Restoring Balance to Digital Competition - Sensible Rulse, Effective Enforcement' (2020) Konrad-Adenauer-Stiftung, Berlin, 40; *Facebook case* (n 2).

(2) If we limit the harvesting of data, could we result in the 'quiet life' exploitation?

In dynamic industries, competition could be depicted as a race to develop new products or replace existing technologies through innovation. Winners of this race have achieved an undisputed leadership position in several product markets. However, they must continuously innovate otherwise they could be overtaken by the next successful innovative product. Hence, in a data-driven economy, it becomes apparent that data enhances economic competitiveness and drives innovation.[762] As discussed, Google and Apple introduced plans to limit collection of data, by reducing cookies. Here, a short overview is provided that explains how such conduct could hinder innovation.

Google's Privacy Sandbox and Apple ATT initiatives aim to reduce data collection and might limit the personalisation of advertising. In fact, the concept of minimising data collection is a cornerstone of data privacy law.[763] Based on this, privacy could act as a quality parameter with companies competing to offer more protective privacy features. Recently, the US Department of Justice, Antitrust Division suggested that reducing privacy allegedly reduces quality and exploits users:

> "[b]y restricting competition in search, Google's conduct has harmed consumers by reducing the quality of search (including on dimensions such as privacy, data protection, and use of consumer data)."[764]

Google's Privacy Sandbox and Apple ATT initiatives are labelled as pro-privacy, allowing consumers to enjoy the quality of privacy protection. However, the proposed interfaces are not going to limit online tracking. Both Google's Privacy Sandbox and Apple's ATT do not ban the use of first-party data for purposes of targeted advertising. As both Google and Apple have access to a substantial range of personal data, they might have an incentive to close off completely their advertising markets, which might be regarded as another form of online advertising.[765] This conflict could result in Google and Apple acquiring further data, allowing

---

[762] Daniel F Spulber, Antitrust and Innovation Competition [2023] Journal of Antitrust Enforcement 5.

[763] GDPR (n 57) article 5(1)(c); 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658); Geradin, Katsifis and Karanikioti (n 624).

[764] US Dep't of Justice, 'Justice Department Sues Monopolist Google for Violating Antitrust Laws' (2020), <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws> accessed 2 January 2021.

[765] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini, 'How Can and Would People Protect from Online Tracking?' (2022) 1 Proceedings on Privacy Enhancing Technologies 105.

them to use unfair and exploitative practices and hinder innovation, thus enjoying the quiet life as monopolists.

Given that, Italianer used the example of the innovativeness of a product as a proxy to attract and retain consumers, referring to this phenomenon as an unfair lock-in.[766] In other words, the interfaces of Google and Apple could introduce a dramatic reduction of allowances for tracking and might result in consumers exploitation. However, that is not to indicate that by phrasing-out third parties, Google could exploit its users. Instead, it was suggested that the prohibition of third-party cookies in Chrome could potentially enhance the dominance of Facebook and Google as they already possess direct access to first-party audience data.[767] Indeed, after the ban on third-party cookies, Google is set to be the sole platform that retains the collected data, storing it directly on the browser itself. This data will be processed and analysed securely through the Privacy Sandbox initiative**.** The CMA expressed significant concerns that Google's dominant position could lead to potential users' exploitation by limiting users's choices regarding how their data is used for advertising purposes.[768]

This lack of substantial choice could further strengthen Google's market power and potentially harm competition and user privacy in the digital advertising industry. Particularly, Google aims to develop Privacy Sandbox taking into account users' privacy and experience, and Privacy Sandbox's impact on competition in digital advertising.[769] Yet, the CMA can open its investigation into the practices and impose interim measures in future if necessary, including any potential chances in offered trading conditions.[770] For instance, Google's pro-privacy policy amendment may have a significant effect on users, notwithstanding the fact that the policy change is ambiguous and difficult to estimate.[771] Google might introduce more invasive methods of data collection, requiring users to provide more of their personal

[766] Alexander Italianer, 'Innovation and Competition' (2015) International Antitrust Law & Policy, Competition Law Institute < https://www.fordham.edu/download/downloads/id/11451/FCLI2018_Conference_Day1_CLEMaterials_asof6September2018_v_1.pdf> accessed 17 May 2022.

[767] 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658).

[768] ibid.

[769] 'The path forward with the Privacy Sandbox' (n 668).

[770] See, Google (n 659); CMA (2023) (n 659).

[771] The CMA keeps monitoring the inventive. See, particularly, CMA (n 2023) (n 659).

data to use Google's products or services. The Privacy Sandbox interface may also restrict data consumption, with users having a limited access to free content. Google has been admonished for exploiting its market dominance to prefer its own services. This could result in negative effects on competition law and innovation, as consumers might be put in a difficult position, as consumers might feel more pressure to give up their personal data or experience risk of being lock out of certain digital platforms or services.

4.3. Privacy justifications in anticompetitive proceedings

The European approach to privacy protection within the context of competition represents a nascent evolution from separatism stance towards a form of integration that has been labeled as such. As demonstrated above, the Commission has gradually considered privacy in competition law assessments. This thesis turns to discuss to what extent undertakings could rely on improvements of privacy to avoid anticompetitive liability, within Article 102 TFEU.[772] Though this theory is in its early stage, there are questions about whether the increased protection for an individual's data privacy could justify otherwise anticompetitive conduct. This is one of the most nascent interactions on the horizon between competition law and data privacy law. To scrutinise the findings, the recent developments introduced by Google and Apple are discussed.

4.3.1 Efficiency defences and data privacy

4.3.1.1. Efficiency defences: overview

Efficiency defences rely on the positive competitive effects resulting from anticompetitive business practice.[773] The inherent efficiency nature might be assessed in the case of Microsoft, concerning a tied Windows Media Player product to its operating system.[774] The Microsoft defence was based on an argument that trying two products resulted in a cost-saving since it was no longer required to set up a different channel for media player distribution. Hence, customers would face a decrease in price, as well as spending less time installing a media player channel. However, the Commission indicated that the argument on efficiency could be potentially irrelevant, as the software cost remains low and might be

[772] A Gorecka, 'The Other Side of the Coin: Privacy Justifications in Anticompetitive Proceedings under Article 102 TFEU' (2022) 9(2) North East Law Review

[773] Anna-Lena Baur, 'Analysing the Commission's Guidance on Enforcement Priorities in Applying Article 102 TFEU — An Efficiency Defence for Abusive Behaviour of Dominant Undertakings? ' (2012) 19 (3) Maastricht Journal of European and Comparative Law 1.

[774] See, *Microsoft* (n 252).

replicated with little effort.[775] The Commission focused on the different aspects, including innovation and consumer choice rather than the efficiencies. The usage of free digital services and products might be disseminated without any effort from users. A key issue is what weight is given to efficiency standards: while economics considers social welfare,[776] EU competition law focuses on consumer welfare.[777] Economic efficiency is not the sole objective considered by enforcement authorities. Firstly, EU competition law has the central objective of promoting economic integration between the different Member States.[778] The overarching goal of the EU was indeed the creation of a single market, where intra-community trade barriers would be abolished.[779] The case of *Consten and Grundig* points out that the integral market might have been compromised if an agreement between undertakings was designed to partition markets along national lines.[780] Geradin demonstrated that such an argument might be supported by the decisional practice of the Commission, which emphasises the application of per se prohibition to different conducts of dominant firms.[781] Others lamented that the rigid and formalistic Commission's approach indicated that the EU was unable to consider future demands for innovation.[782]

The case law appears to demonstrate a twofold nature of efficiency arguments. Firstly, efficiency arguments should not be general, theoretical or vague, and should not rely on the commercial interests of undertakings.[783] Moreover, the CJEU established in *Post Danmark*

---

[775] A Andreangeli, 'Case note on T-201/04, Microsoft v Commission, Judgment of 17 September 2007' [2008] Common Market Law Review 863.

[776] Bishop and Walker (n 169) 24.

[777] ibid, 24.

[778] Claus Dieter Elherman, 'The Contribution of EC Competition Policy to the Single Market' [1992] Common Market Law Review 257, 257.

[779] Consolidated Version of the Treaty on European Union, 2010 OJ C 83/01, article 3.

[780] Joined Cases 56/64 and 58/64, *Consten-Grundig* ECLI:EU:C:1966:41; see also Case 262/81, *Coditel SA, Compagnie générale pour la diffusion de la télévision, and others v Ciné-Vog Films SA and others ('Coditel II'),* EU:C:1982:334.

[781] Damien Geradin and Monika Kuschewsky, 'Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges' (2014) 37 World Competition 69.

[782] James Ponsoldt and Christopher David, ''Comparison between U.S. and E.U. Antitrust Treatment of Tying Claims against Microsoft: When Should the Bundling of Computer Software Be Permitted' (2007) 27 Northwestern Journal of International Law & Business 421.

[783] *Google Search (Shopping)* (n 192), para 553.

that there needs to be a causal link between the conduct and the alleged improvements.[784] Also, the CJEU insisted on the consumer choice benefits, claiming efficiency benefits emanating from the conduct should not lead to harmful competition in that market.[785] The CJEU's approach might be quite symmetrical —actual or potential anticompetitive effects need to be demonstrated beyond purely hypothetical considerations, such as the efficiencies.[786] The Court appears to follow a strict consumer welfare approach,[787] with the consideration that a dominant undertaking might not legitimately protect their commercial interest. Also, the Court developed a system of pseudo-hierarchies while dealing with efficiency arguments.[788] For instance, in *Google Search (Shopping)*, the CJEU explained that generating efficiency by improving consumer experience did not help Google in justifying its conduct, as the conduct materialising the improvement led to harming competition by reducing shopping services available to consumers.[789] Again, the Court opted to triumph consumer choice over welfare increases. Generally, it might be sufficient to assume that increased consumer welfare is justified as anticompetitive conduct. In the reverse scenario, increases in consumer welfare does not result in better consumer choice, rendering the argument inadmissible.[790] Such consideration reaffirms that EU competition law remains under the influence of ordoliberalism; competition is considered as a vehicle ensuring competitive freedom intended to foster consumer welfare though maintaining open choices.[791]

4.3.1.2. Efficiency defence and privacy-related harms

In the light of the above discussion, the question remains: is it desirable to maintain privacy considerations as a recognisable efficiency argument in EU competition law? In the

---

[784] Case C-23/14, *Post Danmark A/S v. Konkurrencerådet (Post Danmark II)* EU:C:2015:651; 6 September 2017

[785] ibid, see also *Servizo Elettrico Nazionale* (n 81).

[786] *Post Danmark II* (n 784) para 65.

[787] *Irish Sugar plc* (n 753).

[788] *Microsoft/LinkedIn* (n 90).

[789] *Google Search (Shopping)* (n 192) para 566-572.

[790] *Microsoft/LinkedIn* (n 90).

[791] Robertson (n 522) 161; Valletti and Caffarra (n 353); C Baldwin and C Woodard, 'The architecture of platforms: a unified view' in Annabelle Gawer (ed) *Platforms, Markets and Innovation* (Edward Elgar Publishing 2009) 19; Christian Alhborn and Carten Grave, 'Walter Eucken and Ordoliberalism: An Introduction from a Consumer Welfare Perspective' (2006) 2 Competition Policy International, 199/200.

consideration of this thesis, it is likely that competition law assessment would increasingly consider privacy as an efficiency argument. There exist two reasons leading to this conclusion.

Firstly, to ensure a healthy market function, efficiency[792] and innovation are vital.[793] Amato indicated that the efficiency standard is a synonym for consumer welfare.[794] Article 101(3) TFEU indicated that consumers should receive a fair share of the resulting benefit.[795] Yet, in the broader consideration, Ahdar argued that an efficiency-only model for competition could fail to disregard value judgement.[796] This is because such a singular focus on efficiency may lead to issues of subjectivity and value judgments, particularly by disregarding distributional considerations in decision-making. In the application of the efficiency defence, it is necessary to counterbalance the advantages of the conduct to show their efficiency and consumer benefits.[797] This ruling indicated that when a dominant company succeeds in the market because of its superior efficiency, this achievement is not inherently considered as an abusive practice. If the company meets all the legal criteria related to efficiency, its behaviour is justified. Nazzini claimed that this approach is doubtful, as not complying with the Guidance.[798] In his consideration, the Guidance requires the net effect on consumer welfare to be at least neutral, unlike the *British Airways* case's approach to emphasise a benefit on consumers. However, in *Post Danmark*, the CJEU held that the burden falls on the dominant company to demonstrate that the efficiency improvements arise from the conduct in question will outright any possible adverse impact on competition and consumer well-being in the affected markets.[799] Furthermore, it should be established that their actions are essential for realising these efficiency gains and that they do not eliminate effective

---

[792] Guidelines on the assessment of horizontal mergers (n 216) para 76; Geradin and Kuschewsky (n 781) 315.

[793] Guidance on the Commission's Enforcement Priorities in Applying Article 82 (n 87).

[794] G Amato, *Antitrust and the Bounds of Power: The Dilemma of Liberal Democracy in the History of the Market* (Hart Publishing 1997) 95–129

[795] O Brook, 'Struggling With Article 101(3) TFEU: Diverging Approaches Of The Commission, Eu Courts, And Five Competition Authorities' (2009) Common Market Law Review 121.

[796] R Ahdar, 'Consumers, redistribution of income and the purpose of competition law' (2002) 23 European Competition Law Review 341, 349–352

[797] *British Airways* (n 229) para 69.

[798] Nazzini (2009) (n 744) 306-309.

[799] *Post Danmark* (n 277) para 42.

competition by eliminating most or all of the existing sources of actual or potential competition.

Diminishing privacy arguments as factors enhancing efficiency represents a myopic consideration of innovation. The digital economy demonstrates a need for dynamic efficiencies (innovation), stimulating dynamic markets, while diminishing marginal returns. Innovation should not be ignored by competition authorities, as it is unquestionably a key driver for competition. This is especially the case for platforms establishing an ecosystem of modules, capable of supporting machines, users, and sectors using data.[800] This capability provides that platforms regulate through a code in a Lessigian manner.[801] Platforms often manage complex expectations, including increased privacy levels of users. Any amendments to platform practice could remediate any market failure. However, platform ecosystem amendments should not be assessed with suspicion; assuming as if every amendment was a harmful act seems premature.

There is also criticism corresponding with the debate condemning the incorporation of non-economic considerations into competition law assessment.[802] Some recommendations attack any attempts to facilitate privacy into competition law assessment, contending that its unscientific nature could lead to dystopic competition assessments.[803] In my consideration, narrow efficiencies would reflect ambiguity and might influence politics. Then, the question of how to support innovation goes either to Arrowian or Schumpeterian assumptions.[804] In simple terms, consumer welfare and efficiency might be interlinked, while considering privacy concerns in competition law assessment. With the Charter implementation, the Commission is bound to facilitate privacy breaches.[805] Due to a reluctance to intervene in cases with the direct excessing pricing harm, there are equally no reasons why the lower

---

[800] Annabelle Gawer, 'Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age' (2021) Innovation, Organization & Management 1.

[801] Lawrence Lessig, 'Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501.

[802] William Baxter, 'Responding to the Reaction: The Draftsman's View' (1983) 71 California Law Review 618.

[803] Geoffrey Manne and Dirk Auer, 'Antitrust Dystopia and Antitrust Nostalgia' (2021) Truth on the Market <https://truthonthemarket.com/author/manneauer/> accessed 7 November 2022.

[804] Schumpeter (n 19); Arrow (n 19).

[805] Lamadrid (n 169).

privacy available to end-users should be a means for competition authorities to intervene.[806] Furthermore, Abbott argued that typically, from the perspective of error-cost analysis, examining complex issues like privacy-related efficiency gains does not meet the cost-benefit evaluation criteria.[807] Yet, by considering the rapid development of digital products and services, such issues are likely to occupy enforcers for years. Moreover, it is also suggested that due to an increased level of complexity in modern economics, there are concerns about the sustainability of simplicity in competition law.[808] Therefore, relinquishing administrative and judicial responsibilities when confronted with technical intricacies can lead to unpreparedness for the future and should be discouraged.[809] The question indicates that the gap is not necessarily whether competition law's application is inadequate in assessing the privacy concerns, but the problem lies within the GDPR application as it is lacking an adequate regulation. Public policy should not be based on the assessment of efficiency and competition since competition law should not be extended beyond its natural limits. This point would be indicative that market forces, as well as competition law, are not adequate in promoting the level of privacy.

Secondly, if we assume that privacy-related harms could be systematically considered by competition analysis, then incorporation of privacy would require a coherence perspective. The previous section proved a possibility of delineating theories of harm based on decreased consumer privacy. It would be inappropriate to consider privacy's negative considerations while not allowing any counterarguments based on the same.[810] Similarly, the EU is currently facing a transformation: a digital and a green one.[811] Recently, the Commission prohibited an

---

[806] Lamadrid (n 169)

[807] Alden Abbott, 'Broad-Based FTC Data-Privacy and Security Rulemaking Would Flunk a Cost-Benefit Test' (*Truth on the Market Blog*, 13 October 2021) <https://truthonthemarket.com/2021/10/13/broad-based-ftc-data-privacy-and- security-rulemaking-would-flunk-a-cost-benefit-test/> accessed 24 November 2023.

[808] Timothy Brennan, 'Is complexity in antitrust a virtue? The accuracy-simplicity tradeoff' (2014) 59 (4) Antitrust Bulletin 827.

[809] Frank Pasquale, 'Paradoxes of Digital Antitrust' (2013) Harvard Journal of Law & Technology Occasional Paper Series, July 2013.

[810] Christine Wilson, 'Breaking the Vicious Cycle: Establishing a Gold Standard for Efficiencies' (*Bates White Antitrust Webinar,* 24 June 2020) <https://www.ftc.gov/system/files/documents/public_statements/1577315/wilson_-_bates_white_presentation_06-24-20-_final.pdf> accessed 7 November 2022.

[811] Jurgita Malinauskaite, 'Competition Law and Sustainability: EU and National Perspectives' [2022] J Eur Compet 336.

agreement between manufacturers that restricted development of less-polluting emission systems.[812] However, there is also evidence of a potential competition law and sustainability clash, as pertinent in the promulgation of the new horizontal guidelines.[813] However, there are more reasons to start scrutinising the equivalent debate in terms of competition and privacy. The intersection between competition law and privacy protection is complicated and goes beyond the boundaries of competition law enforcement. The concept of privacy is a social practice and remains difficult to be defined.[814] Users can rarely contract with the platform providers on the level of privacy, as it is impossible for consumers to negotiate offered privacy levels. However, the digital society is evolving and introducing new threats and vulnerabilities, making the relationship between data protection and competition law even more complex. Competition law, at its core, is concerned with market power that might negatively impact consumer welfare; the Commission Guidelines determined that consumer welfare is considered by assessment of price and other factors, including innovation, choice, and quality.[815] This will be considered in light of Google's Privacy Sandbox or Apple's ATT initiatives, where this thesis argues that both strategies raise concerns about anticompetitive conducts to exploit end-users.

It remains unclear if Apple or Google could justify their initiatives as satisfying efficiency arguments. For example, Apple blocking the third-party apps from accessing data needed for the app personalisation, might be viewed as a refusal to supply, as per *Google Search (Shopping)*.[816] Apple, in the CMA's inquiry, indicated that its business did not engage in third-

[812] Case AT.40178, *Car Emissions* [2021].

[813] EU Commission, 'A European Green Deal' < https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en> accessed 17 May 2023; Klaudia Majcher and Viktoria HSE Robertson, 'Doctrinal Challenges for a Privacy-Friendly and Green EU Competition Law' [2022] SSRN < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778107> accessed 17 May 2023.

[814] IS Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' [2013] Int Data Priv 74, 78.

[815]Guidance on the Commission's Enforcement Priorities in Applying Article 82 (n 87) para 19.

[816] *Google Search (Shopping)* (n 192); Geradin, Katsifis and Karanikioti (n 624); Christophe Carugati, 'The Antitrust Privacy Dilemma' (2021) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968829> accessed 7 November 2022; Daniel Sokol and Feng Zhu, 'Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates' (2021) USC Law Legal Studies Paper No. 21-27.

party tracking.[817] Hence, Apple considered the changes affecting the third-party data collection as beyond the scope of their concern. However, Apple's practice might continue to degrade user privacy, as does Google's Privacy Sandbox initiative. Both infrastructures might correspond to enlargement of first-party tracking, which corresponds to increasing market power for both Apple and Google in the personal advertising market.

As discussed above regarding theories of harm, Apple could potentially argue that the ATT introduced efficiencies through proving users' privacy, as a potential quality metric.[818] The fact that many online consumers changed their habits towards the cross-tacking apps after ATT's introduction could signify that.[819] ATT interfaces, as per *Post Denmark I,* demonstrates that consumer choice would not be constrained. Essentially, ATT does not prohibit cross-app tracking at all. However, consumers might achieve more benefits from personalised advertising through cross-app tracking — they are free and in a better position to consent to it. Essentially, Apple's ATT does not ban personal advertising but has evolved from the default automatic tracking to allowing consumer the choice of whether to consent to third-party tracking. In fact, Apple's initiative could empower the consumer choice.[820] The choice design architecture behind tracking is that the consumer is presented with the opt-in scenario — and this should not overrule the justifications of efficiency. Apple has also taken steps to allow app developers to prompt providing information regarding tracking.

Google's attempts to justify efficiency arguments under its Privacy Sandbox initiative appear weak. Here, the main reason lays in the theory of harm construction: it remains unclear if Google could stop utilising third-party tracking to inform its advertising businesses. This could be seen as demonstrating a possibility of first party-tracking discrimination for which

---

[817] CMA, 'Mobile ecosystems' (2022) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL__.pdf> accessed 2 September 2022.

[818] *Post Danmark* (n 277).

[819] ICO and CMA, 'Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO' (2021) 19 <https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf> accessed 17 June 2021; See also, R Whish, 'The New Competition Tool: Legal comparative study of existing competition tools aimed at addressing structural competition problems, with a particular focus on the UK's market' (European Commission, 2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/kd0420573enn.pdf> accessed 14 September 2021

[820] See *Google Search (Shopping)* (n 192).

Google has already been fined in the EU. Also, by removing cookies, Google reduces consumer choice, especially for users who value online advertisements. It remains unclear if Google is preparing to open any different alternative, equitable on the same level of personalisation. As the current case law stands, Google's pro-privacy product improvement might not be justified under the efficiency defence if its improvement reduces consumer choice.[821]

4.3.2 Objective justifications and privacy

4.3.2.1. Objective justifications: overview

Another route to avoiding liability under European competition law is through objective justifications — the external factors, exonerating the exclusionary abuse under Article 102 TFEU.[822] In fact, there are clear distinctions between efficiencies and objective justifications,[823] and the existence of these routes enables for avoiding liability for competition law abuse in certain instances. The discussion about objective justification could be viewed as an alternative approach to address market failures,[824] which exempt a conduct from breaching Article 102 TFEU. From the Commission's prospect, only a limited number of non-competition policies, often referred to as external to competition law policies, can be taken into considerations during competition law assessment. The examples of external policies, that are, in fact, non-competition law policies, include the protection of employment,[825] media pluralism,[826] environmental protection,[827] or regional development[828] are considered as legitimate factors when applying Article 101(3) TFEU to reviewed

[821] CMA: 'Decision to accept commitments offered by Google' (n 643); CMA (2023) (n 562).

[822] Pablo Ibanez-Colomo, 'The (growing) role of the Guidance Paper on exclusionary abuses in the case law: the legal and the non- legal' (*Chillin'Competition Blog*, 9 February 2022) <https://chillingcompetition.com/2022/02/09/the-growing-role-of- the-guidance-paper-on-exclusionary-abuses-in-the-case-law-the-legal-and-the-non-legal/> accessed 17 August 2022.

[823] Case C-549/10 P *Tomra Systems ASA and Others v European Commission* ECLI:EU:C:2012:221.

[824] Eric Gippini-Fournier, 'Resale Price Maintenance in the EU: In Statu Quo Ante Bellum?' in Barry Hawk (ed), *International Antitrust Law and Policy* (Fordham 2009).

[825] See for example, *Remia* (n 184); *Van Landewyck* (n 184).

[826] See for example, *EBU/Eurovision System* (n 185).

[827] See for example, *Carbon Gas Technologie* (n 186); *KSB/Goulds/Lowara/ITT* (n 186); *ARGEV, ARO* (n 186).

[828] *Ford Volkswagen* (n 187).

agreements. However, the Commission suggested that there could be alternative ways to assess concerns less restrictive to competition law.[829]

On the assessment of coordination between policies, it is important to provide that EU competition law does not exist as a stand-alone statute but is a part of a larger framework — the TFEU. Over the issue of the influence of external policies on competition law, the works of Townley or Van Rompuy identified four potential scenarios for coordination of EU external policies with competition policy.[830] I considered these scenarios in Chapter 2, while discussing the potential coordination between competition law and privacy protection. Here, this is reiterated. Firstly, the TFEU enables for the potential external policy value to override and exclude competition policy, as per Article 346(1) TFEU. Secondly, competition law could act as a complementary process if violations of competition law could be balanced. It is noted that an incidental consideration of external to competition law policies may be used to find competition law infringement. Here, competition law breaches would not have existed if that external, to competition law, policy was not breached. Thirdly, the Treaty introduced a 'policy-linking' or 'cross-sectorial' clauses, which requires competition enforcement to consider other polices in "definition and implementation."[831] The last scenario relates to the silence of the TFEU: it will be for the case law to determine and ensure a consistent interpretation across various policies.[832]

The EU competition law approach to objective justifications could be a subject of criticism due to practical problems in its application.[833] For example, Nazzini suggested that there are recognisable practical difficulties in making a distinction between the anticompetitive conduct and its justifications.[834] Although this view could be seen as being less relevant in the light of present developments, the notion of objective justifications remain undiscussed: there are no practice examples where an anticompetitive conduct could have been

---

[829] Case AT.39984, *Romanian Power Exchange/OPCOM* [2014].

[830] Van Rompuy (n 181) 227; Townley (n 159) 52-53.

[831] Townley (n 159) 53.

[832] *CILFIT* (n 183).

[833] Renato Nazzini, 'The Wood Begun to Move: An Essay on Consumer Welfare, Evidence and Burden of Proof in Article 82 cases' (2006) 4 European Law Review 518.

[834] Case C-53/03, *Syfait and Others* [2005] ECLI:EU:C:2004:673, Opinion of AG Jacobs, para 72.

objectively justified. The CJEU remains skeptical regarding anticompetitive conduct serving as a public objective,[835] demonstrating that private undertakings are unsuited to consider the objectives in the remits of public regulators.[836] In other words, EU competition law does not see such regulatory vigilantism as complimentary.

4.3.2.2. Privacy as an objective justification

In this section, I examine the treatment of privacy as an objective justification in the light of the above analysis, arguing that it remains likely that large digital undertakings could apply pro-privacy incentives to exonerate anticompetitive liabilities.

In the case of privacy protection, neither national laws nor EU competition law recognises the general right to acknowledge privacy protection in the proactive implementation of Article 102 TFEU. In the *Facebook case,* AG Rantos emphasised that conduct adhering to data protection law might still breach competition law while violating GDPR standards does not inherently imply a breach of competition rules.[837] Despite the common denouncement that the relationship between competition law and privacy is complementary, the relationship between competition and data privacy is much more multi-faced and nuanced.

Article 102 TFEU does not provide a list of conditions which would justify an abusive conduct. However, the CJEU emphasised that a dominant undertaking can rely on some 'objective justifications' while defending that its conduct did not breach Article 102 TFEU.[838] Firstly, a dominant undertaking does not infringe Article 102 TFEU if it protects its commercial interests.[839] Secondly, the behaviour will not be deemed as unlawful under Article 102 TFEU if it is "dictated by public interest considerations".[840] However, the invocation of privacy as a ground for objective justification could be problematic due to the

---

[835] Case T-30/89, *Hilti v Commission* [1991] ECLI:EU:T:1991:70, para 118.

[836] Niamh Dunne, 'The Role of Regulation in EU Competition Law Assessment' (2021) LSE Legal Studies Working Paper No. 09/2021 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871315> accessed 6 November 2022; see also Giuseppe Colangelo and Mariateresa Maggiolino, 'Antitrust über alles. Whither competition law after Facebook?' [2019] World Competition Law and Economics Review 1.

[837] *Meta Platforms, Opinion of AG Rantos* (n 85) para 23.

[838] Marco Botta, 'Sanctioning unfair pricing under Art. 102(a) TFEU: yes, we can!' [2021] European Competition Journal 1, 27.

[839] *United Brands* (n 195) para 189.

[840] Botta (n 726) 27.

relationship between sector-specific regulation and competition law. The CJEU in *AstraZeneca* discussed that compliance with other legal orders does not relate to whether an undertaking has abused its dominant position.[841] In this respect, any violation of other legal orders do not imply immediately the competition laws infringement. In this reasoning, it would be impossible for a dominant undertaking to seek justification for its anticompetitive conduct based on compliance with data privacy law, such as the GDPR. Such reasoning seems plausible since it would avoid extending competition law rules to capture conducts and harms outside the scope of competition law. However, the latest case law appears to blur this argument. For example, in *Latvian Copyright Society,* the general Court argued that legislative measures are capable of influencing competition law analysis.[842] Furthermore, the case of *Slovak Telekom* emphasised that "...a regulatory obligation can be relevant for the assessment of abusive conduct..." where an undertaking is subject to specific sectoral obligations.[843]

Here, I note a tension between these judgements from the perspective of privacy consideration. Firstly, within the meaning of *AstraZeneca,* Article 102 TFEU disregards the position of an undertaking and the regulatory regime in question. Recently, *Slovak Telekom* and *Latvian Copyright Society* pointed towards an apparent relevancy of a regulatory regime in question for purposes of Article 102 TFEU applicability. However, it remains unclear if the tendency of such reconciliatory reading might suggest that a regulatory context could form a part of an anticompetitive context. As per *AstraZeneca*'s judgement, we should disregard any potential regulatory breach as a part of competition law assessment, considering breach data privacy law as irrelevant for the purposes of competition law. Conversely, in *Google Search (Shopping) case*,[844] the Court considered external-for-competition-law-policy for the sake of completeness of assessment. This stage is further confused by AG Rantos, who opined that incidental considerations of external-for-competition-law-policies might be

---

[841] *AstraZeneca* (n 99) para 132.

[842] Pablo Ibanez-Colomo, 'GC Judgment in Case T-814/17, Lithuanian Railways – Part I: object and indispensability' (*Chillin'Competition Blog*, 1 December 2020) <https://chillingcompetition.com/2020/12/01/gc-judgment-in-case- t%E2%80%91814-17-lithuanian-railways-part-i-object-and-indispensability/> accessed 26 March 2022; *Latvian Copyright Society* (n 698).

[843] *Slovak Telekom* (n 278).

[844] *Google Search (Shopping)* (n 192).

relevant, as without the infringement of that policy — competition law would not exist.[845] On the same note, in the *Facebook case,* the CJEU had an adamant position in recognising the intersection between competition law and privacy, which is similar to one adopted by AG Rantos.[846] The Court offered a nuanced approach towards the integration of external-for-competition-law-policies, but not to a goal, standard or indicator which could be applied across the EU competition law cases. Hence, to consider the influence of a regulatory regime on the competition assessment of a dominant undertaking's activity, the latter does not need to be subject to that regime.

I suggest here that there are noteworthy implications for the role of privacy as objective justification. If we assume that *AstraZeneca's* approach remains appropriate, the assumption is that Apple and Google should not reply to arguments of compliance with GDPR to avoid anti-competitive scrutiny. In this respect, a theory of harm should not be established on the grounds of infringement of other legal rules. According to the CJEU principles, in an antitrust assessment, it is required to prove that a dominant undertaking employed methods beyond the scope of competition on the merits.[847] To establish this, in *the Facebook case,* the CJEU had to consider the specific circumstances of the case, applying the relevant legal and economic context. Hence, the assessment of non-compliance of a particular behaviour with GDPR, when examined in the context of the entire case rather than in isolation, can serve as a crucial indicator of whether that conduct involves the use of fair competition methods.[848] In other words, even if the development of the digital economy resulted in competition authorities demonstrating an increased level of interest about privacy-related theories of harm, this should not constitute an expansion of the competition legal order to that of other areas of law, such as data protection, for the simple reason that competition law relates to tacking harms caused by market failures which negate the functioning of the market. However, the assumption made here is that, in the light of the recent developments in legal cases, the Court could consider privacy-related harms when they influence the theory of

[845] *Meta Platforms, Opinion of AG Rantos* (n 85) para 24

[846] *Meta Platforms* (n 41) para 62.

[847] See *TeliaSonera Sverige* (n 233); *Post Danmark II* (n 784), *Intel* (n 223); *Case C-307/18, Generics (UK) and Others v. Competition and Markets Authority, EU:C:2020:52; 25 March 202*1, *Deutsche Telekom* (n 262).

[848] *Meta Platforms* (n 41) para 47.

harm - then the CJEU should also consider them when scrutinising claims of objective justifications.

To pursue this further, when a dominant undertaking is found to breach Article 102 TFEU, an undertaking could: 1) argue that their conduct is competition-enhancing; or 2) demonstrate that their conduct is incapable of demonstrating anticompetitive effects.[849] In this respect, if we assume that conduct has been pro-competitive, then such a situation would amount to the ancillary restrain.[850] However, if an undertaking argues that its anticompetitive conduct pursues non-economic objectives in a proportionate manner, the *Wouters* case suggests that such conduct could not be viewed as an intersecting ideas.[851] Hence, the question remains as to whether platforms could argue that their anticompetitive conduct of infringing (or promoting) privacy might be seen as pro-competitive. The answer should remain negative. The question should be answered through the involvement of government power as to whether it is legitimate to pursue non-economic considerations. Accordingly, Google and Apple can only rely on their non-economic considerations if they are granted regulatory powers. This conclusion might still be questionable as EU competition law does not see such regulatory vigilantism as complimentary.

Discussing the cases of ATT and Privacy Sandbox, their relationship with an apparent objective justification remains blurred. There is no settled case law which applies data protection as a justification in antitrust case law, and such possible scenarios might remain rare. Wiedemann discussed the French *Apple ATT case* as an example of a possible objective justification application.[852] In the *Apple ATT case,* the Autorité de la Concurrence determined that Apple's implementation of the ATT interface served as a legitimate objective, as Apple's long-term strategy has included a strong emphasis on privacy, which has aligned with user demand for a high level of privacy.[853] This policy was not seen as infringing antitrust, as

---

[849] Ibanez Colomo (2021) (n 289)

[850]Case T-112/99 *Métropole Télévision (M6) v Commission* EU:T:2001:215; Case T-111/08 *Mastercard v Commission* EU:T:2012:260.

[851] Case C-309/99 *Wouters v Algemene Raad van de Nederlandse Orde van Advocaten*, [2002] E.C.R. I-1577.

[852]Wiedemann (2023) (n 73).

[853] Autorité de la Concurrence, Decision 21-D-07 of 17 March 2021 paras 144-147 <https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2021-04/21d07_en.pdf> accessed 24 November 2023. (Hereinafter: French Apple ATT decision)

pursuing a legitimate commercial interest.[854] The Autorité de la Concurrence also assessed whether Apple's behaviour was proportionate to pursue such a goal,[855] taking into consideration the interests of the relevant parties involved. From Apple users' point of view, there was not any undue influence, but an increased transparency on the data processing purposes.[856] From the advertisers' perspective, Apple's imposed procedure is considered fair because it is standardised, making it objective and non-discriminatory.[857] Apple also waited with its ATT implementation to allow app producers an opportunity to adapt to the new policy. These factors were taken into consideration, allowing the Autorité de la Concurrence to conclude that the policy was reasonable and amounted to objective justification. Wiedemann indicated that this approach was holistic, focusing on both traditional competition law and relevant data protection rules.[858]

The French *Apple ATT* case might serve as a convincing approach.[859] However, the CJEU restricted the applicability of the 'legitimate business interests' defence by emphasising that this justification cannot be used when the true intention behind the conduct is to bolster and exploit the dominant market position held by the company.[860] Both incentives offered by Google and Apple could help the large digital undertakings to increase their market position by excluding the advertisers' access to data, as well as exploiting users through increased data protection. Hence, the question of whether this trade-off is considered abusive or if the data protection interests of the users take precedence is not solely an economic issue, but also a matter of normative judgment. At the time of writing, it remains unclear how the Commission will decide to take enforcement of actions against undertakings which promote product privacy as quality as an objective justification against their anticompetitive conduct at the EU level.

---

[854] French Apple ATT decision (n 853) para 147.

[855]ibid, paras 148-164.

[856] ibid, para 149.

[857] ibid, para 159.

[858] Wiedemann (2023) (n 73) 31.

[859] ibid.

[860] ibid.

4.4. Conclusions

In this chapter, I presented an overview of the exploitative theories of harms under Article 102 TFEU resulting from apparent privacy-related harms. Various theories of harm were explored in the context of user privacy breaches and their limits to existing competition law tools. This chapter has been limited to considering exploitative theories of harm as the growing digital economy has sparked apprehensions about the interplay between competition law and privacy, necessitating a more nuanced approach that reconciles these legal domains. Both areas of law share the common objective of preventing the exploitation of consumers' data and privacy. The analysis here demonstrated that in certain instances, privacy-related harms might constitute a violation of Article 102 TFEU.

In practice, the chapter demonstrated that it seems challenging to identify any clear complementarity or synergy between competition and data protection laws. Article 102 TFEU is wide-ranging, and its nature provides a non-exhaustive list of examples of conduct that might be seen as abusive. Given the broad scope of Article 102 TFEU, it cannot be excluded that privacy-related harms could potentially be considered as an instance of abuse, as privacy-related harms are broad in nature and might become identifiable as forming unfair trading terms, excessive data collection or the quiet life abuse. The determination of whether a particular behaviour qualifies as a prohibited abuse under Article 102 TFEU is always evaluated on a case-by-case basis. Competition law should intervene in conduct involving privacy-related theories of harm only if privacy-related harm relates to market failure, not to the breach of privacy rights itself. In other words, it is the conduct that not merely involves data mistreatment and breach of users' privacy, but the conduct must hurt competition. Reduction of privacy may not necessarily amount to a competitive issue; any reduction of privacy equally may not immediately breach data privacy law if the data processes comply with data protection law. A thorough examination is essential to assess whether a company's legitimate business interests can serve as a valid justification. It is crucial to determine whether the measures taken are both necessary and proportionate in pursuing a legitimate business model.

Chapter 5: Addressing Privacy Violations and Competition Law through Integration and Separation: can we achieve a nexus?

5.1 Introduction

At the level of competition law enforcement, I argued that Article 102 TFEU could use certain privacy-related infringements to trigger competition proceedings. The GDPR fails to acknowledge the long-term harms associated with personal data acquisition and remains silent on the theory of competitive harm. By recognising the aggregation of personal data as a potential source of market power, competition law enforcement might provide recourse where companies use their market power to inflict harm and degrade privacy. Even if we assume that platforms are aware of consumers' lack of engagement with privacy policies, large digital firms attempt to further fuel data-driven network effects and expand into related markets by imposing misleading practices. However, if more privacy-oriented terms are offered, we cannot be sure that privacy-sensitive solutions would not create further competition law concerns, where large digital companies abuse their market position.

To address such a complex interaction between competition law and data privacy law, a coherent approach to law enforcement is necessary. However, it is necessary to keep competition law and data privacy law enforcement as separate, even though privacy standards are relevant to competition analysis as a qualitative parameter. Essentially, maintaining the analytical independence of legal orders could contribute to the achievement of predictability.

In this chapter, I present a practical nexus between competition law and privacy protection. Section 5.2 focuses on mapping out the points of intersection between competition law and data protection, discussing why they deserve greater scrutiny. Importantly, I present two regulatory circles of a problem, recognising the limited scope of competition law in protecting the privacy of users. In this respect, I name the regulatory circles of the problem as the privacy-trap theorem. The theorem acknowledges the existence of privacy infringements as a proxy to trigger competition law assessment. The aim is to demonstrate that competition law could act as an effective practical tool for protecting privacy, but it is noted that competition law could only answer privacy-related concerns if they directly influence competition. Section 5.3 further explains the nexus between competition law and

privacy-related harms. The perceived incompatibility between competition and data privacy laws is mostly due to implementation issues. Often, these laws overlap and can be interpreted cohesively. Problems arise when dominant companies excessively collect personal data, risking market manipulation and user privacy. The ongoing privacy concern is tied to major digital corporations' practices. Based on the theorem, section 5.4 introduces a risk-based approach, acknowledging the limited scope for competition law in remediating privacy-related harms. Section 5.5 concludes the chapter.

5.2. Achieving a nexus between competition law and privacy: privacy-trap theorem

Article 102 TFEU could be seen as an open-ended provision, encompassing a broad list of possible exploitative practices.[861] Collecting, processing, and analysing personal data involved data protection and privacy issues that constrain the practice of the platform's use of data.[862] In this respect, privacy infringements could fall within the scope of competition law, as the use and collection of data through misleading practices could correspond to abuse of dominant position.[863] Essentially, to trigger Article 102 TFEU proceedings, this thesis argues that competition law is not capable of establishing mere privacy violations and prosecuting them as an infringement of competition law, as this is beyond the scope of its completeness as attributed by EU law, and inadmissibility of expansion of competition law.

This section presents the privacy-trap theorem, and develops this theory based on the findings presented in the previous sections (especially chapter 4), where the extensive data acquisition has been labeled as the main problem for both competition law enforcement and privacy protection. The privacy-trap theorem attempts to acknowledge the existence of privacy-infringement as a proxy to trigger competition law assessment, in instances where consumers are exploited through unfair terms and conditions, informational asymmetry, and the limited nature of GDPR. In such a scenario, I assume that the market for privacy protection is recognised. Here, consent is required, and individuals cannot consent to a precise purpose of data processions.

---

[861] *Deutsche Telekom* (n 262) para 173.

[862] See *Meta Platforms* (n 41).

[863] See *Facebook case* (n 2); *Meta Platforms* (n 41); *Meta Platforms, Opinion of AG Rantos* (n 85).

Second scenario refers to instance where the market for privacy protection has not been recognised. I use the examples of Google's Privacy Sandbox and Apple's ATT initiatives which have, arguably, introduced a better privacy protection for users. In the light of Article 102(a) TFEU, both Google and Apple could act as privacy regulators introducing false hope in regards protecting the privacy of digital users. It is noted that pro-privacy changes in product delivery could still be considered as unfair trading conditions. In both scenarios, it is noted that it is evident that the relationship between competition and data protection laws deserve greater scrutiny. However, even if the regimes overlap, this should not be seen as an expansion of competition law enforcement, for the simple reason that competition law relates to tacking harms caused directly inflecting the competitive equilibrium in a relevant market.

5.2.1. Scenario 1: there is a market for privacy protection

I present a model where the market for privacy protection exists but operates ineffectively and introduces several incentives for possible end users' exploitation and competition law infringement. The general problem is that in digital-consumer-oriented markets, consumers cannot adequately manage their data and privacy.[864] Consumers who attempt to become informed about the consequences of consenting to access online services and products fail to adequately assess the offered terms of conditions because of the informational asymmetry existing between them and online services and product providers. The data collection and potential privacy breaches appear to demonstrate Janus-faced features. The GDPR attempts to provide a set of rules supporting data subjects against any potential data protection. Simultaneously, many discussions have pointed out that the limited nature of its protection strengthens the data controllers' market dominance.[865] The analysis undertaken in this thesis suggests that the more data is collected, the knowledge acquired from its analysis might become largely distributed. In fact, consumers are worried about how the digital platforms are collecting and processing their data. I use the model of Facebook to

[864]BKartA, 'Wettbewerbskommission 4.0' (2019) 43 <https://www.bmwk.de/Redaktion/DE/Artikel/Wirtschaft/kommission-wettbewerbsrecht-4-0.html> accessed 17 May 2023; Akman (2022) (n 640); Fred H Cate and Viktor Mayer-Schönberger, 'Notice and Consent in a World of Big Data' (2013) 3 International Data Privacy Law 67; J Luzak, 'Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online' [2014] Privacy, Journal of Consumer Policy 547.

[865]Filistrucchi, Geradin, van Damme, and Affeldt (n 195) 302; Kerber and Zolna (n 715); Wiedemann (2021) (n 65).

take into consideration the costs of losing privacy, and deepening information asymmetry. Facebook's terms of use provide:

> "Sharing Your Content and Information you own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.
>
> [...]
>
> Our goal is to deliver advertising […] that is valuable to our users and advertisers. In order to help us do that, you agree to the following:
>
> 1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content […] served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.
>
> 2. We do not give your content or information to advertisers without your consent."[866]

Under the business models of digital platforms, users provide valuable data from which the digital companies could extract their profits.[867] Generally, Facebook's terms and conditions offer a limited scope of control over users' data; users can only control access to their data by other Facebook users. The situation is different in relation to Facebook's third parties (i.e. advertisers and infomediaries) collection of data. In that context, Facebook specifies that users might be able to opt out from tracking and targeted advertising. Here, Facebook only provides website links to European Digital Advertising Alliance, making it opaque for its users in relation to control over their own data. In other words, users face further difficulties in opting out from processing of their data by third parties. In this respect, consumers are given a false sense of control over their own data. Consumers are unaware of the value of

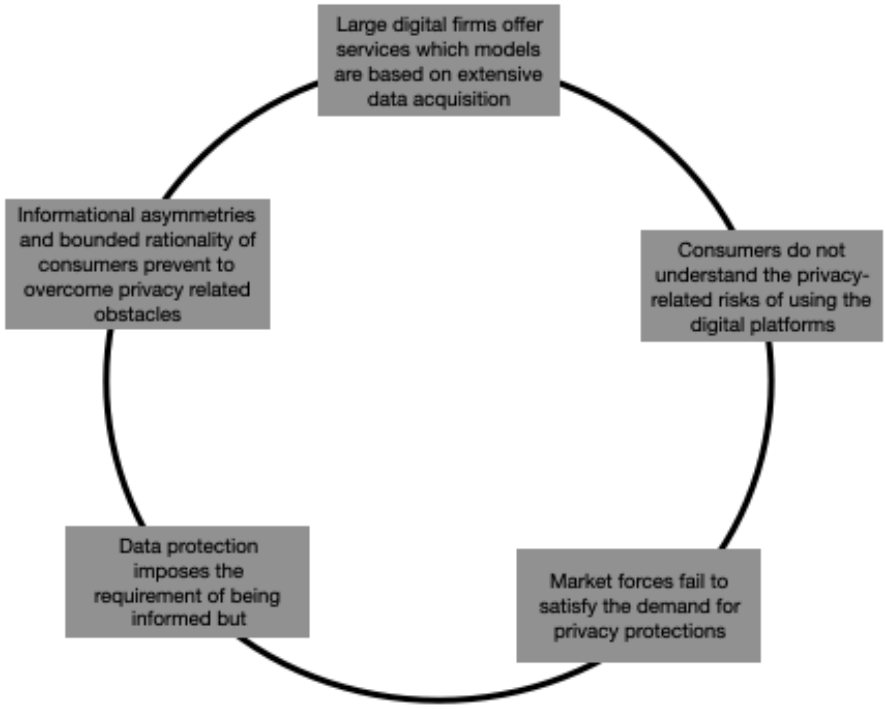
---

[866] Facebook, 'Terms of Service' <https://www.facebook.com/terms.php> accessed 1 November 2022.; see also Brendan Van Alsenoy and Valerie Verdoodt, 'From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms' (2015) Belgian Data Protection Authority 22 <https://kuleuven.limo.libis.be/discovery/search?query=any,contains,lirias1662185&tab=LIRIAS&search_scope=lirias_profile&vid=32KUL_KUL:Lirias&foolmefull=1&&lang=en> accessed 17 July 2020; Alessandro Acquisti and Ralph Gross, 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook', In Danezis G, Golle P (eds), *Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, vol 4258* (Springer, 2006).

[867] See Gal and Aviv (n 18) 9; Dan Costa, 'Facebook: Privacy Enemy Number One?' (2010) *PCMAG* <http://www.pcmag.com/article2/0,2817,2362967,00.asp> accessed 17 October 2021.

their personal data for Facebook and advertisers as they have no access to the information regarding the data value in the context of transaction with advertisers and infomediaries.[868] The reliance on data might vary between the digital undertakings, equally implying that competitive advantage varies across businesses and activities. The following phenomenon can be shown (figure 5.1) in the form of a vicious circle, which demonstrates that competition law could remediate privacy-related harms, only if the harm is directly linked to harming competition.

Figure 5.1: Vicious cycle in the 'market for privacy' conditions



Here, I demonstrate how concerns of competition law and privacy are interlinked. There is a lack of transparency users face when giving consent online. Arguably, markets do not provide as many privacy opinions as would be necessary to carer users' preferences. In fact, when it comes to joining to a social network, direct network effect leads to market concentration.[869] For example, the BKartA's *Facebook case* emphasises on the 'take it or leave it' nature of Facebook's terms and conditions — users have to either consent to the

[868] Botta and Wiedemann (2019) (n 415) 428; Giuseppe Colangelo and Mariateresa Maggiolino, 'Data accumulation and the privacy-antitrust interface: insights from the Facebook case' (2018) 8 (3) International Data Privacy Law 224; Colangelo and Maggiolino (2019) (n 836).

[869] *Facebook case* (n 2).

given terms or abstain from using the service.[870] Considering the role of data in creating a digital platform's value, the platforms rely on technology to aggregate services and content, allowing users to connect for purposes of sharing, transactions, or communicating. Hence, the potential privacy violation arising from an aggressive data acquisition is that Big Data connotes the concept of Big Analysis, which is a competitive danger. The sole discussion, in this respect, should be devoted to the concept of Big Analysis, which is a commercial practice based on acquired personal data, which allows digital undertakings to establish knowledge which could introduce anticompetitive conduct.

The approaches to measuring privacy from a competition perspective are at a nascent stage, but they appear to play a role in the integration of privacy consideration in competitive law analysis. Podszun argued that EU competition law contains a "principle of autonomy of economic actors".[871] It implies that independent and autonomous decision-making of market participants, including digital consumers, can and should be considered as a key concept of EU competition law. For example, a requirement of independence has been definite in various CJEU's cases on Article 101 TFEU. In *Suiker Unie,* the CJEU found that that:[872]

> "[t]he criteria of coordination and cooperation laid down by the case-law of the Court (...) must be understood in the light of the concept inherent in the provisions of the Treaty relating to competition that each economic operator must determine independently the policy which he intends to adopt on the common market including the choice of the persons and undertakings to which he makes offers or sells."

This formula has become established in case law in Article 101 TFEU.[873] Yet, the Court does not provide any indication that only possible horizontal indication might have been covered. The requirement for independence might be transferred to constellation involving applied digital abuse-of-dominance involving any horizontal and/or vertical relations. Particularly, for many business models, where data assume the role of contractual consideration, the right

---

[870] Bart Custers, 'Informed Consent in Social Media Use—The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10 SCRIPTED 435, 456–457; see also a discussion on the 'pay or okay' model in section 4.3.2. in Chapter 4.

[871] Podszun (2019) (n 302) 3.

[872] Case C-40/73, *Suiker Unie*, 16 December 1975, ECLI:EU:C:1975:174, paras. 173–174.

[873] See for instance, Case C-609/13 P, *Duravit*, 26 January 2017, ECLI:EU:C:2017:46, para. 72 and Case C-194/14 P, *AC Treuhand,* 22 October 2015, ECLI:EU:C:2015:717, para. 32.

legal basis will be consent under Article 6 GDPR. In fact, how users give their consent might be the key question in the dispute, as showed by the CJEU's approach in the *Facebook case*.[874] In the proceeding, it was found that Facebook should have given its users a choice whether or not they prefer a more intensive data-related personalisation when they joined Facebook.[875] On the contrary, if users are to provide their consent freely for non-essential data processing activities, they must have a choice to decline such consent without losing access to that social network service. In the *Facebook case,* the CJEU emphasised this requirement in the context of Facebook, specifically emphasising its applicability to data processing activities carried out beyond Facebook's platform.[876] In highlighting this argument and considering the significant commercial value associated with extensive data processing capabilities, the CJEU clarified that for Facebook to justify its use of consent, it must offer users an "equivalent" social network membership if they opt-out to consent to non-essential data collection and processing for which Facebook has been seeking their approval.[877]

Reduced consumer autonomy, and or unfairness of consent given, might impede competition and innovation in the long run. The concerns raised over the dominant position of some digital service and product providers and their practices are that they negatively impact competition.[878] In fact, the more data is gathered and processed by large digital undertakings, the higher the chances are that valuable information and predictive abilities drawn from that data could be acquired. In this respect, large digital firms collect user data in various forms to improve the quality of services and products offered and to develop new services and products. Their ability to collect large quantities of data and process this through sophisticated algorithms contributes to increased market power which in turn requires the special attention of competition law authorities. That demonstrates the existence of the normative links between competition law and data protection law: exploitation of users' data often entails a reduction of users' online privacy. It does not

[874] *Meta Platforms* (n 41) para 140.

[875] ibid, para 148.

[876] ibid, para 150.

[877] ibid.

[878] J Gregory Sidak and David J Teece, 'Dynamic Competition in Antitrust Law' (2009) 5 Journal of Competition Law and Economics 581.

necessary mean that we need increased competition.[879] Instead, we need a careful consideration of large digital undertaking's behaviour, on the case-by-case basis, as the digital companies often resort exploitative conducts to collect more users' data. Therefore, I observe that competition law will intervene in situations where conduct or agreement exploits consumers as to privacy policy or the change of quality of digital products offered. This approach has been recently recognised in the CJEU's Facebook.[880] Applying the theory of privacy-related harms with the assistance of GDPR as a normative benchmark could allow an unfair privacy policy to qualify as unfair trading conditions and/or excessive data collection under Article 102 TFEU.

5.2.2. Scenario 2: No market for privacy in the Web 2.0 has been recognised yet

The consensus remains that extensive data acquisition is the key problem for both competition and data protection laws. In this section, I assume that even if we consider that there is no market for privacy protection recognised yet, then privacy could still be demonstrated as an element of quality. In this section, I use the recent incentives of Google and Apple, introducing privacy-oriented market models to demonstrate this argument in practice. The presented scenario is hypothetical.

[879] Stucke (n 26) 80.

[880] *Meta Platforms* (n 41).

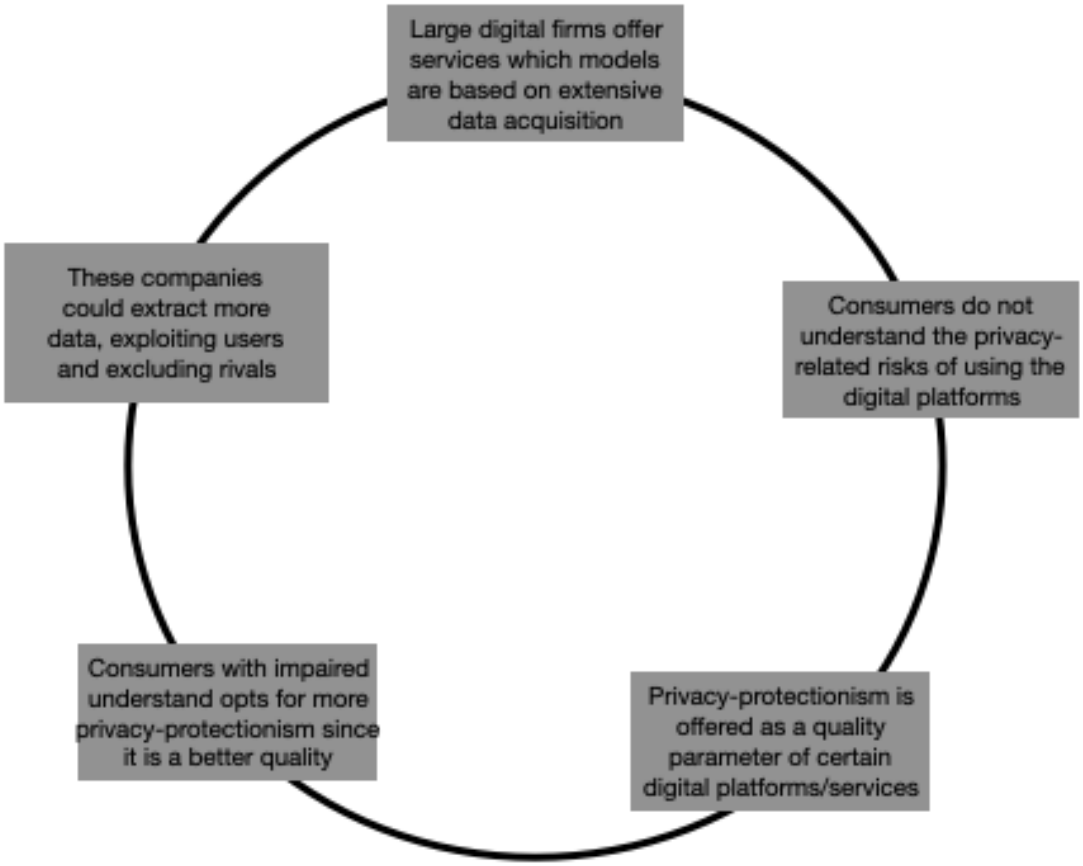


Figure 5.2: Privacy-as-quality could still exploit consumers

In Figure 5.2, I demonstrate that, in theory, increased privacy protection could exploit consumers via increased data (rent) leverage. It is shown that the recent pro-privacy amendments pursued by Google and Apple could harm competition, as per Article 102 TFEU. The assumption made in this thesis is that it remains difficult to meet the increased consumer demand for more privacy protection, as the digital economy relies on collected data to supply products, and services and generate revenue. From a privacy protection point of view, Google and Apple's decision to limit a third party's ability to identify users, results in a welfare gain for users. It remains unclear to what extent such an act could result in a quality increase. Such gains must be balanced against welfare losses resulting from legitimate advertising limitation, as such limitation could imply welfare losses for users who

value personalised advertising, or ad-funded content online.[881] This could raise further competition concerns, for example, Google and Apple could introduce policy changes that make everyone worse off while benefitting themselves. The Commission declared that it "[took] into account the need to protect user privacy, in accordance with EU laws in this respect" which could possibly underscore that competition law and data protection law have to be balanced to ensure an optimal performance in which all market participants protect privacy of users.[882] Similarly, the CMA expressed concerns over Google's Privacy Sandbox, and eventually launched a formal antitrust investigation, aiming, "to ensure that both privacy and competition concerns can be addressed as the [Privacy Sandbox] proposals are developed."[883] The investigation appears to be focused more on the advertising concentration of Google's ecosystem at the competitor's expense, rather than its impact on user privacy.

It has been argued antitrust regulators could potentially use privacy policies as a means to intervene when dominant companies, particularly those heavily reliant on data as a fundamental component of their products and services, impose non-negotiable terms on individuals, effectively giving them no choice but to accept data collection and usage practices they may not desire.[884] I assume that pro-privacy changes of Google and Apple could raise privacy-related concerns from a competition perspective. De facto privacy regulators are not constrained anyhow by competition and/or data protection authorities and could make the decision for everyone regarding the right trade-offs between privacy and competition. Essentially, the incentives introduced by Google and Apple do not limit online tracking, and still allow for automated tracking that might strengthened both Apple's and Google's market position. If companies, such as Google, were concerned about user privacy, they would choose the purpose limitation principle.[885] At the core, Google is

---

[881] See for example, D Srinivasan, 'The Antitrust Case Against Facebook' [2019] Berkeley Business Law Journal 40.

[882] European Commission, 'Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector' (Press release, 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143> accessed 24 November 2023.

[883] 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658).

[884] The most notable example remains *Meta Platforms* (n 41).

[885] 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658); Google (n 562); CMA (2023) (n 562).

oriented towards a profit maximising strategy,[886] and it could be cynical to assume that Goggle would choose to reply on data protection when Privacy Sandbox has the potential to introduce opportunities to seize more data for Google's purposes alone. Consequently, increased incentives to acquire personal data might strengthen the market power of gatekeepers, and exploit users by harvesting more data and introducing confusing terms and conditions.

In addition, the Autorité de la Concurrence investigated Apple's ATT. It was alleged that Apple implemented a significant obstacle to third-party thought tracking apps available in the Apple Store, resulting in financial losses for app producers, no longer able to efficiently personalise their advertising.[887]

Apple ATT serves as a counterpart to the German Facebook's case, which considered if imposing terms of conditions violating GDPR also represented exploitative abuse of dominance. In Apple ATT, users were made aware of possible tracking due to the tracking permission prompt in a direct and concise manner.[888] Consequently, representatives from an industry, that frequently presents users with consent requests, sometimes within pre-selected checkboxes and intrusive pop-ups that often violate regulations,[889] were expressing dissatisfaction with Apple's approach of having users make a decision using a straightforward and unbiased consent form. Many market participants' business models depend on revenue from online advertising. Their adjustment to Apple's changes depends on the actual impact of the tracking prompt. The actual problem lies somewhere else — the choice to permit tracking ultimately rests with users, not Apple. Apps developments rightly fear those users, when faced with a binary choice, will likely opt for "no" more often. Such approach is logical as users generally do not perceive an immediate advantage in granting privacy access.

The motives behind Apple's implementation of the framework might be just speculated upon. In fact, Apple might be aiming to culture an image of prioritising users' privacy.

---

[886] Vincent Giovannini, 'The French Apple competition & privacy case' (2021) 18 Competition Forum.

[887] Wiedemann (2021) (n 65).

[888] French Apple ATT decision (n 853).

[889] Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801. See, GDPR (n 57), recital 32: "Silence, pre-ticked boxes or inactivity should not (...) constitute consent."

However, the long-term effects of the incentive are still to be seen. It is still possible to consider that users might end up being exploited by Apple. Article 6 GDPR would still serve as allowing consent's ability. Apple ATT is, therefore, a good example. Advertisers relying on third-party tracking must have users' consent. In the light of BKartA Facebook's case approach, one might suggest that consumer welfare plays a vital role in asserting any possible deviation to competition law through the spectra of the GDPR infringement. On the same note, BKartA opened an investigation against Google, considering whether "Google/ Alphabet makes the use of services conditional on the users agreeing to the processing of their data without giving them sufficient choice as to whether, how and for what purpose such data are processed."[890] The question that BKartA faced was to consider how consent is granted, taking into account the terms of service offered. These proceedings underline how data protection and competition law are intertwined, underlining that possible users' exploitation will be assessed in the line of normative values underlying GDPR. In other words, the rationale behind the decision's harm theory is rooted in competition policy, while data protection regulations were factored in when weighing various interests.

Based on that, consumers would choose platforms offering increased privacy protection as the service or product quality.[891] Though far from settled in its application, the conception of privacy as a part of quality in competitive assessment has received the most attention. The Commission practice has served as acknowledging privacy protection as part of the competitive assessment. The decisions which articulated privacy as a non-price competition factor are *Facebook/WhatsApp* and *Microsoft/LinkedIn* mergers. In the *Facebook/WhatsApp* merger, the Commission held that in the consumer communications markets, privacy was the key element of competition.[892] In this case, the Commission realised the need to recognise data privacy as introducing competitive edges: privacy is valued by consumers. In *Microsoft/LinkedIn,* the Commission further supported such a statement, stating that privacy concerns could be considered during the competition assessment to the extent that

[890] Bundeskartellamt, 'Proceeding against Google based on new rules for large digital players (Section 19a GWB)' (Press release, 2021) < https://www.bundeskartellamt.de/SharedDocs/ Meldung/EN/ Pressemitteilungen/2021/25_05_2021_Google_19a.html.> accessed 31 July 2023.

[891] See the discussion in Chapter 4, section 4.2.2(2).

[892] *Facebook/WhatsApp* (n 90).

consumers see it as '*a significant factor of quality*'.[893] Furthermore, the Commission observed that, "[m]any businesses also promote respect for personal data as a competitive differentiator … by offering innovative products and services with novel privacy or data security solutions."[894] However, privacy protection can only impact competition assessment when privacy is a defined and a recognised parameter of competition. It is still not a case of privacy-related harms, as its quantifiable methods are far from being settled. At present, EU competition law does not recognise an integration between competition law and privacy, as matters of privacy-related harms are outside the scope of competition law enforcement. However, if privacy-related harms are not put forward as a standalone argument in competition law assessment, privacy-related harms might be used as a proxy to find a competition law harm under Article 102 TFEU.

5.3. Mapping synergies: the privacy trap theorem explained

In this section, I present two possible scenarios for merging competition law and data protection, with their corresponding effects on competition. An assumption is made that privacy-related harms might be considered by competition authorities only when privacy-related harms are not a standalone argument in competition law assessment. As demonstrated in the previous section, competition law and privacy-related harms are capable of being interpreted consistently, especially when privacy-related harms also introduce anticompetitive constraints. Behavioural problems, a combination of personal data and market power could endanger the excessiveness of personal data collection, which is a problem for exploitative abuse of market power as well as for informational self-determination and protection of user privacy.[895] In this respect, due to the practices of large digital undertakings, there is an unsolved privacy problem, which is a challenge for competition law: the frequently mentioned integrated approach is frequently claimed rather than effectively implemented.

5.3.1. Positive competition outcomes

5.3.1.1. Overlaps with positive privacy outcomes

Extensive data acquisition remains a significant concern for competition law and data privacy law. The GDPR impact on the straightening of economic power of large digital firms

[893] *Microsoft/Linkedin* (n 90).

[894] 'Data Protection as a Pillar of Citizens' (n 331) 8.

[895] Boerman, Kruikemeier and Borgesius (n 16).

remains interesting, as, arguably, the GDPR makes it easier for them to obtain consent to collect, process and analyse personal data than for their competitors. If such an argument remains true, then companies might abuse their market power by offering a reduced level of privacy protection, correspondingly exploiting end users. Such conduct leads to negative outcomes for both competition law and data protection law.[896]

If consumers have a better understanding of the risks associated with sharing their personal data, they could value digital products and services which offer an increased commitment to protecting their personal data. I discussed consent as a dogmatic link between competition law and data protection law in this thesis by focusing on examples of the BKartA's *Facebook case*, and the French *Apple ATT case*. When it comes to situations involving dominant platforms, the crucial issue is determining whether consent is genuinely voluntary.[897] This aspect connects both competition and data protection regulations, as the independent and unconstrained giving of consent reflects the choices made by consumers. Several GDPR-related rulings against Facebook, in Germany,[898] Ireland[899] or the CJEU[900] indicated that large digital undertakings can only collect data with explicit user consent. A freely given consent to the collection of data is required whether collection takes place on- or outside the platform in question.[901] In October 2023, Facebook began to offer its paid, ad-free version of its flagship platforms — Facebook and Instagram.[902] Facebook still offers its services with ads if users consent to them. In other words, Facebook is now introducing a payment option where users could either pay for an ad-free experience or consent to see ads, akin to a paywall model. However, pay-or-consent models are still considered problematic. For

[896] *Microsoft/LinkedIn* (n 90); *Facebook/WhatsApp* (n 90); *Meta Platforms, Opinion of AG Rantos* (n 85).

[897] Klaus Wiedemann, 'A matter of choice: the German Federal Supreme Court's interim decision in the abuse-of-dominance proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)' [2020] IIC 1168.

[898] Facebook case (n 2).

[899] See, Data Protection Commission, 'Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland' (Press Release 2023) <https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.> accessed 20 November 2023.

[900] *Meta Platforms* (n 41) para 111-117.

[901] ibid, para 151.

[902] Carugati (n 44); see also a discussion of the pay-or-okay model in section 4.2.3.

example, they are illegal in Belgium.[903] Yet, the French data protection authority allows for such a model to operate under certain, strict, conditions.[904] Here, users should be provided with an alternative option if they prefer not to make a payment, and the pricing for the paid opinion must be reasonable. The economic justification for such payment is that digital undertakings have a legitimate claim to compensation for ad revenue they lose due to their inability to offer personalised ads, which depend on tracking a user's online activities. The CJEU considered that a paid version is lawful if users who refuse to consent can access to an equivalent service for a reasonable fee.[905] In practice, several companies have acknowledged privacy as a competitive advantage, allowing them to compete through the level of privacy protection offered; for example, the search engine DuckDuckGo does not track and share personal user data, correspondingly differentiating its product from different search engines.[906]

5.3.1.2. Overlaps with negative privacy outcomes

Arguably, practices that hinder privacy outcomes could introduce positive competition outcomes. According to Graef, with the absence of robust data protection principles, such an approach could favour economic efficiency, which are often different from the goals of data protection laws.[907] In fact, consumers' privacy concerns and the emphasis on privacy-driven competition are in direct contrast to the advertisement-centred business model employed by major online platforms. Large digital platforms design their privacy policies in ways that create significant barriers for users to comprehend the privacy implications tied to their service usage and to hinder the prevention of personal data collection and sharing with

---

[903] Carugati (n 44); Autorite de Protection des Données, 'L'APD publie une checklist pour une utilisation correcte des cookies' (Press Release, 2023) <https://www.autoriteprotectiondonnees.be/citoyen/actualites/2023/10/20/lapd-publie-une-checklist-pour-une-utilisation-correcte-des-cookies. + Bruegel> accessed 24 November 2023.

[904] Commission Nationale de l'Informatique et des Libertés, 'La CNIL Publie des Premiers Critères d'évaluation' (Press Release, 2022) <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation> accessed 24 November 2023.

[905] *Meta Platforms* (n 41) para 150.

[906] Danny Sullivan, 'Duck Duck Go's Post-PRISM Growth Actually Proves No One Cares About "Private" Search' (2013) *Search Engine Land* <http://searchengineland.com/duck-duck-go-prism-private-search-164333> accessed 1 March 2022.

[907] Inge Graef, Damian Clifford, and Peggy Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law' [2018] International Data Privacy Law 200.

external parties such as advertisers and app developers.[908] The platforms are motivated to maintain consumer unawareness and perplexity regarding their data handling practices, as this situation results in the emergence of services which might challenge their advertising-focused business model.[909] Consent might be invalid in certain circumstances where the controller demands consent for proceeding of too many of personal data.[910] Article 7(4) GDPR is critical in the debate on 'data as counter-performance'.[911] Yet, its scope of application is difficult to define, as it remains unclear on how far can the data controller go when demanding personal as a counter-performance for a service. There is no consistent answer to this question and a case-specific assessment is crucial, considering not only the data subject's right to the data protection but also the freedom of contract both parties can rely on. To sustain this lack of awareness while projecting a false sense of control over personal data, online platforms resort to unjust contract terms with consumers and engage in deceptive commercial practices that deliberately complicate the management of privacy settings for their services. This approach cannot be considered as "competition based on merits".[912]

5.3.2. Negative competition outcomes

5.3.2.1. Overlaps with negative privacy outcomes

Data collection on an unprecedented scale, via the default opt-in option, could be considered as an abuse of dominant position, comparable to excessive pricing and unfair trading conditions.[913] The ‘default opt-in’ option offered by the digital platforms and service providers are seen as a market failure,[914] which might give rise to an infringement of competition law under Article 102 TFEU. For instance, in the BKartA's *Facebook case*, Facebook's terms and conditions violated the GDPR and competition law, as they were “neither justified under data protection principles nor are they appropriate under

[908] See for example, *Facebook case* (n 2).

[909] Michael Weiner, ‘Antitrust Is Cool Again’ (2018) New York Law Journal; Magdalena Kedzior, ‘GDPR and beyond – a year of changes in data protection landscape of the European Union’ (2019) 19 ERA Forum 505.

[910] *Meta Platforms* (n 41).

[911] Drexl (n 79).

[912] *Post Danmark* (n 277).

[913] I discussed extensive data collection as compatible with extensive pricing and unfair trading conditions as the theory of harm in Chapter 4, sections 4.2.2 and 4.2.3.

[914] Pasquale (n 163) 1011; Kerber and Specht-Riembenschneider (n 716); Kerber (2022) (n 158).

competition law standards".[915] Generally, consent is required, individuals are unable to thoroughly consent to the real purpose of data processions.[916] Increased market powers enable firms to engage in practices that are opaque for consumers on how digital platforms use their data. For both zero-priced platforms, as well as positive-price platforms (e.g. Netflix), personal data is used for targeted marketing models, giving a competitive advantage. Consumers could lack the power of accountability in negotiating contracts between the digital service or the providers of the products. In the recent BKartA investigation against Google, users are said to not be given a sufficient choice as to how their data is processed across services.[917] According to the BKartA, Google heavily relies on the processing of user data in its business model. Google's current terms allow to merge data from various sources. This allows Google to create highly detailed user profiles, which can be utilities for advertising purposes, as well as to increase the Google services functionality. Google can, for various reasons, collect and process data across services. Mundt highlighted that this confers a "strategic advantage" to Google over other companies.[918]

However, if data is considered as a non-monetary cost for accessing digital platforms and services, it is possible to apply the logic of overcharging in price-oriented markets. The same rationale can be achieved by looking at the new Facebook's 'pay-or-okay' model.[919] Under this scenario, digital product suppliers and services are allowed to impose the costs that inadequately reveal consumer preference and valuation of the product in question. Consumers remain unaware of the extent of their personal data being collected while using and accessing such digital services in practice. Within Google's investigation by the BKartA, the choice offered was seen as too general and insufficiently transparent for users. According to the BKartA, there had to be an adequate level of choice and users should have the ability to restrict data processing to the particular service they are using.[920] Moreover, they should also have the capacity to distinguish between the different reasons for which

[915] *Facebook case* (n 2).

[916] GDPR (n 57) article 4.

[917] Bundeskartellamt, '*Statement of Objections Issued Against Google's Data Processing Terms*' (Press Release, 2023) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html> accessed 23 November 2023.

[918] ibid.

[919] See section 4.2.3 in Chapter 4.

[920] *Facebook case* (n 2); *Meta Platforms* (n 41) para 82.

the data is being processed.[921] The Google investigation is similar to the *Facebook case*, where the fundamental concern was a data-accumulation strategy, giving large digital undertakings a competitive advantage with possible user exploitation.

Alternatively, if one assumes that the data collection might be within users' expectations, then Article 6(1)(b) GDPR could limit the purpose-limitation of data collection. According to the CJEU, in the *Facebook case*, Article 6(1)(b) GDPR defines an objective performance necessity test that varies somewhat, oscillating between the need for objective indispensability for a purpose integral to the contractual obligations and the requirement for essentiality to ensure the proper execution of a contract, consequently excluding practical, less invasive alternatives.[922] In cases where the justification of consent depends on the requirement of data processing under offered contract, a compelling necessity argument, as per Article 6(1)(b) GDPR, renders a consent assessment for that specific purpose as irrelevant.[923] Concerting personalisation as an objectively necessary feature under Article 6(1)(b) GDPR, the CJEU indicated, without providing specific details, that there should be an alternative, less intrusive, method for ensuring the relevance of content.[924]

Hence, a twofold nature of data acquisition is recognisable: creating network effects and lock-in effects; the more users are active on a platform, the more data is acquired thereby improving potential advertisement or search results. Privacy policies are designed in an ambitious manner, which downplay the risks of using the service. This could influence the lock-in effect based on consumer action regarding privacy.[925] Nevertheless, despite regulatory attempts to define how personal data is collected and processed, this asymmetry persists, allowing large digital undertakings to impose unfair trading conditions. The assessment of any promising legislative approach that offers individuals greater control over their data, might enhance the accountability of their power in negotiation. However, this approach does not always offer a great response to any protection. The potential

---

[921] This was one of the points raised up by the CJEU judgment. *Meta Platforms* (n 41) paras 82-85.

[922] ibid, paras 148-150.

[923] ibid*,* para 93.

[924] ibid, paras 148-150.

[925] A Reyna, ''The psychology of privacy—what can behavioural economics contribute to competition in digital markets?' [2018] International Data Privacy Law 240.

alternatives are as follows: (1) behavioural discrimination, witnessed by information that digital users witness while relying on digital services and products, to which they immediately select 'accept all';[926] or (2) the default privacy notices, which as per the case of *Microsoft*,[927] offer an omnibus privacy support. Any potential incentives to create privacy by design might sound promising. Hence, to practically engage in the sphere of informational asymmetry, an under-active consumer should have their enhanced discourse protected, as its negative dimension might impose negative externalities on them, thus reducing competition.[928]

5.3.2.2 Overlaps with positive privacy outcomes

The overlap between negative competitive outcomes with positive data protection outcomes is the most nuanced interaction between both regimes, as it comes from the phenomenon of the 'competition on privacy'. It is potentially the most vibrantly discussed concept now, given the attempts of Google and Apple to enhance the protection of user privacy. The problem could also be extended to exploit users by Apple and Google's practice to exclude third-party tracking and collect more data for their purposes. The recent Apple iOS 14 update serves as an example of this process. Increasingly, Apple has been contaminating the mobile ecosystem with their privacy protection incentives. Recognising competition on privacy could be seen as a legitimate and beneficial strategy, fostering competition: companies might then compete on the level of privacy protection offered. This privacy-enhancing action could still be captured under the Article 102 TFEU infringement.

Sokol and Zhu suggested that Apple's policy amendment could introduce negative competition outcomes.[929] Their argument concerned the consumer welfare benefits from ad-driven models, considering consumer preferences and informational asymmetry, it is difficult to ascertain if personal advertising could generate a positive consumer surplus.[930] There is the possibility of introducing a positive data protection outcome with Apple's action

---

[926] Alex Chisholm, 'Alex Chisholm Speaks about Online Platform Regulation.' (2015) *CMA* <https://www.gov.uk/government/speeches/alex-chisholm-speaks-about-online-platform-regulation> accessed 14 March 2020

[927] *Microsoft* (n 252), and Carugati (n 44) where the new Facebook incentive to pay-or-consent was discussed.

[928] Ezrachi and Stucke (n 385) 226.

[929] Sokol and Zhu (n 816).

[930] Economides and Lianos (n 24).

of weakening third-party app tracking, which in turn could result in a decrease in competition. Apple is compelling third-party apps to change from an ad-driven to a fee-based model, which could raise consumer costs for switching to the different mobile ecosystem - Android. If users prefer to use Apple's iOS, switching to the Android system would be more cumbersome. Furthermore, for consumers who prefer Apple's apps or those offered by third parties, potential fees for a subscription-based model could indicate that they lose access to in-app purchases if they switch to Android. Hence, this could create lock-in effects. The incentives create by Google to protect user privacy by prohibiting third party 'cookies' raises similar concerns.[931]

As a result, Apple and Google are creating a template which could increase their market power. This template could be compared to the 'shield and armour' analogy: Apple and Google weaponise data, blocking other companies access, preventing them from building a competitive database. Consumers could be exploited by Apple and Google's incentives to introduce privacy protection, allowing them to use unfair and exploitative practices and hinder innovation, thus enjoying the quiet life of monopolists. From the perspective of competition law, there is a difference between the attempts of Google and Apple to introduce pro-privacy policy amendments. Essentially, such concentration further distort competition, exploiting consumers.

5.4. Drawing a boundary between competition law and privacy: privacy-related harm as an addition to the competition assessment

In the context of the debate on defining the nexus between competition law and privacy, only one question remains unanswered: to what extent could privacy-related harms be seen as directly influencing competition law assessment? Through discussing this complex interaction, three following problems could arise:

(1) Regulatory gaps

Regulatory gaps remain the most widely covered aspects of the intersection between competition law and privacy.[932] Despite the common denouncement that the relationship

[931]'Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google (n 642); 'Investigation into Google's 'Privacy Sandbox' browser changes' (n 658).

[932] See for example, Furman Report (n 1); Cremer Report (n 1); 'Online Platforms and Digital Advertising Market Study' (n 1).

between competition law and privacy is complementary, the relationship between competition and data privacy is much more multi-faceted and nuanced. It is important to note that competition and data protection laws are two different and separate regimes. However, data protection and competition policy share foundational concerns and similar remedial approaches: how to mitigate unfairness by introducing and imposing obligations on those with market power? Essentially, the goal is to prevent power imbalances arising between individuals and strong companies.

(2) Regulatory conflicts

The mutual application of competition law and data protection law could result in conflict. Antitrust authorities are focused on the competitive effects of any conduct, regardless of whether the conduct in question breaches data privacy laws. Data protection centres around the right-based approach focusing on consent and does not aim to address underlying market failures. For instance, one possible competition law remedy would be to mandate personal data sharing, which introduces a negative outcome for data privacy law.

(3) Synergies

There are possibilities in which the application of both competition law and data protection law would work in the same direction, as supporting privacy protection. However, the question remains as to what possible policy solution could be used to improve such synergies, without expending the scope of both laws, and how competition and data privacy laws could influence each other in achieving their objectives.

Therefore, the focus here is on discussing policy solutions to define a nexus between competition law effectiveness in tacking privacy-related harms. As discussed in this thesis, the normative approach is to be welcome. According to this argument, the availability of personal data and the ability of digital platforms to process this data can be seen as a factor influencing competition among businesses in the digital economy. Disregarding this perspective would fail to consider the actual growth of the digital economy and could weaken the overall effectiveness of competition laws.[933] Article 102 TFEU could encompass privacy-related harms. Article 102 TFEU, which prohibits the abuse of a domination position in a relevant market, could apply to the anti-competitive actions of online platforms, which

[933] *Meta Platforms* (n 41) paras 50–51.

operate on data acquisition.[934] **I**ndependent application of such laws, which do not consider their interlinked effects, could lead to unsolved conflicts.

5.4.1. Policy solutions: context

Drawing from the above discussion, three different contexts are identified where competition law and data protection regimes could intersect:

(1) *Positive perspective*: under this consideration, the assessment of data protection implications offers opportunities for competition policy to protect fundamental rights without changing the established focus on consumer welfare. Data protection parameters could help to address market failures and any competition related harms emerging from the business models of digital platforms.

(2) *Negative perspective*: under this context, the mere breach of data protection provisions should not be seen as a competitive matter. This should not constitute an expansion of the competition legal order into that of other areas of law, such as data protection, because competition law relates to tacking harms caused by market failures. Data protection centres around the right-based approach focusing on consent and does not aim to address underlying market failures.

(3) *Normative perspective*: under normative perspective, competition assessment could be considerably informed by data protection. This includes a consideration of the role of data and attempts to establish competitive parameters of non-monetary price, such as quality and innovation that could serve as a benchmark for the exploitative conducts assessments.

A strategy is here presented that could reconsider the intersection between competition law and data privacy law. Addressing all concerns emerging from the digital economy and acknowledging privacy-related harms, requires an integrated approach between both competition law and data protection law. Competition law has a role to play in protecting user privacy, yet data privacy law should not be seen as extending the scope of competition

[934] I consider privacy-related exploitative theories of harm in chapter 4.

law, nor as a ubiquitous tool to redress any possible harm arising from data collection.[935] Any practical attempts to define competition law boundaries require the development of a formal cooperation agreement. Other practical measures could include the introduction of relevant legislation and guidelines to allow a better consideration of data privacy rules when enforcing competition law.

5.4.2. Strategy: Competition-risk-oriented approach

From the framework provided in section 5.2. of this chapter, and assessment of exploitative theories of harm considering potential privacy-related harms from chapter 4, a risk-focused approach is provided which follows that it could be necessary to bring clarity in defining the relationship between competition law and privacy. The "competition-risk-oriented' approach (hereinafter: risk-based approach) focuses on creating a more integrated, and holistic approach, respecting the boundaries of competition law and data protection law respectively.

The risk-based approach could address the tendencies affecting digital markets, and privacy-related concerns, enhancing the EU's legal coherence, and would emphasise that competition might assess privacy-related harms as a broader context of antitrust regulations.

The analysis in the next section provides two components of this approach.

5.4.2.1. Components

(1) Component 1: Privacy-concerns and competition policy: the overlapping consensus

Until now, I have discussed that there is an apparent dogmatic and normative link between competition law and GDPR. I have also demonstrated that, in practice, privacy-related harms can be investigated in competition law: this is especially plausible if individuals find themselves compelled to agree to unfair trading conditions (and excessive data collecting practices), whereas this could solidify a dominant position for a particular large digital undertaking. In consequence, prospective competitors might struggle to collect the required magnitude of data to rival the confirmed marked player. Hence, interpreting competition law and data protection in a coherent matter is not just sensible but also imperative to

[935] *Meta Platforms, Opinion of AG Rantos* (n 85); *Meta Platforms* (n 41).

effectively evaluate and address the behaviour of dominant large digital undertaking.[936] Therefore, a unified and logical interpretation and implementation should be sought in appropriate situations to accommodate all relevant interests.

When it comes to competition law, competition authorities need to delve deeper into the intricacies of data privacy regulation and enhance their comprehension of the limitations on consumer decision-making.[937] In other to determine that the data could have been collected and processed unlawfully, distorting competition on the merits, competition authorities require a crucial factor for making well-informed judgements. In other words, competition authorities need to understand the informational and behavioural problems of consumers in the relevant market. This correspondingly calls for an optimal form of relationship between competition law and data protection law. I cover this argument as a second component. Here, I focus on the informational and behavioural problems of consumers as showing a possible overlapping consensus between these two regimes.

It has been argued that competition and data protection law overlap to a certain extent: (1) both regimes aim to ensure consumer welfare; (2) possible privacy-related harms might be understood as consumer harm.[938] Competition law is limited in its application to protecting user privacy and should only focus on concerns detrimental to a healthy functioning competition. Hence, it implies that data protection law would have to help in solving these problems and could be used for a more effective contribution. At the policy level, a combination of competition and data protection law might be effective in answering market-related problems and consumer empowerment in the digital market regarding their data. In other words, an analysis of a benchmark might be useful in applying a more integrated approach between competition law and data protection. As data protection law is a subjective standard, I discuss a privacy-as-quality theory as a possible benchmark in

[936] See Chapter 3 for a detailed discussion of the case law. I discussed the *Facebook case* saga in Chapter 3 in details. This case serves as a crux in the relationship between competition law and data protection.

[937] See for example, Orla Lynskey, 'Non-price Effects of Mergers' OECD Competition committee meeting (2018) DAF/COMP/WD(2018)70; Kerber and Specht-Riemenschneider (n 716) for a discussion on informational (behavioural) market failure.

[938] See Douglas (n 158) 62-72; Costa-Cabral and Lynskey (n 152).

investigating privacy-related harms in competition law.[939] The discourse will demonstrate that the competitive focus on Article 6 GDPR infringement in response to possible privacy-related harms serves as an indicator or proxy for identifying both anticompetitive harm and diminished quality.

If we consider the *Facebook case*, the CJEU indicated that inspecting each legal requirement outlined in the GDPR to establish a violation of competition law was not about entreating the area of data protection law without authority. Instead, GDPR was applied to evaluate the consistency in which Facebook conducted its data processing activities with applications under GDPR.[940] In this context, competition law could use the GDPR rules to assess the quality of the offered digital product or service. If one considers principles such as (1) lawfulness, fairness, and transparency;[941] (2) purpose limitation;[942] (3) integrity and confidentiality;[943] (4) accuracy;[944] (5) data minimisation;[945] and (6) storage limitation,[946] one could possibly evaluate data processing activities and offered privacy terms as a quality parameter through competition law spectra. Also, this approach could be valuable in conducting competitive assessments that might be applied to formulate theories of harm, such as unfair trading conditions under Article 102 TFEU.

The question remains as to how competition law should deal with this balancing practice. I recommend the use of a cautious approach. The problems of competition law and privacy-related harms are interlinked, and competition law should only remediate such concerns that directly harm competition in a relevant market. In the *Facebook case*, the CJEU focused

---

[939] This theory has been discussed in detail in section 2.2.2.1 in Chapter 2. Here, I supplement the analysis of the theory for the sake of this section's argument.

[940] *Meta Platforms* (n 41) para 36.

[941] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2019) paras 62-64 < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 23 November 2023. (Hereinafter: "EDPB, 'Guidelines 4/2019")

[942] ibid, para 66

[943] GDPR (n 57) article 5(1)(f).

[944] EDPB, 'Guidelines 4/2019' (n 941) para 72

[945]ibid, para 68.

[946] ibid, para 75.

on the relationship between market power, GDPR-defined imbalances, and exploitative conduct. Importantly, this case has not focused on possible privacy-related harms; privacy-related harms were noted as *obiter dictum*. Instead, from its beginning, the BKartA focused on the exploitation of users taking forms of unfair trading terms under Article 102(a) TFEU, manifested through a single catch-all consent. The BKartA case has not provided a clear basis for indicating that checking a box for privacy terms could appear more secure than automatically accepting offered terms. Cases can vary in complexity, and competition authorities do not have expertise in data protection. Depending on intuition to determine better privacy protection might lead to a lack of consistency and legal certainty. By consulting a data protection framework, competition authorities could make their assessment more coherent and legitimate. As per the Facebook scenario, the CJEU asserted an incidental consideration of GDPR as a theory of harm to capture the anticompetitive conduct of Facebook.[947] In other words, the GDPR does not preclude the identification of an abuse under Article 102 TFEU, and it could be considered in the overall case-by-case analysis of the circumstances. In this context, the incidental consideration of the GDPR might serve as a significant indicator to conclude whether the conduct has not impaired competition on the merits.

If the GDPR had been applied correctly, Facebook might have changed the way the consent was obtained. In this case, this would not alter the decision — Facebook remains a dominant undertaking on the market, exploiting users in terms of their comprehensive choices, not just limited to the extent of data protection. This case is an example of a fine line between competition law and data protection. Yet, it is necessary for a distinction between the two regimes to be respected and authorities refrain from exceeding their authority to address gaps beyond their expertise.

It is possible to ascertain that privacy-related harms might be acknowledged as a competition law factor on a case-by-case basis.[948] In other words, competition authorities

[947] *Meta Platforms* (n 41) para 36.

[948] Henrique Schneider, 'From Deontology to Pragmatism: Dynamics in the Pursuit of Goals of Competition law' [2017] CORE 245, 254.

should be aware of how data protection principles apply in practice.[949] Once the conduct has been identified, the debate should focus on which conduct should be of importance to the competition law regime, i.e. whether conduct should be seen as abusive, or not. Then, an assessment of the competition processes should be conducted within these objectives. It is possible to conclude that the objectives of protection of competition structures applied on normative value, which derives from the particular in question objective, makes the protection of competition law worthy.[950]

(2) Component 2: Close cooperation to identify the anticompetitive scenarios: market observation

The next step of the competition-risk-focused approach is to aim for more interaction between competition and data protection. Here, I aim to develop an enforcement strategy that guides companies' behaviour which leads to better market functioning, promoting competition and data protection law. It is recognised that there are very few instances of a single regulatory instrument being an efficient means of addressing a particular data-relating problem.[951] Instead, it might be possible to consider "policy mixing". The idea of combining competition and data protection enforcement is not novel. For instance, in Italy, the competition and market authority, the data protection authority, and the regulator for the communication industry collaborated on a comprehensive study. They aimed to develop an understanding of the implications for privacy, competition and consumer protection arising from the digital markets.[952] Similarly, the BKartA cooperated with the German data protection authority while investigating Facebook.[953] In a coordinated approach, policymakers should focus on all policies necessary for solving the problem and should

---

[949] It needs to be emphasised that data protection authorities operate on the national-member-state level. I discussed data protection authorities' institutional jurisprudence in section 3.2.2. in Chapter 3.

[950] Nazzini (2009) (n 744) 17.

[951] See Neil Gunningham and Darren Sinclair, 'Designing Smart Regulation', this article is an abridged version of the concluding Chapter in N Gunningham & P Grabosky *Smart Regulation: Designing Environmental Policy* (OUP 1998) 3. The authors have focused on the environment concerns in their research.

[952] Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni and il Garante per la protezione dei dati personali, 'Big Data, Indagine Conoscitiva Congiunta, Linee Guida e Raccomandazioni di Policy' (2019) <https://www.garanteprivacy.it/documents/10160/0/Big+Data.+Linee+guida+e+raccomandazioni+di+policy.+Indagine+conoscitiva+congiunta+di+Agcom%2C+Agcm+e+Garante+privacy.pdf/563c7b0e-adb2-c26c-72ee-fe4f88adbe92?version=1.1> accessed 24 November 2023.

[953] *Facebook case* (n 2).

assess each effect separately. It implies that policymakers should develop a common understanding of the problem, as well as acknowledge the effects that each policy has. To demonstrate this intersection, I discuss possible close cooperation between competition and data protection authorities through market observation.

It might be challenging to determine the appropriate level of intervention and necessary steps to reinstate competition in the affected market. In such situations, market examination can serve as a valuable resource for competition authorities to uncover the underlying causes of market failures. Dunne argued that by "by enabling a more holistic and comprehensive examination of the causes and consequences of market failures, market studies can, in theory, identify and facilitate the most appropriate means to resolve such problems."[954] The market examination might be particularly useful in the context of data protection issues. While data protection regulation is also focused on market operation, data protection authorities lack the necessary expertise and tools to analyse the market dynamics. Competition authorities, with their expertise, can shed light on these aspects, helping data protection authorities determine when and how to intervene effectively, and encouraging compliance among digital undertakings. Such an approach helps determine issues such as: (1) whether there is a correlation between increased market competition and the quality of data protection terms;[955] and (2) whether increased privacy protection reflects consumer demand.[956] While competition authorities' market investigation could provide insight as to why a market is not functioning well, in certain instances data protection authorities have better tools to correct the market failure. In other words, comprehending market dynamics and the impediments to its proper functioning would enable data protection authorities to establish and supervise specific requirements aimed at addressing these obstacles, such as: (1) simplifying terms and conditions to overcome information overload and consumer inertia; and (2) requiring and promoting consumers to actively choose rather than defaulting to the status quo.

---

[954] Niamh Dunne, *Competition Law and Economic Regulation: Making and Managing Markets* (2015 CUP) 280.

[955] Based on the findings in this thesis, my tentative answer is that generally more competition might lead to better privacy outcomes. However, in this thesis I focused on exploitative theories of harm, and it has been suggested that more privacy does not solely indicates that better outcomes for consumers. See chapter 3 and 4 for a detailed overview.

[956] This answer is interlinked to my answer included in footnote 955. See the case of Google Privacy Sandbox and Apple ATT presented in section 4.2.2(2) in Chapter 4.

The approach suggested in this section is similar to the approach taken by the CMA in its market investigation. The CMA can assess market conditions, by considering the overall market's performance rather than relying on just one aspect or specific undertaking's behaviour.[957] The CMA initiates a market investigation when it reasonably suspects that certain aspects of a market or markets are impeding, limiting, or distorting competition in the supply or acquisition of goods or services in the UK or a specific region.[958] The CMA conducted a market study on online platforms and digital advertising, addressing concerns that align with the issues I discussed in this thesis. The CMA focused on the concerns that the digital market effectively limited consumers' ability to negotiate the collection and use of their data, due to concerns of a trade imbalance between consumers and large digital undertakings, which could result in the reinforcement of large digital undertakings' market dominance.[959] The findings of the CMA study offered recommendations to both government and data protection authority uncovering concerns such as the disproportionate impact of data protection regulation enforcement and/or market distortion.

At the EU level, the Commission enjoys the authority to conduct sector inquiries in cases where market conditions indicate that competition is not functioning effectively as per Regulation 1/2003.[960] The process aims to investigate possible market issues. While the Commission does not enjoy the direct power to enforce remedies, it might lead to possible specific market investigations and subsequent legislative proposals. Dunne argued that possible sector inquiries go beyond investigating violations of competition law.[961] Their findings may discover market issues that can be effectively addressed through possible regulatory changes rather than antitrust enforcement. In this respect, the Commission can generally assess the market landscape in conjunction with individual player roles, expanding

[957] CMA, 'Guidelines for market investigations: Their role, procedures, assessment and remedies' (2013) para 18 <https://assets.publishing.service.gov.uk/media/5a7c1b7340f0b645ba3c6bcc/cc3_revised.pdf> accessed 24 November 2023.

[958] CMA, 'Market Studies and Market Investigations: Supplemental guidance on the CMA's approach' (2017) <ttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624706/cma3-markets-supplemental-guidance-updated-june-2017.pdf.> accessed 24 November 2023.

[959] 'Online Platforms and Digital Advertising Market Study' (n 1) paras 64-66.

[960] Regulation 1/2003 (n 54) article 17(1); see also section 3.2.1. in Chapter 3 for a discussion on institutional jurisprudence of competition authorities.

[961] Dunne (n 952) 282.

the scope of the effectiveness of its market supervisory efforts.[962] Even if market studies do not result in any new legislation, they can generate recommendations on the application of exciting frameworks.

5.4.2.2. Possible criticism of the approach

There is the suggestion that alighting data protection enforcement with market dynamics might enhance the ability of large digital undertakings to adhere to the rules and provide greater incentives to do so. Such an alignment might be achieved by close cooperation during marker examination. This collaborative approach benefits both regulatory domains by promoting voluntary compliance with data protection regulations and fostering competition.

In this section, I discuss two possible shortcomings of the risk-based approach. They include: (1) relying on data protection law to assess anticompetitive harms that might be seen as possible expanding the scope of competition law; (2) mere violations of privacy should be addressed by data protection regulators.

(1) Possible expansion of Article 102 TFEU scope

To trigger an Article 102 TFEU breach, there needs to be a recognisable competitive concern. Treating mere data protection violations as exploitative and exclusionary abuses may face criticism. There could be possible risks that it becomes overly simple to find an abuse of dominance by connecting it to various other legal areas, or that any possible privacy-related harms could be considered as also infringing Article 102 TFEU. Dominant undertakings might violate several laws that have no connection whatsoever with their market position. For instance, an agricultural company could neglect safety or cleanliness standards relevant to food processing, while a computer processor company might breach employment discrimination regulations.[963] These violations clearly cannot be used as a ground to initiate Article 102 TFEU proceedings, as they have any substantial competitive implications. Article 102 TFEU requires competition-related issues to be triggered, which is why only violations of non-competition laws that can reasonably be linked to significantly contributing to the establishment, maintenance, or reinforcement of a dominant position can be used to establish an abuse of dominance.

---

[962] Dunne (n 952) 282

[963] Maurice E Stucke, 'How Do (and Should) Competition Authorities Treat a Dominant Firm's Deception?' (2010) 63 SMU L. Rev. 1069, 1114.

Article 102 TFEU aims to prevent dominant undertakings from abusing their position by *inter alia* raising prices, reducing quality, limiting choice, shifting innovation, or negatively affecting other aspects of competition. Hence, for any non-competition violations to form a basis for Article 102 TFEU proceedings, it must have a detrimental impact on one or more of these competition-related parameters. Assuming that competition law infringements being equated with data protection infringements is theoretically unsound,[964] this could serve as an unnecessary expansion of the available competition law toolkit. There are recognised risks involved that by referring to multiple areas of law, finding an abuse of dominant position would be an easy task.[965] Essentially, the mere breach of data protection provisions should not be seen as a competitive matter. I argue that privacy standards are relevant as a quality parameter during a competitive analysis. Yet, this should not constitute an expansion of competition legal order to that of other areas of law, such as data protection, for the simple reason that competition law relates to tacking harms caused by the market failures and remedying competitive harm. A mere privacy-related breach has little or no competitive impact.

Ezrachi suggested that their implementation could require trade-offs between the goals, which could introduce further ambiguity or balancing points.[966] Hence, the question as to whether potential privacy breaches might influence the competition law structure could be answered by Ezrachi's analogy, which pictures the relationship between competition policy and wider societal deliberations with a sponge and membrane analogy.[967] In his research, he recognises competition law as a sponge with a political core, and economics as a membrane which allows certain external by-passes into its realms.[968] Consequently, both general values on the maximisation of consumer welfare and social and political priorities, that shape local enforcement, could be part of the competition law objectives.[969] Competition policy

[964] Costa-Cabral and Lynskey (n 152) 22.

[965] ibid, 22.

[966] Ezrachi (2016) (n 174) 18.

[967] ibid.

[968] ibid, 4-14.

[969] ibid, 17.

objectives need to be carefully defined, as the incorporation of a multitude of different principles might lead to the unpredictability of the competition law enforcement.

(2) Alternative approach: violations of privacy should be addressed by data protection regulators

The core behind this approach is to show that competition law should address only competition concerns.[970] In this approach, one draws a line between the mutual application of different laws since each law should be enforced to address the concerns directly within their own respective remits. However, it appears to be implicit that the parallel enforcement of competition and data protection laws would be a more logical and simpler way to assess any online market failures.[971] For instance, the Italian consumer protection authority (AGCM) fined WhatsApp for imposing unfair and abusive commercial practices in their offered terms and conditions, where consumers unduly consented to share their data with Facebook.[972] Here, consumer protection enforcement could increase transparency and consumer awareness of the privacy-related consequences of using online platforms.

Although the mutual concern for both competition law and data protection law is extensive data acquisition, competition law could be only effective in answering privacy-related harms if the harm directly influences competition law by taking the form of exploitative conduct. Given the different mandates of data protection and competition law, there are only a few instances in which the question of the boundary between the regimes arises. The main situation in which this happens is when a problematic data practice of a dominant firm is in some way related to its market power. While I have discussed that the regulatory framework allows for a possible interaction,[973] the regimes should refrain from doing so. Given the existence of the indirect link between market dynamics and data protection, mere GDPR non-compliance does not automatically warrant antitrust intervention. In such situations, it is crucial to establish a compelling case that the dominant undertaking is abusing its market

---

[970] *Asnef-Equifax* (n 89) para 177.

[971] See also a discussion on the CJEU approach to the Facebook case, where a duty of cooperation was discussed. - section 3.5.3. of chapter 3.

[972] Autorità Garante della Concorrenza e del Mercato, 'Sanzione Da 3 Milioni Di Euro per WhatsApp, Ha Indotto Gli Utenti a Condividere I Loro Dati Con Facebook' (2017) <http://www.agcm.it/stampa/comunicati/8754-ps10601-cv154-sanzione-da-3milioni-di-euro-per- whatsapp,-ha-indotto-gli-utenti-a-condividere-i-loro-dati-con-facebook.html> accessed 1 May 2022.

[973] See, section 5.2 where I covered the privacy trap theorem.

position by imposing unfair terms, which it could not enforce in a competitive environment.[974] Arguably, the open-ended character of competition law allows for a tailored approach to the unique circumstances of each case. Competition law, in essence, holds a crucial and distinct role in addressing unilateral behaviour that distorts competition. In this respect, competition authorities must prioritise their resources on combating abusive conduct. Competition authorities, while pursuing a case involving exploitative abuse, have to demonstrate that the conduct in question both harms consumers and stems from anticompetitive behaviour.[975] Furthermore, given the comprehensive protection provided by the GDPR, competition authorities are unlikely to argue that in competitive markets data protection regulations should go beyond what is necessary to comply with the GDPR. This suggests that competition authorities are not justified in initiating exploitative misconduct and intervening concerning unfair data protection provisions. Such interventions, essentially, aim to protect the same interests protected by data protection regulations, but they take place within a legal framework in which proving harm is not as easy.

5.5. Conclusions

This chapter presented observations for framing competition law and privacy law together when it comes to assessing privacy-related harms. The aim was to understand the different ways in which competition law and data protection law can affect one another and what circumstances would demand a closer interaction between the regimes. Crucially, there is no analytical framework to define the relationship between competition law and data protection when it comes to privacy-related concerns. I noted that in certain instances Article 102 TFEU could encompass privacy-related harms. Collaborative efforts among authorities can enhance their comprehension of factors influencing market dynamics, aiding in policy development. Conflicts between regulatory regimes must be addressed, as inconsistent policies can jeopardise the overall effectiveness of the regulatory framework.

Additionally, I introduced the privacy-trap theorem, which serves as an attempt to develop a complementary enforcement strategy to solve the issue of consumers having limited control over their data in the online market. The suggested competition authorities can enhance data protection enforcement at various levels while pursuing their primary goal of

[974] Akman (2009) (n 258) 20.

[975] ibid.

preserving market competitiveness. The theorem illustrates that privacy violations can serve as a trigger for assessing competition law, indicating that competition law can only address privacy-related issues when they have a direct impact on competition. Yet, competition law authorities have a limited means to grasp privacy-related infringements. In this respect, I provide a risk-focused approach which follows that it could be necessary to bring clarity in defining the relationship between competition law and privacy. The risk-based approach focuses on creating a more integrated, and holistic approach, respecting the boundaries of competition law and data protection law respectively. The theory is labelled as 'risk-based' since the risks of privacy-related harms are recognised by both the markets and consumers. It was further noted that there are unsolved market failure problems and the tendency to exploit consumers provides for a competition law and data protection law deficit. Correspondingly, the risk-based approach could address the tendencies affecting the digital markets, and privacy-related concerns, enhancing EU legal coherence. It should be kept in mind that competition law can only offer a limited solution to the problem through the economic power of large digital undertakings.

Chapter 6: Conclusions

6.1. Thesis overview: problems and solutions

The thesis focused on defining the relationship between competition law and privacy-related concerns. The key objective was to assess the extent to which Article 102 TFEU could consider privacy-related harms as forming exploitative theories of harm.

The thesis began by indicating that the relationship between competition law and privacy has been seen as novel. The introductory chapter provided an overview of the research aim — whether competition law might acknowledge possible privacy-related harm as a part of an investigation under Article 102 TFEU. I discussed that the growing importance of data introduced the potential to exchange personal information for digital services and content, essentially turning it into commodity. This was the case in both cases of users: (1) paying with their attention and privacy; (2) paying with their attention, privacy and money. The thesis focuses primarily on users paying for digital services with their privacy and attention. I also highlighted why the unique nature of big data and how it derives its value can make it challenging for consumers to make well-informed decisions regarding the terms of sharing their personal data. Chapter 1 also emphasised that applying Article 102 TFEU to data privacy violations has raised concerns about the equilibrium between competition law and data protection law. Data protection regulation is primarily intended to address the issue of individuals' loss of control over personal data and is typically considered the initial course of action. However, the data protection regulatory framework does not encompass the influence of market power on individuals' interests, a domain that falls under the purview of competition law. Competition law is designed to uphold the competitive process and safeguard consumers' economic interests by preventing the unlawful exercise of market power.

Based on this, Chapter 2 assessed the most discussed theories about competition law and privacy concerns: integrationist, separatist and value pluralism theories. The interconnectedness of data protection and competition law, along with their potential for collaboration, has been acknowledged in academic literature and recognised by the relevant authorities for some time. Regarding the evaluation of policy coordination, it was significant to note that EU competition law is not a standalone statute but rather a component of a

larger framework known as the TFEU. As a result, the competition authorities may resolve each case by adapting broad principles to the issue at hand. Since competition law does not exist in a vacuum and is intertwined with societal values, the conceptual background of the EU competition law indicated the absence of a single unifying policy.

Thus, Chapter 2 has made the case that there are other elements besides data that can influence competition in each market. In essence, the most complicated issues for courts and agencies are those involving possible mutuality between competition law and data privacy legislation, rather than their complementarity; these situations call for novel analytical trade-offs and approaches. The courts and competition authorities may be helped in coming to a context-specific and principled judgments by possible value pluralism initiatives to create a framework for balancing competition law with data protection. This is not meant to imply that competition legislation would be a "magic bullet" for all privacy issues. The assessment of competition law should instead consider objectives like economic freedom, consumer welfare, fairness, and transparency in law. The Commission contends that evaluations of competition do not immediately take data privacy into account. EU competition law functions within the more expansive TFEU framework, allowing for case-specific adaptation. Instead of a straightforward association, cases frequently result from potential connections between competitiveness and data privacy regulation. The goals of Article 102 TFEU include general consumer welfare, which includes harm caused by exploitation.

Chapter 3 addressed the enforcement issues regarding the interaction between competition law and data protection law. Taking a comprehensive approach to examining the interrelationship between these regulatory frameworks allows to uncover novel ways in which these regimes can enhance each other's effectiveness to develop a more cohesive approach. Chapter 3 discussed three prescriptive positions which emphasise for the need to have a coherent approach to the interaction between the regimes: from emphasising that competition law does not apply to data privacy law to pondering the possibility that competition law might acknowledge privacy infringements in the context of the broader legal and economic framework around the activity in question. From a substantive point of view, I did not propose that both competition law and data protection law should incorporate objectives beyond their scope. Instead, I proposed that it should acknowledged

that a cooperative interaction could be beneficial. This is based on mutual reinforcement in general and the possibility of cooperation when actions may have unintended consequences. I emphasised that privacy protection can only impact competition law when privacy is a key parameter of competition and this is not the case for consumer communication apps where price, user base, popularity or reliability are important factors. As this approach suggests, any privacy infringements could be relevant from a competition law perspective only if privacy-related harm is considered in a broader context surrounding the conduct in question. This chapter used the German Facebook's case as an attempt to bring competition law and data privacy law together. The BKartA used data protection law as a benchmark to establish the abusive nature of Facebook's conditions and applied German competition law to determine whether Facebook's requirement for consent to combine personal data from various sources was prohibited as an exploitative abuse by a dominant undertaking.[976] AG Rantos and the CJEU evaluated the overlap between competition law and demonstrated how incidental study of data privacy law in competition law evaluation may serve as a proxy for discovering an exploitative exploitation in a wider economic context.[977]

Based on the findings, I turned to the question whether privacy-related harms might form exploitative theories of harm under the traditional competition law. Chapter 4 offered an analysis of theories of harms as per Article 102 TFEU. The problems arising from practices of large digital firms are not confined to the competition paradigm only. This raises an important consideration of the need to develop a well-sustained understanding of whether privacy harms might be accounted as a competitive theory of harm.

Privacy might bear a positive connotation, and serve as an intermediate good, in situations where nondisclosure of data is beneficial for a data subject, or when users decide to disclose their data to obtain a monetary payment. However, one concept remained certain — there is a lack of understanding of how privacy concerns could amount to the theory of harm. The discussion in Chapter 4 demonstrates how privacy-related concerns might be annexed as a theory of harm under Article 102 TFEU. As privacy-related harms are often sourced from extensive data acquisition, this thesis offered to only focus on exploitation theories of harm.

---

[976] *Facebook* (n 2).

[977] *Meta Platforms, Opinion of AG Rantos* (n 85); *Meta Platforms* (n 41).

This forms a departure from a long-lasting emphasis on EU exclusionary abuses.[978] Large digital undertakings generate personal or industrial data on big scale sufficient for machine learning purposes. There might be able to collect and process unlimited amounts of data by exploiting their position in their relevant markets.[979] Such conduct, in turn, relates more to the exploitation of users rather than their exclusion. At the European level, privacy-related harms might amount to exploitative abuse under Article 102 TFEU, taking the form of excessive price, or unfair terms and conditions. Arguably, competition law could act as an effective practical tool for protecting privacy. However, using competition law alone, without considering privacy regulation, will not lead to the desired outcome. Competition law should intervene in conduct involving privacy-related theories of harm only if privacy-related harm relates to the market failure, not to the privacy rights itself.

A legal solution is required which maps the confusing relationship between competition law and data privacy law. Digital markets have unquestionably linked competition law with data privacy law concerns. Lack of control over personal data appears to be the 'core theme' for consumers and might lead to market failures that impact on a market's optimal performance with respect to user privacy. Fundamentally, competition law is a tool for managing the private market: that is, the exchange of goods and services for value between individual particulars in the market. By recognising the aggregation of personal data as a potential source of market power, competition law enforcement might provide recourse where companies use their market power to collect more data and introduce misleading privacy protection initiatives.[980] To address such a complex interaction between competition law and data privacy law, however, a coherent approach to law enforcement is necessary. However, it is important to keep competition law and data protection as separate. Maintaining the analytical independence of competition law and data protection might contribute to the achievement of predictability. In such instances, competition authorities could approach competition law infringement in the traditional approach of Article 102 TFEU to assess if privacy-related infringement has had a negative effect on competition law and consumer

[978] Miriam Caroline Buiten, 'Exploitative abuses in digital markets: between competition law and data protection law' [2021] Journal of Antitrust Enforcement 270; H Schweitzer, ' The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal' [2021] ZEuP 503.

[979] Gebicka and Heinemann (n 217) 165.

[980] See mainly, Kerber and Specht-Riemenschneider (n 716).

welfare. Correspondingly, Chapter 5 offered an evidence-based approach was offered, called 'the privacy trap'. I develop this theorem as an attempt to point that privacy infringements can act as a proxy to trigger competition law assessment in certain instances. The aim here was to demonstrate that competition law could act as an effective practical tool for protecting privacy. Yet, as noted, competition law could only answer privacy-related concerns if they directly influence competition. In other words, to achieve the clarity in defining the relationship between competition law and privacy, it was suggested that a more robust cooperation between competition authorities and data protection authorities is needed to understand the precise impact of privacy-related harms and its potential limit of competition in each market. It should be kept in mind that competition law can only offer a limited solution to the problem through the economic power of the large digital undertakings.

The goal of the thesis was not to provide a definitive answer but to stimulate thought and discussion on the relationship between these regulatory frameworks. I conclude that there is scope to make the traditional competition law enforcement effective in addressing consumer disempowerment concerning personal data requires making their approaches more cohesive, identifying opportunities for synergy, and gaining a better understanding of the actual dynamics of these markets, including their shortcomings. Although I kept practical considerations in mind when researching and writing this thesis, I am confident that the open-minded nature of Article 102 TFEU at both theoretical and practical levels, can consider possible privacy harms as distorting competition on the merits.

6.2. Approach adopted

Competition law and privacy were chosen for an in-depth investigation as it remains unclear to what extent competition law might remediate user data privacy concerns. In pursuing a solution, the starting point was the relationship between competition law and data privacy law. A reliance on the digital products and services, which collect and process personal, data has blurred the divide between privacy and competition law regulation. The discussion in this thesis refers to the GAFAM company practice as they remain the most influential firms in the digital economy, controlling digital behaviour and market forces. Arguments have been tested throughout this thesis using examples of previous competition proceedings at

the EU level, concerning Big Data, and reports from competitive authorities. From this foundation, five proposals have been developed.

This work has reviewed EU competition law and data protection law with the emphasis on their relationship with protecting user privacy (both through case law and in theory), their own enforcement system and the extent in which competition could acknowledge privacy-related harms. I noted that both competition law and data protection law aim to address digital market failures which prevents achieving an optimal level of protection. Although I discussed that competition law will not remediate them all, the market failures approach was used as a proxy to demonstrate instances in which competition law might trigger its assessment under Article 102 TFEU and provides some form or enforcement system. Against that background, I concluded that EU competition law might consider abuses related to extensive data collection. From a structural perspective, the most effective means of proceeding would be to consider privacy-related harm as forming a part of a broader category of data related harms — exploitative harms, taking form of extensive data acquisition or unfair trading conditions.

In developing this solution, I adopted a macro-level approach on the relationship between EU competition law and data privacy harm. This was done in light of the previous competition law proceeding relating to Big Data at the EU-level, in respect of the relationship between competition and data protection law; the common mutualities between competition and data protection law; the EU competition law approach to privacy-related harms under Article 102 TFEU; and the potential for justification of the privacy-related harms as being pro-competitive in light of efficiency defence under Article 101(3) TFEU. The macro-level approach also assessed the views of various competition law authorities at the EU level and reports that attempted mapped out the intersection between competition law and data protection law.

6.2.3. Proposals developed

Throughout this thesis, I developed considerations on competition law and privacy-related harms. These are summarised in this section.

Firstly, I noted that EU competition law and data privacy are overlapping in complex and multifaceted ways particularly in the digital economy.[981] **Secondly**, although EU competition law and data protection law are seen as interlinked, this thesis argues that this does not suggest that EU competition law could and should be extended to remediate all privacy-related harms.[982] Competition law should only intervene in data-related market failures where a digital undertaking unilaterally engages in a misconduct that limits competition.

Taken together, I assessed on the extent in which EU competition law might acknowledge any privacy-related harms while establishing an abuse under Article 102 TFEU. Therefore, **thirdly,** I proposed that EU competition exploitative theories of harm, as per Article 102 TFEU, can consider privacy-related harms in a broader scope of the legal and economic context surrounding the conduct to establish if the conduct introduced distortion to merit-based competition. Article 102 TFEU is enough broad to cover various types of exploitative conducts.[983] Excessive data acquisition could be captured as a form of unfair trading conditions, or excessive pricing vis-a-vis excessive data acquisition (or excessive subscription fee payment) within the meaning of Article 102(a) TFEU. In my analysis, two arguments could be considered used in relation to data-driven theories of harm. Firstly, network effects are strong in the data-driven markets. Here, large digital firms collect and process more data and thereby effectively creating high entry barriers and limiting consumer choice. Secondly, such a tipping effect might spill over to related data-oriented markets. Google's and Apple's pro-user and pro-privacy advancement could advance consumer fallacy and act as a proxy to further data collection of digital giants and exploit users. Therefore, there could be two ways in which privacy could intersect or influence competitive theory of harm: increased and decreased privacy protection strategy by Big Tech firms, as per the latest pro-privacy terms and conditions amendments, which increases product quality, as offered by Google and Apple.[984] The element of increased privacy protection deals with requiring users to consent to data collection. This reasoning has been noted in the Facebook case.[985]

---

[981] See a discussion in Chapter 2.

[982] See a discussion in Chapter 3 where I discussed the case-law relating to Article 102 TFEU and privacy-related harms.

[983] See a discussion in Chapter 4. Here, I demonstrated that Article 102 TFEU has a flexible tendency to consider external-to competition law policies they enable to capture anticompetitive conducts.

[984] See Chapter 3 in general.

[985] *Facebook case* (n 2)

Fourthly, it was noted that large digital undertakings might rely on improvements of privacy to avoid anticompetitive liability, within Article 102 TFEU.[986] Though this theory is at an early stage, there are questions about whether the increased protection for individual data privacy could justify otherwise anticompetitive conduct. There are two possibilities. Firstly, to successfully apply can the efficiency defence, large digital undertakings have to satisfy the accumulative criteria defined by EU case law, not only consumer choice criterion. Hence, privacy-enhancing technologies might exonerate abuse of dominant position if merged with reduction of consumer choice. Secondly, as per concept of objective justifications in abusive conduits, it remains unclear if EU competition law interprets any privacy concerns as objective justifications.

Fifthly, competition law should intervene in conduct involving privacy-related theories of harm only if privacy-related harm relates to market failure, not to the privacy rights itself.[987] In other words, it is the conduct that not merely involves data mistreatment, and breaches of user privacy, but the conduct must have a negative impact on the competition. Reduction in privacy may not necessarily amount to a competitive issue; any reduction of privacy equally may not immediately breach data privacy law if the data processes comply with data protection law. In this respect, this work developed an effect-based approach, called the privacy trap. The analysis of case law offered in this thesis demonstrates that EU competition authorities consider the data-related impact on limiting consumer welfare and competition. Accordingly, if privacy-related harms are not seen as an autonomous argument but affixed to a broader data-relating theory of harm, then they could be taken into account under Article 102 TFEU.

Fundamentally, the purpose of competition law in digital economy should ensure the right balance between static and dynamic efficiencies. This is only possible if the economic and legal considerations are assessed within antitrust investigation. This will require an effect-based test.

---

[986] See chapter 4 for a more detailed discussion, section 4.2.2(2).

[987] See chapter 5, where I discussed the' privacy trap' theorem. The theory emphasises on the open-ended nature of Article 102 TFEU.

6.3. Potential limitations

Development of the above described arguments would not be possible without limiting the scope of this thesis. In this section, the limitations of this thesis are summarised.

Firstly, this thesis focuses only on the relationship between competition law and privacy from a perspective of the traditional EU competition law. The discussion does not cover the DMA, as having no strictly legal impact on Article 102 TFEU, and its precise relationship between Article 102 TFEU is still debated. Also, the issues of whether competition law might annex privacy-related harms as a part of competitive parameter arise not only in the EU. The discussion of this work might have an impact on EU competition law, yet this does not suggest that the solution developed in this thesis might apply elsewhere, given its focus on EU legislations. Nevertheless, this thesis might provide a starting point for substantial work in different jurisdictions considering their own competition law rules, international law,[988] constitution, or approach to privacy law, as a part of fundamental rights. The thesis has identified consistencies across different national competition legislations, and regulatory approaches to competition law and privacy protection.

Secondly, the research focuses only on exploitative theories of harm. EU competition law does not penalise for being a dominant undertaking in each market. EU competition law would only intervene when there is evidence of an abuse of dominant position in which an undertaking unilaterally engages in a misconduct that limits competition. Mostly, the focus is on preventing practices that negate consumer welfare, and such practices are categorised as exclusionary and exploitative theories of harm. For a long time, competition law enforcement primarily fluctuated around exclusionary, rather than exploitative abuses.[989] The influence of digital industries, especially the GAFAM companies and an increased reliance on zero-priced digital products and services, created market failures that could be grounds for competition law enforcement. Most EU competition law proceeding, as discussed in this thesis, do not directly discuss the impact of unilateral conducts on user privacy. Data related theories of harm are not novel, and the attention given to them has been proliferated by the rise of the digital economy. Also, data accumulation is not abusive

[988] Douglas (n 158).

[989] Guidance on the Commission's Enforcement Priorities in Applying Article 82 (n 87); Botta and Wiedemann (2019) (n 415); Buiten (n 978) 270; Schweitzer (n 978).

on its own, and might contribute to service improvements. In fact, the essential element that creates competition law violation relates to some form of conduct that might be regarded as abuse of dominant position. As this thesis solely considered the extent to which existing EU competition law rules might accommodate privacy-related harms, the focus was on exclusionary theories of harm. This thesis has not considered exclusionary theories of harm, which have been considered in multiple jurisdictions, and did not provide an overview of privacy-related effects on them.[990] Such limitation corresponds to the idea that the collection and processing of personal data has allowed for the creation of markets for the acquisition and sale of users's data to digital platforms and service providers. In such consideration, exploitative theories of harm were connected to large digital undertakings extracting excessive data collection or providing unfair terms and conditions. They emphasise on the unique interaction between competition law and privacy.[991]

6.4. Future research

Several potential research projects might build on the findings of this thesis. As mentioned in the introduction, this thesis aimed to assess if existing EU competition law could accommodate privacy-related harms as an element of the theory of harm under Article 102 TFEU. The assessment was carried out from a 'macro approach' on the EU contract. As a result, this thesis: 1) discussed three theories of harms annexing privacy-related harms; 2) developed the stance that privacy-related harms might form a part of efficiency defence arguments; and 3) demonstrated a theory which envisages the nexus between competition law and privacy-related-harms. To an extent, this was possible due to the stated limitation, namely the omission of exclusionary theories of harm. This thesis assumes that privacy-related harms connote exploitation of digital end-users; privacy protection is a highly personalised concept and varies amongst societal perspectives.

One potential future research project is to work on establishing the competitive effects of privacy protection. This is a rapidly developing area of law. The intersection between competition law and data privacy is new, but the benefits from continuous evaluation with existing tools have been expanded in cases relating to extensive data acquisition. In practical terms, future research should consider: *how might competition authorities measure the*

[990] An overview of possible exclusionary theories of harm can be found in Douglas (n 158) 107-108.

[991] See the discussion of the *Facebook case* saga, section 3.5.

relevant effect of privacy-related harms in each market? What evidence is precisely needed to consider a potential privacy infringement as affecting consumers in each market? As this thesis has found, there is a possibility of considering privacy-related harms as a part of the competition theory of harm when privacy-related harms are considered from a broader perspective of competitive harm. In other words, competition law might acknowledge any deviation in offered privacy protection indirectly. It means that existing competition law tools might annex privacy-related harms when any extensive data acquisition of a monopolist directly corresponds to exploiting users in each market. More cases might come to light where exercised monopoly power reduces personal data privacy. This raises an important opportunity to develop well-sustained methods and tools for measuring competitive effects on privacy. Such research might take the form of evidence-based approaches, which allow for collaboration between data privacy and antitrust authorities. Data privacy authority expertise might enrich competition law's approach to understanding the scope of privacy interest adequately and accurately in each market. Equally, the privacy-related experience might help to determine if gatekeepers are obliged with relevant data protection rules to the extent that does not limit competition, nor exploit digital users. Such collaboration might allow the development of competitive tools and methodologies in which competition authorities understand how to evaluate privacy-relates harms and their effect on competition. It would also allow a development of an understanding of whether privacy-related harm might impact the features or quality of products and services in each market.

Another potential research project might investigate the question at a micro-level scale to EU Member States. This work considered the extent to which existing EU competition law could incorporate privacy-related harms. This thesis adopted a macro-level approach and discussed the impact of privacy-related harms on existing EU competition law tools. Although this offered an overview of the BKartA *Facebook case* as an example of the Member State approach to acknowledge the apparent intersection between the phenomena of competition law and privacy, there does not appear to be any research that has considered a micro-level approach of each Member State to the intersection between competition law and privacy. The introduction of Member State perspective could have a significant impact on the anticompetitive potential that arises from extensive data acquisition. The most prominent example remains the *Facebook case*, which was extensively covered in this thesis. However, other Member States, such as Italy or Ireland, have adopted

a different stance to the intersection between competition law and privacy. The Italian Antitrust Authority, in its proceeding against Facebook, concluded that the economic value of personal data also complies with consumer law, with Facebook having a duty to properly inform consumers and users about its commercial purposes of the data collection. In addition, it was held that competition law was closely interlinked with consumer law and data protection law, as they all aim to remediate exploitation of digital users.[992] Therefore, it remains to be seen how the Member States will approach competition law and privacy-related harm at the practical level. The debate around data relates only to the common grounds between competition law and data protection law, namely arguing that data is a factor contributing to market power, increasing market transparency, and acting as a competitive instrument. This raises a further question: should competition law make end-users better? And, if so, how? The Member State approach might offer an interesting analytical overview which could allow for the development of tools and methods that acknowledge privacy-related harms in competition law assessment, even if they should be seen as indirectly remediated by competition law. On a similar note, an international perspective might offer similar outcomes. To reconcile this approach, any potential competition law amendments should ensure that companies cannot obtain or maintain a dominant position through competition law means, and they should aim to ensure that overall consumer welfare is increased.

[992] Decisione TAR n. 260/2020 *Il Consiglio di Stato su AGCM c. Facebook – 1;* or Maciej Janik and Marta Sznajder, 'Main Developments in Competition Law and Policy 2022 – Poland' (Kluwer Competition Law, 2023) < https://competitionlawblog.kluwercompetitionlaw.com/2023/05/23/main-developments-in-competition-law-and-policy-2022-poland/> accessed 24 November 2023. Poland does not consider non-competition law factors when investigating possible unilateral conducts.

Bibliography

Primary sources

EU Treaties

Consolidated Version of the Treaty on the Functioning of the European Union, 2008 OJ C 115/47

Charter of Fundamental Rights of the European Union 2010 OJ C 83/02

EU Legislations

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

Council Regulation (EC) No. 139/2004 on the Control of Concentrations between Undertakings (the EU Merger Regulation) [2004] OJ L24/1

Council Regulation (EC) of 5 February 2004 on Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2004/C 31/03) [2004] OJ C 31/5

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201/37 Commission Nationale de l'Informatique et des Libertés, 'Cookie walls : la CNIL publie des premiers critères d'évaluation', 16 May 2022, <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation> accessed 19 April 2024.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), article 5(2).

Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (Text with EEA relevance.) PE/42/2018/REV/1

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/ EC, [2019] OJ L-130/92.

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)

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1

European Commission decisions and European Court of Justice judgments

C-107/82 *AEG-Telefunken* v *Commission* ECLI:EU:C:1983:293

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

C-41/96 - VAG-Händlerbeirat eV v SYD-Consult 1997 I-03123

C-439/09 Pierre Fabre Dermo-Cosmétique EU:C:2011:649

C-457/10 P AstraZeneca/Commisson ECLI:EU:C:2012:770

Case 226/84 British Leyland Public Limited Company v Commission of the European Communities. Cominant position - Type approval for motor vehicles ECLI:EU:C:1986:421.

Case 26/75 General Motors v Commission [1975] ECR 1367

Case 26/76 Metro SB-Großmärkte v Commission [1977] ECR 1875

Case 262/81, Coditel SA, Compagnie générale pour la diffusion de la télévision, and others v Ciné-Vog Films SA and others ('Coditel II'), EU:C:1982:334.

Case 283/81 CILFIT and Lanificio di Gavardo SPA v Ministry of Health (1982) ECHR 3415

Case 395/87 Ministère public v. Jean-Louis Tournier, [1989] ECR 2521.

Case 42/84 Remia v Commission [1985] ECR 2545

Case 6-72 Europemballage Corporation and Continental Can Company Inc. v Commission [1973] ECR-215

Case AT.39740 Google Search (Shopping), 27 June 2017

Case AT.39984, Romanian Power Exchange/OPCOM [2014].

Case AT.40099 – *Google Android,* Commission decision of July 18, 2018

Case AT.40178, *Car Emissions* [2021].

Case C- 85/ 76, Hoffman-La Roche & Co v Commission [1979] ECR 461

Case C-112/00 *Schmidberger* [2003] ECR I-5659

Case C-117/20 *bpost*, Opinion of 2 September 2021, ECLI:EU:C:2021:680

Case **C**-127/73 *BRT v SABAM;* ECLI:EU:C:1974:25, 27/03/1974

Case C-151/20 *Nordzucker,* ECLI:EU:C:2021:681

Case C-165/19 P, *Slovak Telekom* [2021] ECLI:EU:C:2021:239

Case C-17/10 *Toshiba Corporation et al*, Opinion of 8 September 2011, ECLI:EU:C:2011:552

Case C-179/90 Merci Convenzionali Porto di Genova SpA v Siderurgica Gabrielli [1991] EU:C:1991:464

Case C-194/14 P, *AC Treuhand,* 22 October 2015, ECLI:EU:C:2015:717
Case C-202/07 P, France Télécom v Commission ECLI:EU:C:2009:214

Case C-203/08 *Sporting Exchange* [2010] ECR I-4695, Opinion of AG Bot

Case C-209/10 Post Danmark A/S v Konkurrencerådet, EU:C:2012:172

Case C-23/14, Post Danmark A/S v. Konkurrencerådet (Post Danmark II) EU:C:2015:651; 6 September 2017

Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios ECR I-11125. [2006]

Case C-252/21 *Meta Platforms and Others* (Conditions Générales d'Utilisation d'un Réseau Social)

Case C-252/21, Request for a preliminary ruling, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social) 22/04/2021

Case C-252/21, Request for a preliminary ruling, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social) ECLI:EU: C:2022:704, Opinion of AG Rantos

Case C-27/76 United Brands Company and United Brands Continentaal v Commission, [1978] EU:C:1978:22.

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

Case C-307/18, Generics (UK) and Others v. Competition and Markets Authority, EU:C:2020:52; 25 March 2021

Case C-309/99 Wouters v Algemene Raad van de Nederlandse Orde van Advocaten, [2002] E.C.R. I-1577.

Case C-322/81 NV Nederlandsche Banden Industrie Michelin v Commission [1983] ECR I-3461

Case C-333/94P Tetra Pak International SA v. Commission (Tetra Pak II), [1996] ECR I-5951

Case C-377/20 Servizio Elettrico Nazionale ECLI:EU:C:2022:379

Case C-40/73, *Suiker Unie*, 16 December 1975, ECLI:EU:C:1975:174

Case C-413/14 P, *Intel v. Comm'n*, EU: C:2017:632

Case C-42/07 Liga Portuguesa de Futebol Profissional and Bwin International [2009] ECR I-7633, Opinion of AG Bot

Case C-468/06 Sot. Lélos Kai Sia v. GlaxoSmithKline [2008] ECR I-7139

Case C-52/09, Konkurrenverket v TeliaSonera Sverige AB ECLI:EU:C:2011:83

Case C-53/03, *Syfait and Others* [2005] ECLI:EU:C:2004:673, Opinion of AG Jacobs

Case C-609/13 P, *Duravit*, 26 January 2017, ECLI:EU:C:2017:46

Case C-617/10 *Åkerberg Fransson*, Judgement of 26 February 2013, ECLI:EU:C:2013:105

Case C-617/17 *Powszechny Zakład Ubezpieczeń na Życie*, Opinion of 29 November 2018, ECLI:EU:C:2018:976

Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801

Case C-680/20 Unilever Italia Mkt. Operations Srl v Autorità Garante della Concorrenza e del Mercato, EU:C:2023:33.

Case C-8/08, T-Mobile Netherlands BV, KPN Mobile NV, Orange Nederland NV and Vodafone Libertel NV v Raad van bestuur van de Nederlandse Mededingingsautoriteit ECLI:EU:C:2009:110

Case C-95/04 British Airways plc v Commission [2007] ECR 1-2331

Case C-549/10 P Tomra Systems ASA and Others v European Commission ECLI:EU:C:2012:221.

Case C-61/19, Orange Romania EU:C:2020:901

Case COMP/39.525 *Telekomunikacja Polska*, Decision of 22 June 2011.

Case M.8788, *Apple/Shazam* 6 February 2018.

Case M.9660 – *Google/Fitbit* (Commission decision of 17 December 2020)

Case ME/5525/12-Anticipated acquisition by Facebook Inc of Instagram Inc, 14 August 2012

Case No COMP/37685, *GVG/FS* (2004)

Case No COMP/M.5727 – *Microsoft/Yahoo!* OJ L 24, 29.1.2004

Case T- 111/96 ITT Promedia v Commission 17 July 1998.

Case T-111/08 Mastercard v Commission EU:T:2012:260.

Case T-112/99 Métropole Télévision (M6) v Commission EU:T:2001:215

Case T-139/98 Amministrazione Autonoma dei Monopoli di Stato (AAMS) v Commission [2001] ECR II-3413

Case T-139/98 Amministrazione Autonoma dei Monopoli di Stato (AAMS) v Commission ECLI:EU:T:2001:272

Case T-151/01 Duales System Deutschland EU:T:2007:154.

Case T-172/21 *Valve Corporation v Commission*. Luxembourg, 27 September 2023.

Case T-201/04 Microsoft Corpn v Commission [2007] ECR II-3601

Case T-219/99 British Airways plc v Commission, EU:T:2003:343

Case T-235/18, Qualcomm Inc v Commission, 15 June 2022.

Case T-30/89, *Hilti v Commission* [1991] ECLI:EU:T:1991:70

Case T-313/02 David Meca Medina and Igor Majcen v Commission ECLI:EU:T:2004:282

Case T-321/05 AstraZeneca AB and AstraZeneca plc v European Commission [2010] ECR II-2805

Case T-329/01 *Archer Daniels Midland v Commission*, Judgement of 27 September 2006, ECLI:EU:T:2006:268

Case T-38/02 *Groupe Danone v Commission*, Judgement of 25 October 2005, ECLI:EU:T:2005:367

Case T-399/16 CK Telecoms UK Investments Ltd v EC [2020] ECLI:EU:T:2020:217

Case T-512/12 *Front Polisario*, ECLI:EU:T:2015:953.

Case T-59/02 *Archer Daniels Midland v Commission*, Judgement of 27 September 2006, ECLI:EU:T:2006:272

Case T-604/18 *Google & Alphabet v EC* (*Google Android)* [2022] ECLI:EU:T:2022:541

Case T-612/17, Google v Commission (Google Shopping), 10 November 2021

Case T-83/91 Tetra Pak International SA v Commission [1994] ECR II-755

Case T–203/01 Manufacture française des pneumatiques Michelin v Commission Judgment of 30 September 2003, ECLI:EU:T:2003:250

Case T–228/97 *Irish Sugar Plc v Commission* Judgment of 7 October 1999, ECLI:EU:T:1999:246

Case-319/20, Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen and Verbraucherverbände – Verbraucherzentrale Bundesverband eV (28 April 2022) ECLI:EU:C:2022:322

CJEU 17 January 1984, VBVB and VBBB vs. Commission, Joined Cases 43 and 63/82ECR

CMA, Case 50972 *Google Privacy Sandbox* Commitments (4 February 2022)

Commission Decision 97/745/EF *Port of Genoa* [1997] L 301/27

Commission decision IV/29.971 of 4 December 1981, *GEMA II*, OJ 1982 L 94/12

Commission Decision of 11 June 1993, IV/32.150 - *EBU/Eurovision System*, 93/403/EEC, *OJ*, 22 June 1993 L179/23

Commission Decision of 12 December 1990, IV/32.363 – *KSB/Goulds/Lowara/ITT,* 91/38/EEC, *OJ*, 25 January 1991, L 19/25

Commission Decision of 14 January 1992, IV/33.100 *Assurpol*, 92/96/EEC, OJ, 14 February 1992, L 37/16

Commission Decision of 16 October 2003, COMP D3/35470 — *ARA*

Commission Decision of 17 September 2001, COMP/34493 – DSD, 2001/837/EC, *OJ*, 4 December 2001, L319/1

Commission Decision of 23 December 1992, IV/33.814 - *Ford Volkswagen*, 93/49/EE, OJ, 28 January 1993, L20/14.

Commission Decision of 24 January 1999, (IV.F.1/36.718. – *CECED*), 2000/475/EC, OJ 26 July 2000, L187/47

Commission Decision of 25 November 1981, IV/428, *VBBB/VBVB*, 82/123/EEC, OJ 25 February 1982, L54/36

Commission Decision of 29 September 2010, *ENI* (Case COMP/39.315), OJ 2010, C352/8.

Commission Decision of 4 July 1984, 84/380/EEC *Synthetic Fibres*, OJ 1984, L207/17.

Commission Decision of 8 December 1983, IV/29.955 – *Carbon Gas Technologie*, 83/669/EEC, *OJ*, 31 December 1983, L 376/17

COMP D3/35473 — *ARGEV, ARO*, 2004/208/EC, *OJ*, 12 March 2004, L 75/59.

Deutsche Post AG (Case COMP/C-1/36.915) Commission Decision 2001/892/EC [2001] OJ L331/40

Google/DoubleClick (Case COMP/M.4731) Commission Decision [2008] OJ C184/10

Joined Cases 1377/5/7/20 and 1378/5/7/20, Epic Games Inc, Epic Games International SARL and Epic Games UK Ltd v Apple Inc and Apple (UK) Ltd

Joined Cases 209/78 to 215/78 – Heintz van Landewyck SARL v Commission [1980] ECR 3125

Joined Cases 56/64 and 58/64, *Consten-Grundig* ECLI:EU:C:1966:41

Joined Cases C-501/06 P, C-513/06 P, C-515/06 P and C-519/06 P, *GlaxoSmithKline Services and Others v Commission and Others* ECLI:EU:C:2009:610.

Joined Cases T-213/01 and T-214/01 Österreichische Postsparkasse AG and Bank für Arbeit und Wirtschaft AG v Commission [2006] ECR II-1601

Telefónica UK/Vodafone UK/Everything Everywhere/JV, No COMP/M.6314, 4 September 2012

TomTom/Tele Atlas, Case No COMP/M.4854, Decision of 14.5.2008

Virgin/British Airways (Case IV/D-2/34.780) Commission Decision of 14 July 1999.

Wanadoo España v Telefónica (COMP/38.784) Commission Decision 4 July 2007

Italian case law

Decisione TAR n. 260/2020 *Il Consiglio di Stato su AGCM c. Facebook – 1*

US case law and legislation

FTC, *Google/DoubleClick* [2008] FTC File No. 071-0170 6:

German case law and legislation

Act Against Restraints of Competition 2013, as last amended by Article 10 of the Act of 12 July 2018

BGH, 07.06.2016, KZR 6/15, *Pechstein/International Skating Union*

Bundeskartellamt, 'Decision B7-70/21, Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB, adopted in the administrative proceedings involving Alphabet Inc., Google Ireland Limited and Google Germany GmbH' < https://www.bundeskartellamt.de/SharedDocs/Entschei-> accessed 1 May 2024.

Case 1 BvR 209/83 et al., *Volkszählungsurteil*, 15 December 1983, 65 BVerfGE 1

Case B6-22/16 *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*. <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108> Accessed 28 August 2019

Case KVR 69/19, *Facebook v Bundeskartellamt* <https://www.bundesgerichtshof.de/SharedDocs/Termine/DE/Termine/KVR69-19.html;jsessionid=F09CB5804920B1DDFF6B994C11C0E3D8.2_cid286?nn=11439166> accessed 30 June 2020

Case KVZ 90/20, *Facebook,* BGH, 15.12.2020

Competition Act in the version published on 26 June 2013 (Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245), as last amended by Article 2 of the Act of 19 July 2022 (Federal Law Gazette I, p. 1214) (GWB)

OLG Düsseldorf (2019). Order of 26.08.2019, Case VI-Kart 1/19 (V) ECLI:DE:OLGD:2019:0826.VIKART1.19V.0A

French proceedings

Autorité de la Concurrence, Décision N° 14-MC-02 du 9 Septembre 2014 Relative à une Demande de Mesures Conservatoires Présentée par la Société Direct Energie dans les Secteurs du Gaz et de l'électricité, September 9, 2014

Autorité de la Concurrence Decision 19-D-26, 19 December 2019 (*Google Ads Rules*) < https://www.autoritedelaconcurrence.fr/en/decision/regarding-practices-implemented-sector-online-search-advertising-sector> accessed 16 April 2024.

Autorité de la Concurrence, Decision 21-D-07 of 17 March 2021<https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2021- 04/21d07_en.pdf> accessed 24 November 2023.

Autorité de la Concurrence Decision 21-D-17, 12 July 2021 (*Google News*) <https://www.autoritedelaconcurrence.fr/fr/decision/relative-aurespect-des-injonctions-prononcees-lencontre-de-google-dans-la-decision-ndeg> accessed 16 April 2024.

GDF Suez Décision n° 14-MC-02 du 9.9.2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité) (2014) <https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9-september-2014-gas-market> accessed 23 November 2023.

Law 2019-775 tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse, 24 July 2019, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038821358> accessed 18 April 2024

Paris Court of Appeal, 20/03811 Google (7 April 2022)

UK Competition Market Authority proceedings

Epic Games Inc and Epic Games International SARL v Alphabet Inc, Google LLC, Google Ireland Ltd, Google Commerce Ltd, Google Payment Ltd (UK CAT, 22 February 2021, Roth LJ)

Austrian proceedings

Österreichische Datenschutzbehörde, Decision on Complaint Dated 25 May 2018 GZ: DSB-D122.931/0003-DSB/2018, Issued on 30 November 2018 <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf> assessed 19 April 2024.

Irish proceedings

DPC Inquiry Reference: IN-20-7-4 (2022) <https://www.dataprotection.ie/sites/default/files/uploads/2022-09/02.09.22%20Decision%20IN%2009-09-22%20Instagram.pdf> accessed 25 October 2022.

Irish Data Protection Commission, Final Decision against Meta Platforms Ireland Limited (Facebook service), DPC Inquiry Reference: IN-18-5-5, 31 December 2022 <https://www.dataprotection.ie/sites/default/files/uploads/2023- 04/

M e t a % 2 0 F I N A L % 2 0 D E C I S I O N % 2 0 % 2 8 A D O P T E D % 2 9 % 2 0 3 1 - 1 2 - 2 2 % 2 0 - %20IN-18-5-5%20%28Redacted%29.pdf> accessed 19 April 2024.

Secondary sources

Academic articles and book chapters

Acquisti A, Brandimarte K, Loewenstein G, 'Privacy and human behaviour in the age of information' (2015) Science.

Acquisti Alessandro and Gross Ralph, 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook', In Danezis G, Golle P (eds), *Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, vol 4258* (Springer, 2006).

Acquisti Alessandro, Taylor Curtis and Wagman Liad, 'The Economics of Privacy' [2016] J Econ Lit 422

Ahdar R, 'Consumers, redistribution of income and the purpose of competition law' (2002) 23 European Competition Law Review 341

Akman Pinar, 'Exploitative Abuse in Article 82EC: Back to Basics?' (2009) ESRC Centre for Competition Policy CCP Working Paper No 09-1.

Akman Pinar, 'Searching for the Long-Lost Soul of Article 82 EC' (2009) 29 2 OJLS 267.
Akman P, 'A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets' [2022] Virginia Law & Business Review 1.

Alhborn Christian and Grave Carten, 'Walter Eucken and Ordoliberalism: An Introduction from a Consumer Welfare Perspective' (2006) 2 Competition Policy International, 199/200.

Andreangeli A, 'Case note on T-201/04, Microsoft v Commission, Judgment of 17 September 2007' [2008] Common Market Law Review 863.

Arrow KJ, 'Welfare and the Allocation of Resources for Invention' in R Nelson (ed) *The Rate and Direction of Economic Activities: Economic and Social Factors* (NBER Books 2016)

Averitt N and Lande R, 'Consumer Choice: The Practical Reason for Both Antitrust and Consumer Protection Law' (1998) 10(1) Loyola Consumer Law Review 44

Baldwin C and Woodard C, 'The architecture of platforms: a unified view' in Annabelle Gawer (ed) *Platforms, Markets and Innovation* (Edward Elgar Publishing 2009)

Barnett J, 'The costs of free: commoditization, bundling and concentration' [2018] Journal of Institutional Economics 1097.

Baur Anna-Lena, ‘Analysing the Commission's Guidance on Enforcement Priorities in Applying Article 102 TFEU — An Efficiency Defence for Abusive Behaviour of Dominant Undertakings? ' (2012) 19 (3) Maastricht Journal of European and Comparative Law 1.

Baxter William, ‘Responding to the Reaction: The Draftsman’s View’ (1983) 71 California Law Review 618.

Bergkamp L, ‘The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy’ [2002] CLSR 31

Behrens Peter, ‘The “Consumer Choice” Paradigm in German Ordoliberalism and its Impact upon EU Competition Law’ (2014) Europa-Kolleg Hamburg Discussion Paper No. 1/14

Boerman S, Kruikemeier S, Zuiderveen Borgesius F, 'Online Behavioral Advertising: A Literature Review and Research Agenda' [2017] Journal of Advertising 363.

Botta Marco, 'Sanctioning unfair pricing under Art. 102(a) TFEU: yes, we can!' [2021] European Competition Journal 1

Botta Marco, 'Exploitative abuses: recent trends and comparative perspectives' in Pınar Akman, Or Brook, and Konstantinos Stylianou (eds) *Research Handbook on Abuse of Dominance and Monopolisation* (Elgar 2023)

Botta Marco and Borges Danielle, 'User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with Article 5(2) DMA' Robert Schuman Centre for Advanced Studies Research Paper No. 2023_68

Botta Marco, Svetlicinii Alexandr and Bernatt Maciej, 'The Assessment of the Effect on Trade by the National Competition Authorities of the “New” Member States: Another Legal Partition of the Internal Market?' [2015] Common Mkt L Rev 1247.

Botta Marco and Wiedemann Klaus, ‘EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy Exploring the Terra Incognita’, [2018] Max Planck Institute for Innovation and Competition Research Paper No. 18-08.

Botta Marco and Wiedemann Klaus, ‘The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey’ (2019) 64 Antitrust Bulletin 426

Brennan Timothy, ‘Is complexity in antitrust a virtue? The accuracy-simplicity tradeoff’ (2014) 59 (4) Antitrust Bulletin 827.

Brook O, 'Struggling With Article 101(3) TFEU: Diverging Approaches Of The Commission, Eu Courts, And Five Competition Authorities' (2009) Common Market Law Review 121.

Brook Or and Cseres Katalin J., 'Priority setting in EU and national competition law enforcement' (2021) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3930189> accessed 14 August 2023.

Brook Or and Eben Magali, 'Article 3 of Regulation 1/2003: A Historical and Empirical Account of an Unworkable Compromise' (SSRN, 2022) <https://ssrn.com/abstract=4237413 or http://dx.doi.org/10.2139/ssrn.4237413> accessed 29 October 2023.

Buiten Miriam Caroline, 'Exploitative abuses in digital markets: between competition law and data protection law' [2021] Journal of Antitrust Enforcement 270

Calo R, 'Consumer Subject Review Boards: A Thought Experiment' [2013] Stan L Rev Online 97

Cappai Marco and Colangelo Giuseppe, 'Taming digital gatekeepers: the more regulatory approach to antitrust law' (2021) 41 Computer Law & Security Review 105559.

Carugati Christophe, 'The Antitrust Privacy Dilemma' (2021) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968829> accessed 7 November 2022

Cate Fred H and Mayer-Schönberger Viktor, 'Notice and Consent in a World of Big Data' (2013) 3 International Data Privacy Law 67

Chirita Anca, 'Data-Driven Unfair Competition in Digital Markets' [2023] Boston University Journal of Science & Technology Law 241

Colangelo Giuseppe, 'The Privacy-Antitrust Curse: Insights from GDPR Application in EU Competition Law' (2023) ICLE White Paper 2023-10-12

Colangelo G and Desogus C, 'Antitrust Scrutiny of Excessive Prices in the Pharmaceutical Sector: A Comparative Study of the Italian and UK Experiences' (2018) 41:2 World Competition 225.

Colangelo Giuseppe and Maggiolino Mariateresa, 'Data accumulation and the privacy-antitrust interface: insights from the Facebook case' (2018) 8 (3) International Data Privacy Law 224

Colangelo Giuseppe and Maggiolino Mariateresa, 'Antitrust über alles. Whither competition law after Facebook?' [2019] World Competition Law and Economics Review 1

Condorelli D and Padilla J, 'Harnessing Platform Envelopment in the Digital World' [2020] Journal of Competition Law & Economics 1.

Cooper James C, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity' [2013] Geo Mason L Rev 1129.

Coppi L and Walker M, ‘Substantial Convergence or Parallel Paths? - Similarities and Differences in the Economic Analysis of Horizontal Mergers in the US and EU Competition Law’ (2004) 49(1) Antitrust Bulletin 101.

Costa-Cabral Francisco and Lynskey Orla, ‘Family Ties: The Intersection Between Data Protection and Competition in EU Law’ (2017) 54 Common Market Law 11

Custers Bart, 'Informed Consent in Social Media Use—The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10 SCRIPTED 435

D’Amico Alessia, Meta’s Pay-Or-Okay Model: An Analysis Under Eu Data Protection, Consumer And Competition Law' (2024) Working Paper 1-2024 08-04-2024 < https://www.uu.nl/sites/default/files/rebo-renforce-working-paper-2024-Meta's Pay-or-Okay Model - An Analysis Under EU Data Protection, Consumer, and Competition Law.pdf> accessed 10 April 2024.

Daskalova V, "Consumer Welfare in EU Competition Law: What Is It (Not) About?" (2015) 11(1) The Competition Law Review 133.

Davis Steven J, MacCrisken Jack and Murphy Kevin M, ‘Economic perspectives on software design: PC operating systems and platforms’ in David Evans (ed) *Microsoft, Antitrust and the New Economy: Selected Essays* (Kluwer 2002)

Day Gregory and Stemler Abbey, ‘Infracompetitive Privacy’ (2019) 105 Iowa Law Review 61.

De Gregorio G, 'The rise of digital constitutionalism in the European Union' (2021) 19(1) International Journal of Constitutional Law 41.

Decker Christopher, 'Concepts of the Consumer in Competition, Regulatory, and Consumer Protection Policies’ [2017] J Competition L & Econ 151

Deutscher Elias and Makris Stavros, ‘Exploring the Ordoliberal Paradigm: The Competition-Democracy Nexus’ [2016] Comp LRev 181

Dimakopoulos Philipp, Sudaric Slobodan, ‘Privacy and Platform Competition’ (2017) Rationality & Competition Discussion Paper No 67 <https://rationality-and-competition.de/wp-content/uploads/discussion_paper/67.pdf> accessed 4 April 2020

Drexl Josef, ‘Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy’ in A De Franceschi and R Schulze (eds), *Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice* (Beck 2019)

Dunne Niamh, ‘The Role of Regulation in EU Competition Law Assessment’ (2021) LSE Legal Studies Working Paper No. 09/2021 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871315> accessed 6 November 2022.

Economides N and Lianos I, ‘Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective’ [2021] J Compet Law Econ 765

Efroni Zohar, ‘Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing’ (2019) 3 EDPL 352

Efroni Zohar, ‘Gaps and Opportunities: The Rudimentary Protection for “Data-Paying Consumers” under New EU Consumer Protection Law’ (2020) 57(3) Common Market Law Review 799.

Elherman Claus Dieter, ‘The Contribution of EC Competition Policy to the Single Market’ [1992] Common Market Law Review 257

Esayas S, 'Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism' [2017] Faculty of Law, Stockholm University Research Paper No 43 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075239> accessed 17 November 2022

Ezrachi Ariel, ‘Sponge’ [2016] J Antitrust Enforc 1

Ezrachi Ariel, ‘EU Competition Law Goals and The Digital Economy’ (2018) Oxford Legal Studies Research Paper No 17/2018

Ezrachi A and Robertson V, ‘Competition, Market Power and Third-Party Tracking’ [2018] World Comp: L&C Rev 5

Evans D, 'The Antitrust Economics of Free' (2011) John M. Olin Law & Economics Working Paper, University of Chicago, No. 555 <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article =1483&context=law_and_economics> accessed 30 March 2024.

Filistrucchi Lapo, Geradin Damien, van Damme Eric, Affeldt Pauline, ‘Market Definition in Two-sided Markets: Theory and Practice’ [2014] JCL& E 293

Gal Michal, ‘Monopoly Pricing as an Antitrust Offense in the U.S. and the EC: Two Systems of Belief about Monopoly?’ (2004) 49:1–2 Antitrust Bulletin 343.

Gal M, ‘Abuse of Dominance - Exploitative Abuses’ in I Lianos and D Geradin (eds), *Handbook on European Competition Law* (Edward Elgar 2013)

Gal Michal S., 'The Social Contract at the Basis of Competition Law: Should We Recalibrate Competition Law to Limit Inequality?' in Damien Gerard and Ioannis Lianos (eds), *Competition for the People* (CUP 2019)

Gal MS and Aviv O, ‘The Competitive Effects of the GDPR’ [2020] JCLE 1

Galston William, ‘The Idea of Political Pluralism’ in H Richardson and M Williams (eds), Moral Universalism and Pluralism (New York University Press 2008)

Gawer Annabelle, ‘Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age’ (2021) Innovation, Organization & Management 1.

Gebicka Aleksandra and Heinemann Andreas, ‘Social Media & Competition Law’ [2014] World Competition 149

Geradin Damien and Katsifis Dimitrios, “Trust me, I’m fair”: analysing Google’s latest practices in ad tech from the perspective of EU competition law" [2020] European Competition Journal 11.

Geradin Damien, Katsifis Dimitrios and Karanikioti Theano, 'Google as a *de facto* privacy regulator: analysing the Privacy Sandbox from an antitrust perspective' [2021] European Competition Journal 617.

Geradin Damien and Kuschewsky Monika, 'Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges' (2014) 37 World Competition 69.

Giovannini Vincent, ‘The French Apple competition & privacy case’ (2021) 18 Competition Forum.

Gippini-Fournier Eric, ‘Resale Price Maintenance in the EU: In Statu Quo Ante Bellum?’ in Barry Hawk (ed), *International Antitrust Law and Policy* (Fordham 2009).

Goldfarb Avi and Que Verina F, 'The Economics of Digital Privacy' [2023] Annu Rev Econ 15.

Gorecka A, 'The Other Side of the Coin: Privacy Justifications in Anticompetitive Proceedings under Article 102 TFEU' (2022) 9(2) North East Law Review

Gorecka Arletta, ‘Is "Privacy" a Means to Protect the Competition or Advance Objectives of Innovation and Consumer Welfare?’ in Maria Tzanou (ed.) *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020)

Gotsch Mauro Luis and Schögel Marcus, 'Addressing the privacy paradox on the organizational level: review and future directions' [2023] MRQ 263.

Graef Inge, Clifford Damian, and Valcke Peggy, 'Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law' [2018] International Data Privacy Law 200.

Graef I and Van Berlo S, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility' [2020] European Journal of Risk Regulation 674.

Guinchard Audrey, 'Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law' (2018) 24 European Law Journal 434.

Gunningham Neil and Sinclair Darren, 'Designing Smart Regulation', this article is an abridged version of the concluding Chapter in N Gunningham & P Grabosky *Smart Regulation: Designing Environmental Policy* (OUP 1998)

Gündoğar Meltem, 'EU's Approach To Abuse Of Dominance Concerning Online Platforms: A New Era For Eu Competition Policy?' Europa Kolleg Hamburg Study Paper No.02/2023 < https://europa-kolleg-hamburg.de/wp-content/uploads/2023/01/Study-Paper-Meltem-Guendogar-pdf.pdf> 14 March 2024.

Ham C, 'Exploring how consumers cope with online behavioral advertising' [2017] International Journal of Advertising 632.

Harbour Pamela and Koslov Tara, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' [2010] Antitrust Law Journal 769

Heilberger N, Zuiderveen F, Borgesius, Reyna A, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) CMLRev 1427.

Himeur Y, Saquib Sohail S and Bensaali F, 'Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives' [2022] Computers & Secuty 1

Holles de Peyer Ben, 'EU Merger Control and Big Data' (2017) 13 (4) Journal of Competition Law & Economics 767

Hutchinson Christophe Samuel and Trescakova Diana, 'The challenges of personalized pricing to competition and personal data protection law' [2021] European Competition Journal 105

Ibáñez Colomo Pablo, 'Beyond the 'more economics-based approach': a legal perspective on Article 102 TFEU case law' [2016] CMLR 709.

Ibáñez Colomo Pablo, 'Anticompetitive Effects in EU Competition Law' [2021] Journal of Competition Law & Economics 309.

Ibáñez Colomo Pablo, "The (Second) Modernisation of Article 102 TFEU: Reconciling Effective Enforcement, Legal Certainty and Meaningful Judicial Review" (SSRN, 2023) 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4598161> accessed 22 October 2023.

Jacobides Michael G and Lianos Ioannis, 'Ecosystems and competition law in theory and practice' [2021] Industrial and Corporate Change 1199.

Karova R and Botta M, ‘Sanctioning Excessive Energy Prices as Abuse of Dominance: Are the EU Commission and the National Competition Authorities on the Same Frequency?’ in PL Parcu, G Monti and M Botta (eds), *Abuse of Dominance in EU Competition Law: Emerging Trends* (Edward Elgar 2017)

Kemp Katharine, 'Concealed data practices and competition law: why privacy matters' [2020] European Competition Journal 628

Kedzior Magdalena, ‘GDPR and beyond – a year of changes in data protection landscape of the European Union’ (2019) 19 ERA Forum 505.

Kerber Wolfgang, ‘Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection’ [2016] J of Intellectual Property L & Practice 856

Kerber Wolfgang, 'Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law' [2022] The Antitrust Bulletin 280

Kerber Wolfgang and Specht-Riemenschneider Louisa, 'Synergies Between Data Protection Law and Competition Law' (2020) Bundesverband <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3977039> accessed 1 June 2022.

Kerber Wolfgang and Zolna Karsten, ‘The German Facebook case: the law and economics of the relationship between competition and data protection law’ (2022) European Journal of Law and Economics 217

Kira B, Since V and Srinivasan S, 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' [2021] Industrial and Corporate Change 1337

Kosinski M, Stilwell D and Graepel T, "Private Traits and Attributes are Predictable from Digital Records of Human Behaviour" [2013] Proceedings of the National Academy of Sciences of the United States of America 5802.

Kuenzler Adrian, 'What competition law can do for data privacy (and vice versa)' [2022] Computer Law & Security Review 1.

Kysar Hanson D, 'Taking Behavioralism Seriously: The Problem of Market Manipulation' [1999] NYU L Rev 630.

Lamadrid A, ‘Competition law as Fairness’ [2017] JIPLP 14

Lancieri Filippo and Sakowski Patricia Morita, ‘Competition in Digital Markets: A Review of Expert Reports’ (2021) 26 Stanford J of Law, Bus & Finance 84

Lande Robert, Consumer choice as the goal antitrust (2001) 62 University of Pittsburg Law Review 503

Larsson Stefan, ‘Putting trust into antitrust? Competition policy and data-driven platforms’ (2021) 36 (4) European Journal of Communication 391

Lessig Lawrence, ‘Law of the Horse: What Cyberlaw Might Teach’ (1999) 113 Harvard Law Review 501.

Lianos Ioannis, ‘Categorical Thinking in Competition Law and the ‘Effects-based’ Approach in Article 82 EC’ in Ariel Ezrachi (ed), *Article 82 EC – Reflections on its recent evolution* (Hart 2009)

Lianos Ioannis, ‘Competition law in the European Union after the Treaty of Lisbon’ in Diamond Ashiagbor, Nicola Countouris, Ioannis Lianos (eds), The European Union after the Treaty of Lisbon (CUP 2012)

Lianos I, 'Polycentric Competition Law' [2018] Current Legal Problems 161.

Lianos I, 'Competition Law for the Digital Era: A Complex Systems Perspective' (2019) CLES Research Paper Series 3

Lianos Ioannis and Carballa Smichowski Bruno, 'Economic Power and New Business Models in Competition Law and Economics: Ontology and New Metrics' (2021) Centre for Law, Economics and Society Research Paper Series: 3/2021 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3818943> accessed 12 November 2022.

Lianos Ioannis and Motchenkova Evgenia, ‘Market Dominance and Search Quality in the Search Engine Market’ [2013] JCL&E 419

Luzak J, 'Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online' [2014] Privacy, Journal of Consumer Policy 547.

Luzak J, 'Preserving Consumers’ Choice Online: Competition Law to the Rescue!' [2021] Tijdschrift voor Consumentenrecht en handelspraktijken 1.

Lynskey Orla, ‘Non-price Effects of Mergers’ OECD Competition committee meeting (2018) DAF/COMP/WD(2018)70

Lynskey O, 'Grappling with ‘data power’: Normative nudges from data protection and privacy' (2019) 20(1) Theoretical Inquiries in Law 189.

Majcher Klaudia and Robertson Viktoria HSE, 'Doctrinal Challenges for a Privacy-Friendly and Green EU Competition Law' [2022] SSRN < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778107> accessed 17 May 2023.

Malinauskaite Jurgita, 'Competition Law and Sustainability: EU and National Perspectives' [2022] J Eur Compet 336.

Malgieri G and Custers B, 'Pricing privacy: The Right to Know the Value of Your Personal Data' [2018] CLSR 296

Makris Stavros, 'Applying Normative Theories in EU Competition Law: Exploring Article 102 TFEU' (2014) UCL Journal of Law & Jurisprudence 30

Manne Geoffrey A and Sperry R Ben, "The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework" [2015] CPI Antitrust Chronicle 1

Marsden P and Podszun R, 'Restoring Balance to Digital Competition - Sensible Rulse, Effective Enforcement' (2020) Konrad-Adenauer-Stiftung, Berlin, 40

Martini Mario and Drews Christian, 'Making Choice Meaningful – Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy Law' (SSRN, 2022) <https://ssrn.com/abstract=4257979> accessed 14 April 2024.

Mehrnezhad Maryam, Coopamootoo Kovila, and Toreini Ehsan, 'How Can and Would People Protect from Online Tracking?' (2022) 1 Proceedings on Privacy Enhancing Technologies 105

Milaj Jonida, 'Safeguarding Privacy by Regulating the Processing of Personal Data – An EU Illusion?' [2020] EJLT 1.

Monti G, 'Article 81 EC and Public Policy' (2002) 39 Common Market Law Review 1090

Monti G, 'The Digital Markets Act – Institutional Design and Suggestions for Improvement' (2021) TILEC Discussion Paper DP 2021-004.

Monti Giorgio, 'Balancing in Competition Law" (2022) TILEC Discussion Paper No. DP2022-007.

Monti G and Mulder J, 'Escaping the Clutches of EU Competition Law: Pathways to Assess Private Sustainability Initiatives' (2017) 42 European Law Review 635.

Motta Massimo, 'Self- Preferencing and Foreclosure in Digital Markets: Theories of Harm for Abuse Cases' (2022) BSEWorking Paper 1374 < https://bse.eu/sites/default/files/working_paper_pdfs/1374_0.pdf> accessed 10 May 2023.

Nazzini Renato, 'The Wood Begun to Move: An Essay on Consumer Welfare, Evidence and Burden of Proof in Article 82 cases' (2006) 4 European Law Review 518.

Nazzini R, 'Parallel Proceedings in EU Competition Law: *Ne Bis in Idem* as a Limiting Principle' in Bas van Bockel (ed) *Ne Bis in Idem in EU Law* (CUP 2016).

Nazzini R, 'Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision' (CPI, 2019) <https://www.

competitionpolicyinternational.com/wp-content/uploads/2019/03/EU-News-Column-March-2019-4- Full.pdf> 23 June 2021

Newman J, 'The Myth of Free' [2017] George Washington Law Review 86.

Newman Nathan, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2014) 40 William Mitchell Law Review 849

Nottingham Mark, Playing fair in the Privacy Sandbox: competition, privacy, and interoperability standards' [2021] SSRN < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891335> accessed 17 May 2022.

Ocello Eleonora, Sjödin Cristina, and Subočs Anatoly, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case' (2015) 1 European Commission-Competition Merger Brief 6

Ohlhausen Maureen K and Okuliar Alexander P, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' [2015] Antitrust LJ 121

Pasquale Frank, 'Paradoxes of Digital Antitrust' (2013) Harvard Journal of Law & Technology Occasional Paper Series, July 2013.

Pasquale Frank, 'Privacy, Antitrust, and Power' [2013] Geo Mason L Rev 1009

Petit N, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review' [2021] JECL & Pract 529.

Phelps Joseph, Nowag Glen and Ferrell Elizabeth, 'Privacy Concerns and Consumer Willingness to Provide Personal Information' [2000] J Public Policy Mark 27

Podszun R, 'Digital ecosystems, decision-making, competition and consumers – On the value of autonomy for competition' (2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3420692> accessed 14 August 2023

Podszun Rupprecht, 'The Consumer as a Market Player: Competition Law, Consumer Choice and Data Protection in the German Facebook Decision' (SSRN, 2023) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4400552> accessed 17 October 2023.

Podszun R and Rohner T, 'Making Article 102 TFEU Future-Proof – Learnings from the Past' (2023) <https://ssrn.com/abstract=4428170> accessed 30 August 2023.

Ponsoldt James and David Christopher, ''Comparison between U.S. and E.U. Antitrust Treatment of Tying Claims against Microsoft: When Should the Bundling of Computer Software Be Permitted' (2007) 27 Northwestern Journal of International Law & Business 421.

Posner Eric A, 'The Law, Economics, and Psychology of Manipulation' (2015) Coase-Sandor Inst for Law & Econ Working Paper No 726.

Reyna A, ''The psychology of privacy—what can behavioural economics contribute to competition in digital markets?' [2018] International Data Privacy Law 240.

Robertson V, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2020) 57 (1) Common Market L Rev 161

Rubinstein IS, 'Big Data: The End of Privacy or a New Beginning?' [2013] Int Data Priv 74

Sang Wong Chun and Lam Chan Sze, 'At the Junction of Consumer Protection: Dual Role of Data Protection in EU Law' (2021) 6(2) London School of Economics Law Review 109

Savage S and Waldman D, 'Privacy tradeoffs in smartphone application' [2015] Economic Letters 137.

Schmidt Hedvig, 'Taming the Shrew: There's no need for a new Market Power Definition for the Digital Economy' (2017) Stockholm Faculty of Law Research Paper Series No 1

Schneider G, 'Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's Investigation against Facebook' (2018) 9 JECLAP 213.

Schneider Henrique, 'From Deontology to Pragmatism: Dynamics in the Pursuit of Goals of Competition law' [2017] CORE 245

Schweitzer H, ' The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal' [2021] ZEuP 503.

Schwartz Paul M, 'Global Data Privacy: The EU Way' [2019] NYU L Rev 772.

Sidak J Gregory and Teece David J, 'Dynamic Competition in Antitrust Law' (2009) 5 Journal of Competition Law and Economics 581.

Skoumu G and Leonard L, 'On-line Behavioural Tracking: What may change after the Legal Reform on Personal Data Protection' in S Gutwirth, R Leenes, P de Hert (eds) *Reforming European Data Protection Law* (Springer 2015)

Sokol Daniel and Zhu Feng, 'Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates' (2021) USC Law Legal Studies Paper No. 21-27.

Spulber Daniel F, Antitrust and Innovation Competition [2023] Journal of Antitrust Enforcement 5.

Srinivasan D, 'The Antitrust Case Against Facebook' [2019] Berkeley Business Law Journal 40.

Srinivasan Dina, 'Why Google Dominates Advertising Markets' (2020, SSRN) < https://ssrn.com/abstract=3500919> accessed 27 April 2024.

Stucke Maurice E, 'How Do (and Should) Competition Authorities Treat a Dominant Firm's Deception?' (2010) 63 SMU L. Rev. 1069

Stucke Maurice E, 'Should We Be Concerned About Data-Opolies?' [2018] Geo L Tech Rev 275

Stucke Maurice E and Ezrachi Ariel, 'When Competition Falls to Optimise Quality: A Look at Search Engines' [2016] Yale JL & Tech 70

Stucke Maurice E and Grunes Allen P, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' [2015] Antitrust Source 1

Stylianou K and Iacovides M, "The Goals of EU Competition Law: a Comprehensive Empirical Investigation" (2022) 42 Legal Studies 620

Susser Daniel, Roessler Beate, and Nissenbaum Helen, 'Online Manipulation: Hidden Influences in a Digital World' [2020] Geo L Tech Rev 1.

Šmejkal Václav, 'Abuse of Dominance and the DMA – Differing Objectives or Prevailing Continuity?' [2023] Acta Universitatis Caroliniae – Iuridica 33

Thomson Erin, 'Will the DMA trigger competition in the Digital Advertising Market?' (2022) 34 Competition Forum

Thouvenin Florent, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' [2021] JIPITEC 246.

Trzaskowski Jan, 'Data-driven value extraction and human well-being under EU law' [2022] Electronic Markets 447

Tsai Janice, Egelman Serge, Cranor Laurie and Acquisti Alessandro, 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study' [2011] Information System Research 234.

Vande Walle Simon, 'The European Commission's Approval of Google/ Fitbit – A Case Note and Comment' (2021) Concurrences Competition Law Review Nr. 3-2021

Wasastjerna MC, 'The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface' [2019] European Business Law Review 337.

Weiner Michael, 'Antitrust Is Cool Again' (2018) New York Law Journal

Wiedemann Klaus, 'A matter of choice: the German Federal Supreme Court's interim decision in the abuse-of-dominance proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)' [2020] IIC 1168.

Wiedemann K, 'Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary' [2021] IIC 915.

Wiedemann Klaus, 'Can Data Protection Friendly Conduct Constitute an Abuse of Dominance under Art. 102 TFEU?' (2023) Max Planck Institute for Innovation and Competition Research Paper No. 23-15.

Witt A, 'Data, Privacy and Competition Law' (2021) Graz Law Working Paper No 24-2021 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3989241> accessed 16 April 2023

Wu T, 'The Attention Economy and the Law' [2017] ALJ 771.

Books

Akman Pinar, *The Concept of Abuse in EU Competition law: Law and Economic Approach* (Hart Publishing 2012)

Amato G, *Antitrust and the Bounds of Power: The Dilemma of Liberal Democracy in the History of the Market* (Hart Publishing 1997)

Bilić Paško, Prug Toni and Žitko Mislav, *The Political Economy of Digital Monopolies Contradictions and Alternatives to Data Commodification* (Bristol University Press 2021).

Bishop Simon and Walker David, *The Economics of EC Competition law — Concepts, Application and Measurements* (2nd ed, Sweet & Maxwell 2002)

Bostoen Friso, *Abuse of Platform Power Leveraging Conduct in Digital Markets under EU Competition law and Beyond* (Concurrences 2023)

Cenzig F, *Antitrust Federalism in the EU and the US* (Routledge 2013)

Drexl Josef, Kerber Wolfgang and Podszun Rupprecht, *Competition Policy and the Economic Approach* (Edward Elgar 2012)

Dunne Niamh, *Competition Law and Economic Regulation: Making and Managing Markets* (2015 CUP)

Ezrachi Ariel and Stucke Maurice, *Virtual Competition* (Harvard University Press 2016)

Jones Alison, Sufrin Brenda, and Dunne Niamh, *EU Competition Law: Text, Cases, and Materials* (7th edn, OUP 2019)

Kuner C, Bygrave LA, Docksey C and Drechsler L, *The EU General Data Protection Regulation: A Commentary* (1st edn, OUP 2020)

Nazzini Renato, *The Foundations of European Union Competition Law: the Objectives and Principles of Article 102* (OUP 2009)

Niels Gunnar, Jenkins Helen and Kavanagh James, *Economics for Competition Lawyers* (OUP 2011)

Nowag Julian, *Environmental Integration in Competition and Free-Movement Laws* (Oxford University Press 2016)

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

Odudu O, *The Boundaries of EC Competition Law, the Scope of Article 81 EC* (OUP 2005)

Prosser T, *The Limits of Competition Law* (OUP 2005).

Rawls John, *Political Liberalism* (Columbia University Press 1993)

Rodger Barry and Macculloch Angus, *Competition Law and Policy in the EU and UK* (Routledge 2021)

Schulte Benjamin Krischan, *Staying the Consumption Course: Exploring the Individual Lock-in Process in Service Relationships* (Springe 2015)

Schmidtchen Dieter, Albert Max and Voigt Stefan, *The More Economic Approach to European Competition Law* (Mohr Siebeck 2007)

Schumpeter J, *Capitalism, Socialism, and Democracy* (George Allen & Unwin, 1954)

Stucke M, *Breaking Away How to Regain Control Over Our Data, Privacy, and Autonomy* (OUP 2022) 14

Stucke Maurice E and Grunes Alan P, *Big Data and Competition Policy* (OUP 2016)

Townley Christopher, *Article 81 EC and Public Policy* (Hart Publushing 2009)

Van den Bergh Roger and Camesasca Peter, *European Competition Law and Economics: A Comparative Perspective* (2nd edn, Sweet & Maxwell 2006)

Van Rompuy B, *Economic Efficiency: The Sole Concern of Modern Antitrust Policy* (Kluwer Law International 2012)

Zimmer Daniel, *The Goals of Competition Law* (Edward Elgar 2012)

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

Guidelines and reports

ACM, 'ACM's Analysis of the Sustainability Arrangements Concerning the 'Chicken of Tomorrow'' (26 January 2015) <https://www.acm.nl/en/publications/publication/13761/Industry-wide-arrangements-for-the-so-called-Chicken-of-Tomorrow-restrict-competition.> accessed 20 July 2023.

Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (17/EN, WP260 rev.01, as last revised and adopted on 11 April 2018)

Australian Competition and Consumer Commission, 'Digital Platforms Inquiry: Final Report' (2019) <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20%20final%20report.pdf> accessed 14 May 2020.

Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' (2016) <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=7EE1625AF7E8DDAF12967AE0549C9C23.2_cid381?__blob=publicationFile&v=2> accessed 10 February 2020

BKartA, 'Wettbewerbskommission 4.0' (2019) 43 <https://www.bmwk.de/Redaktion/DE/Artikel/Wirtschaft/kommission-wettbewerbsrecht-4-0.html> accessed 17 May 2023

Bundeskartellamt, '2013/2014 Activity Report, German Bundestag – 18th legislative period, printed paper 18/5210, 53-54, <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Taetigkeitsberichte/Bundeskartellamt%20-%20T%C3%A4tigkeitsbericht%202014.pdf?__blob=publicationFile&v=2> accessed 4 August 2023.

Bundeskartellamt, 'Amendment of the German Act against Restraints of Competition' (2021) < https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB Novelle.html?nn=3591568> 14 August 2023.

CMA, 'Guidelines for market investigations: Their role, procedures, assessment and remedies' (2013) <https://assets.publishing.service.gov.uk/media/5a7c1b7340f0b645ba3c6bcc/cc3_revised.pdf> accessed 24 November 2023

CMA, 'Market Studies and Market Investigations: Supplemental guidance on the CMA's approach' (2017) <ttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624706/ cma3-markets-supplemental-guidance-updated-june-2017.pdf.> accessed 24 November 2023.

CMA, 'Online Platforms and Digital Advertising Market Study' (July 2020) < https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> accessed 15 November 2022 (hereinafter: 'Online Platforms and Digital Advertising Study')

CMA, 'Anticipated acquisition by Facebook, Inc. of Kustomer, Inc. Decision on relevant merger situation and substantial lessening of competition' (2021) ME/6920/20 < https://assets.publishing.service.gov.uk/media/618a6328d3bf7f56059042d5/Facebook.Kustomer_-_Phase_1_Decision_.pdf> accessed 10 November 2023

CMA, 'Completed acquisition by Facebook, Inc (now Meta Platforms, Inc) of Giphy, Inc.Summary of Remittal Final Report' (2021) < https://assets.publishing.service.gov.uk/media/634e6ce58fa8f53465d13a35/Facebook_GIPHY_-_Remittal_Summary_.pdf> accessed 1 July 2023.

CMA, Case 50972 - Privacy Sandbox Google Commitments Offer (2022) < https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf> accessed 1 August 2023.

CMA, 'Completed acquisition by Facebook, Inc (now Meta Platforms, Inc) of Giphy, Inc. Final report on the case remitted to the CMA by the Competition Appeal Tribunal' (2022) < https://assets.publishing.service.gov.uk/media/635017428fa8f53463dcb9f2/Final_Report_Meta.GIPHY.pdf> accessed 1 July 2023.

CMA, 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (CMA, 2022) < https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf> accessed 2 August 2023

CMA, 'Mobile ecosystems' (2022) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL__.pdf> accessed 2 September 2022.

CMA, 'CMA update report on implementation of the Privacy Sandbox commitments' (CMA, 2023) < https://assets.publishing.service.gov.uk/media/644a82cd2f62220013a6a19b/CMA_s_Q1_2023_update_report.pdf> accessed 17 August 2023

CMA, 'CMA Q3 2023 update report on implementation of the Privacy Sandbox commitments' (2023) < https://assets.publishing.service.gov.uk/media/653a58e2e6c968000daa9b94/__Q3_2023_update_report____.pdf> accessed 24 November 2023.

CNMC, 'E/CNMC/002/2019 Study on the competition conditions in the online advertising sector in Spain' (2021) <https://www.cnmc.es/sites/default/files/3696007_0.pdf> accessed 10 March 2024.

Cremer J, de Montjoye Y and Schweitzer H, 'Competition policy for the digital era' (European Commission 2019) 30 <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 10 December 2019

Douglas EM, 'Digital Crossroads: The Intersection of Competition law and Data Privacy' (2021) Temple University Legal Studies Research Paper No. 2021-40 <https://iapp.org/media/pdf/resource_center/Digital_Crossroads_The_Intersection_Competition_Law_Data_Privacy.pdf> accessed 4 August 2021

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

EDPS, 'Opinion 8/2016: The Coherent Enforcement of Fundamental Rights in the Age of Big Data' (2016) 9 < https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf > accessed 14 August 2022

EDPS, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy' (2017) < https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 20 April 2020

EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2019) paras 62-64 < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 23 November 2023.

European Commission, 'Commission Notice on cooperation within the Network of Competition Authorities' (2004/C 101/03)

European Commission, 'Guidelines on the application of Article 81(3) of the Treaty' (2004/C 101/08) para 5: "Goals pursued by other Treaty provisions can be taken into account to the extent that they can be subsumed under the four conditions of Article [101(3)]

European 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

European Commission, 'Notice on the definition of relevant market for the purposes of Community competition law' 97/C 372/03 [1997] OJ C372/5.

European Commission, 'Communication from the Commission to the European Parliament and the Council: 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' (2020) 3 <https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN> accessed 17 October 2021.

European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> 14-15 accessed 4 April 2023

FTC, 'Statement of FTC Concerning Google/DoubleClick' FTC File No. 071-0170, 2–3 (Dec. 20, 2007) <https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf> accessed 20 October 2021

Fourberg Niklas, Taş Serpil, Wiewiorra Lukas, 'Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice' (EU Parliament, 2021) 31 < https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf> accessed 12 April 2024.

Google, 'Privacy Sandbox Progress Report Q3 Reporting Period - July to September 2023 Prepared for the CMA, 24 October 2023' (2023) < https://assets.publishing.service.gov.uk/media/653a491d80884d000df71b70/Google_s_Q3_2023_report_.pdf> accessed 24 November 2023

ICO, 'Investigation into Data Protection Compliance in the Direct Marketing Data Broking Sector' (2020) <https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data- protection-compliance-in-the-direct-marketing-data-broking-sector.pdf> accessed 10 December 2020

ICO and CMA, 'Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO' (2021) 19 <https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf> accessed 17 June 2021

Italianer Alexander, 'Innovation and Competition' (2015) International Antitrust Law & Policy, Competition Law Institute < https://www.fordham.edu/download/downloads/id/11451/FCLI2018_Conference_Day1_CLEMaterials_asof6September2018_v_1.pdf> accessed 17 May 2022.

Krämer Jan, Schnurr Daniel and Broughton Micova Sally, 'The Role of Data for Digital Markets Contestability' (CERRE Report, 2020) < https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/> accessed 12 April 2024.

Monopolkommission, 'Competition policy: The challenge of digital markets' (2015) Special report No. 68 <https://www.monopolkommission.de/index.php/en/press-releases/52-competition-policy-the-challenge-of-digital-markets> accessed 20 November 2022

Monopolkommission, 'Recommendations for an effective and efficient Digital Markets Act' (2021) 9 <https://www.monopolkommission.de/en/reports/special-reports/special-reports-on-own-initiative/372-sr- 82-dma.html> accessed 9 April 2023.

Motta M and Peitz M, 'Intervention trigger and underlying theories of harm - Expert advice for the Impact Assessment of a New Competition Tool' (EU Commission, 2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/kd0420575enn.pdf> accessed 12 November 2022.

Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice) (OJ C 291, 30.8.2014, p. 1–4).

Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Additional Procedural Rules Relating To The Enforcement Of Regulation (Eu) 2016/679.

Reyna Agustin, 'Interdisciplinary Enforcement in Competition and Data Protection Law' (BEUC 2023) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4349827> accessed 16 April 2023.

UK Government, 'Report of the Digital Competition Expert Panel, Unlocking Digital Competition' (March 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 10 December 2019

Whish R, 'The New Competition Tool: Legal comparative study of existing competition tools aimed at addressing structural competition problems, with a particular focus on the UK's market' (European Commission, 2020) <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/kd0420573enn.pdf> accessed 14 September 2021

Van Alsenoy Brendan and Verdoodt Valerie, 'From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms' (2015) Belgian Data Protection Authority <https://kuleuven.limo.libis.be/discovery/search?query=any,contains,lirias1662185&tab=LIRIAS&search_scope=lirias_profile&vid=32KUL_KUL:Lirias&foolmefull=1&&lang=en> accessed 17 July 2020

Websites and other sources

Abbott Alden, 'Broad-Based FTC Data-Privacy and Security Rulemaking Would Flunk a Cost-Benefit Test' (*Truth on the Market Blog*, 13 October 2021) <https://truthonthemarket.com/2021/10/13/broad-based-ftc-data-privacy-and- security-rulemaking-would-flunk-a-cost-benefit-test/> accessed 24 November 2023.

Autorité de la Concurrence, 'Press release, 9 September 2014: Gas Market' (2014) <https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9-september-2014-gas-market> accessed 2 August 2023.

Autorité de la Concurrence, 'Sector-specific investigation into online advertising' (Press release, 2018) <https://www.autoritedelaconcurrence.fr/en/press-release/6-march-2018-sector-specific-investigation-online-advertising> accessed 30 April 2024.

Autorité de la Concurrence, 'The Autorité de la Concurrence Hands Down a €150M Fine for Abuse of a Dominant Position' (Press release, 2019) <https://www.autoritedelaconcurrence.fr/en/press -release/autorite-de-la-/concurrence-hands-down-eu150m-fine-abuse-dominant-position> accessed 17 April 2024

Autorité de la Concurrence, 'Droits Voisins: L'Autorité Fait Droit aux Demandes de Mesures Conservatoires Présentées par les Éditeurs de Presse et l'AFP' (Press Release, 2020) <https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/droits-voisins-lautorite-fait-droit-aux-demandes-de-mesures-conservatoires> accessed 17 April 2024.

Autorité de la Concurrence, 'Related rights: The Autorité accepts Google's commitments' (Press release, 2022) <https://www.autoritedelaconcurrence.fr/en/press-release/related-rights-autorite-accepts-googles-commitments> accessed 20 April 2024.

Autorite de Protection des Données, 'L'APD publie une checklist pour une utilisation correcte des cookies' (Press Release, 2023) <https://www.autoriteprotectiondonnees.be/citoyen/actualites/2023/10/20/lapd-publie-une-checklist-pour-une-utilisation-correcte-des-cookies. + Bruegel> accessed 24 November 2023.

Autorità Garante della Concorrenza e del Mercato, 'Sanzione Da 3 Milioni Di Euro per WhatsApp, Ha Indotto Gli Utenti a Condividere I Loro Dati Con Facebook' (2017) <http://www.agcm.it/stampa/comunicati/8754-ps10601-cv154-sanzione-da-3milioni-di-euro-per-whatsapp,-ha-indotto-gli-utenti-a-condividere-i-loro-dati-con-facebook.html> accessed 1 May 2022.

Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni and il Garante per la protezione dei dati personali, 'Big Data, Indagine Conoscitiva Congiunta, Linee Guida e Raccomandazioni di Policy' (2019) <https://www.garanteprivacy.it/documents/10160/0/Big+Data.+Linee+guida+e+raccomandazioni+di+policy.+Indagine+conoscitiva+congiunta+di+Agcom%2C+Agcm+e+Garante+privacy.pdf/563c7b0e-adb2-c26c-72ee- fe4f88adbe92?version=1.1> accessed 24 November 2023.

Barker Alex, 'Apple hit with antitrust complaint in France over privacy controls' (Financial Times, 28 October 2020).

Bauer Alex, 'ATT opt-in rates: the picture so far and the ugly truth behind why the numbers vary so widely' (AdExchanger, 10 May 2021) <https://www.adexchanger.com/data-driven-thinking/att-opt-in- rates-the-picture-so-far-and-the-ugly-truth-behind-why-the-numbers-vary-so-widely/> accessed 15 April 2024.

BEUC, 'Choose to lose with Meta - an assessment of Meta's new paid- subscription model from a consumer law perspective' (2023) <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-

156_Annex_Legal%20assessment_Choose_to_lose_with_Meta_Legal_analysis.pdf> accessed 19 April 2024.

Breton T, 'DSA/DMA Myths – Will the EU regulation create legal uncertainty?' (Blogpost, Linkedin, 2021) < https://www.linkedin.com/pulse/dsadma-myths-eu-regulation-create-legal-uncertainty-thierry-breton/?published=t> accessed 20 March 2024.

Bundeskartellamt, 'Proceeding against Google based on new rules for large digital players (Section 19a GWB)' (Press release, 2021) < https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/25_05_2021_Google_19a.html.> accessed 31 July 2023.

Bundeskartellamt, 'Bundeskartellamt reviews Apple's tracking rules for third-party apps' (14 June 2022) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html?nn=3591568> accessed 15 April 2024

Bundeskartellamt, 'Statement of Objections Issued Against Google's Data Processing Terms' (Press Release, 2023) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html> accessed 23 November 2023.

Cabral Luís, Haucap Justus, Parker Geoffrey, Petropoulos Georgios, Valletti Tommaso and Van Alstyne Marshall, 'The EU Digital Markets Act A Report from a Panel of Economic Experts' (European Commission 2020) < https://ide.mit.edu/wp-content/uploads/2021/02/jrc122910_external_study_report_-_the_eu_digital_markets_act.pdf> accessed 6 May 2023

Carugati Christophe, 'The 'pay-or-consent' challenge for platform regulators' (Bruegel, 2023) < https://www.bruegel.org/analysis/pay-or-consent-challenge-platform-regulators#footnote2_ricgd6g> accessed 24 November 2023.

Chisholm Alex, 'Alex Chisholm Speaks about Online Platform Regulation.' (2015) *CMA* <https://www.gov.uk/government/speeches/alex-chisholm-speaks-about-online-platform-regulation> accessed 14 March 2020

CMA, 'Algorithms: How they can Reduce Competition and Harm Consumers' (CMA, 2021) < https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers> accessed 9 May 2023

CMA, 'CMA to investigate Google's Privacy Sandbox browser changes' (Competition and Markets Authority Press Release, 8 January 2021) <https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes> accessed 15 April 2023.

CMA, 'Investigation into Google's 'Privacy Sandbox' browser changes' (*Press release*, 8 January 2021) < https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes> 28 February 2022

Commission Nationale de l'Informatique et des Libertés, 'La CNIL Publie des Premiers Critères d'évaluation' (Press Release, 2022) <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation> accessed 24 November 2023.

Commission Nationale de l'Informatique et des Libertés, 'Cookie walls : la CNIL publie des premiers critères d'évaluation', 16 May 2022, <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation> accessed 19 April 2024.

Condorelli Daniele and Padilla Jorge, 'Data-Driven Envelopment with Privacy-Policy Tying' (2021) <https://www.condorelli.science/PEPPT.pdf> accessed 6 November 2022

Costa Dan, 'Facebook: Privacy Enemy Number One?' (2010) *PCMAG* <http://www.pcmag.com/article2/0,2817,2362967,00.asp> accessed 17 October 2021.

Coyle Diane and Manley Annabel, 'What is the Value of Data? A review of empirical methods' (2022) Bennett Institute for Public Policy <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/07/policy-brief_what-is-the-value-of-data.pdf> accessed 17 May 2023

Data Protection Commission, 'Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland' (Press Release 2023) <https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.> accessed 20 November 2023.

Dutton Sam, 'Digging into the Privacy Sandbox' web.dev (8 April 2020) <https://web.dev/digging-into- the-privacy-sandbox/>. Accessed 17 October 2022

EDPB, 'EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices –DRAFT PRINCIPLES (Ref. Ares(2023)6863760)', (2023) <https://www.edpb.europa.eu/system/files/2023- 12/edpb_letter_out20230098_feedback_on_cookie_pledge_draft_principles_en.pdf> accessed 19 April 2024.

EU Commission, 'A European Green Deal' < https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en> accessed 17 May 2023

EU Commission, 'Review of the Commission Notice on the definition of relevant market for the purposes of Community competition law' (2022) < https://competition-policy.ec.europa.eu/public-consultations/2022-market-definition-notice_en> accessed 15 August 2023

European Commission, 'Application of Article 102 TFEU' < https://competition-policy.ec.europa.eu/antitrust/legislation/application-article-102-tfeu_en> accessed 31 August 2023.

European Commission, 'Press release, Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (2016) < https://www.europeansources.info/record/mergers-commission-approves-acquisition-of-linkedin-by-microsoft-subject-to-conditions/> accessed 10 September 2021

European Commission, 'Speech of Competition Commissioner Vestager, 'Competition in a big data world' (2016) *DLD 16 Munich*, 17 January 2016, <https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big- data-world_en.> accessed 10 October 2019.

European Commission, 'Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector' (Press release, 22 June 2021) < https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143> accessed 14 January 2022

European Commission, 'Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector' (Press release, 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143> accessed 24 November 2023.

European Commission, 'Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases' (2023) < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609> accessed 23 November 2023.

European Commission, 'Antitrust: Commission announces Guidelines on exclusionary abuses and amends Guidance on enforcement priorities' IP/23/1911 (Brussels, 27 March 2023).

Facebook, 'Terms of Service' <https://www.facebook.com/terms.php> accessed 1 November 2022.

Fleishman Glenn, 'How the tragic death of Do Not Track ruined the web for everyone', FastCompany (17 March 2019) < https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the- web-for-everyone> accessed 17 May 2022.

Google, 'Proposed Adoption By The European Commission Of Article 102 TFEU Guidelines On Exclusionary Abuses: Google Response To The European Commission's Call For Evidence' (EU Commission, 2023) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-Prawo-konkurencji-UE-wytyczne-dotyczace-naduzyc-wykluczajacych-popełnianych-przez-przedsiebiorstwa-dominujace/F3407381_pl> accessed 28 July 2023

Ha Antony, 'Apple defends new ad-tracking prevention measures in Safari' (*TechCrunch*, 16 September 2017) <https://techcrunch.com/2017/09/15/apple-defends-new-ad-tracking-prevention-measures-in-safari/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACJHE OUzBdbgOV96MDbycf1YZwUlAxpibSRBek4odBvKQh-LxcYDj77NF3LpeHFch9JvM-

cJbagU6HEDj9FwVzQazq8ZWvOu0EnlkKRfzUQeL9F5vXBEYoGbdIgrbWrCISsNMD67PX9PJAKtp9zkfqVAMGR kbcphVvYi8SO3V9OY> accessed 6 November 2022.

Harta Lukas, 'Abuse of Dominance and the Digital Markets Act Big Tech companies at risk of double jeopardy' (CepInput, 2021) <https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepInput_Marktmissbrauch_und_DMA/cepInput_Abuse_of_Dominance_and_DMA.pdf> accessed 13 February 2023.

Hewitt Pate R, 'Competition and Politics' [6 June 2005] <http://www.justice. gov/atr/public/speeches/210522.htm> accessed 15 October 2022

Ibanez-Colomo Pablo, 'GC Judgment in Case T-814/17, Lithuanian Railways – Part I: object and indispensability' (*Chillin'Competition Blog*, 1 December 2020) <https://chillingcompetition.com/2020/12/01/gc-judgment-in-case- t%E2%80%91814-17-lithuanian-railways-part-i-object-and-indispensability/> accessed 26 March 2022

Ibanez-Colomo Pablo, 'The (growing) role of the Guidance Paper on exclusionary abuses in the case law: the legal and the non- legal' (*Chillin'Competition Blog*, 9 February 2022) <https://chillingcompetition.com/2022/02/09/the-growing-role-of- the-guidance-paper-on-exclusionary-abuses-in-the-case-law-the-legal-and-the-non-legal/> accessed 17 August 2022.

Irish Legal News, 'Ireland remains 'enforcement bottleneck' for GDPR' (2023) <https://www.irishlegal.com/articles/ireland-remains-enforcement-bottleneck-for-gdpr> accessed 23 November 2023

Isaac Mike, 'Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger' *(The New York Times,* 25 January 2019) < https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html> accessed 23 October 2022.

Janik Maciej and Sznajder Marta, 'Main Developments in Competition Law and Policy 2022 – Poland' (Kluwer Competition Law, 2023) < https://competitionlawblog.kluwercompetitionlaw.com/2023/05/23/main-developments-in-competition-law-and-policy-2022-poland/> accessed 24 November 2023

Johnson Garret, "Economics of Digital Ad Identity" (2020) (paper presented at W3C Workshop on Web and Machine Learning) <https://docs.google.com/presentation/d/1PKHVtO6hgwBJS1vafLyvG_lwupL hfCSelzczvltxjqc/edit#slide=id.p1> accessed 14 April 2023.

Katsifis Dimitrios, 'How tech platforms act as private regulators of privacy' (The Platform Law Blog, 26 October 2020) <https://theplatformlaw.blog/2020/10/26/how-tech-platforms-act-as-pri-vate-regulators-of-privacy/> accessed 10 March 2024.

Katsifis Dimitrios, 'CMA opens investigation into Google's Privacy Sandbox browser changes' (The Platform Law Blog, 8 January 2021) <https://theplatformlaw.blog/

2021/01/08/cma-opens-investigation-into- googles-privacy-sandbox-browser-changes/> accessed 15 April 2024

Lamadrid A, 'On Privacy, Big Data and Competition Law (2/2) On the nature, goals, means and limitations of competition law' (Chillin'Competition, 2014) < https://chillingcompetition.com/2014/06/06/on-privacy-big-data-and-competition-law-22-on-the-nature-goals-means-and-limitations-of-competition-law/> accessed 6 July 2020

Lambrecht A and Tucker CE, 'Can Big Data Protect a Firm from Competition?' (*CPI,* 2017) <https://www.competitionpolicyinternational.com/can-big-data-protect-a-firm-from-competition/> 3, accessed 3 April 2020

Liboreiro J, 'Brussels pitches GDPR reform but without opening 'Pandora's box' (euronews.com 2023) <https://www.euronews.com/my-europe/2023/07/04/brussels-pitches-gdpr-reform-but-without-opening-pandoras-box> accessed 15 October 2023

Lomas Natasha, 'Poland latest to probe Apple's app tracking transparency shift — over self-preferencing concerns' (TechCrunch, 2021) <https://techcrunch.com/2021/12/13/poland-apple-att-antitrust-probe/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJ09573B8vwb9twnmtMW09yenxqHPZzv1e8gUlfM1eU3955osVuhlg_RILhrFz5A1Qp-1Xq1nVvaR0DdxAEqLg9zN_9m1Spes9o1cWVSeRZepl9BY9hebZb9kfKZF9gfhpoLA7Dh_dU3dG0-Yl9YrVoUUfd8maxZczFNbqzwfc6S> accessed 2 May 2024.

Manne Geoffrey and Auer Dirk, 'Antitrust Dystopia and Antitrust Nostalgia' (2021) Truth on the Market <https://truthonthemarket.com/author/manneauer/> accessed 7 November 2022.

Martens B, 'An Economic Policy Perspective on Online Platforms' (2016) Institute for Prospective Technological Studies Digital Economy Working Paper < https://joint-research-centre.ec.europa.eu/system/files/2016-05/JRC101501.pdf> accessed 12 June 2022

Meta, 'Facebook and Instagram to Offer Subscription for No Ads in Europe' (30 October 2023) <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/> accessed 19 March 2024.

Murgia Madhumita and Espinoza Javier, 'Ireland is 'worst bottleneck' for enforcing EU data privacy law – ICCL' (*The Irish Times,* 2023) < https://www.irishtimes.com/business/technology/ireland-is-worst-bottleneck-for-enforcing-eu-data-privacy-law-iccl-1.4672480> accessed 23 November 2023.

Nguyen David and Paczos Marta, 'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective' (2020) OECD < https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf> accessed 17 May 2023.

Noyb, '28 NGOs urge EU DPAs to reject “Pay or Okay” on Meta' (2024) < https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta> accused 20 April 2024.

Noyb, ‘Complaint to the Austrian DPA against Meta’ (2024) <https://noyb.eu/sites/default/files/2024-01/Meta_Withdrawal_Complaint_REDACTED_EN.pdf> accessed 19 April 2024.

Petit N, 'Towards Guidelines On Article 102 Tfeu How Much Leeway Within The Case-Law?' (EU Commission, 2023) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-Prawo-konkurencji-UE-wytyczne-dotyczace-naduzyc-wykluczajacych-popełnianych-przez-przedsiebiorstwa-dominujace/F3407407_pl> accessed 28 July 2023

Reyna A, 'Why The DMA Is Much More Than Competition Law (And Should Be Treated As Such)' (Chilling Competition, 2021) <https://chillingcompetition.com/2021/06/16/why-the-dma-is-much-more-than-competition-law-and-should-not-be-treated-as-such-by-agustin-reyna/> accessed 6 April 2024.

Rohner T, 'Ideas for Sustainable Control of Abusive Practices' (D’Kart, 11.8.2022), <https://www.d- kart.de/en/blog/2022/08/11/agenda-2025-ideen-fur-eine-nachhaltige-missbrauchsaufsicht/> accessed 15 August 2023

Schrepel Thibault, 'Re: Call for evidence regarding the guidelines on exclusionary abuses by dominant undertakings' (EU Commission, 2023) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13796-Prawo-konkurencji-UE-wytyczne-dotyczace-naduzyc-wykluczajacych-popełnianych-przez-przedsiebiorstwa-dominujace/F3405651_pl> accessed 28 July 2023.

Seufert Benjamin, ‘ATT advantages Apple’s ad network. Here’s how to fix that.’ (MobileDevMemo, 1 November 2021) <https://mobiledevmemo.com/att-advantages-apples-ad-network-heres-how-to-fix- that/> accessed 15 April 2024

Seufert Eric Benjamin, ‘The profound, unintended consequence of ATT: content fortresses’ (Mo- bileDevMemo, 15 February 2021) <https://mobiledevmemo.com/the-profound-unintended-conse- quence-of-att-content-fortresses/> accessed 26 July 2022.

Siragusa Mario, 'Excessive Prices in Energy Markets: Some Unorthodox Thoughts' (2007) < https://www.eui.eu/Documents/RSCAS/Research/Competition/2007ws/200709-COMPed-Siragusa.pdf> accessed 30 July 2023.

Shipman Wentworth Sally, 'Pervasive Internet Surveillance – Policy ripples' (*Improving Technical Security,* 26 June 2014) < https://www.internetsociety.org/blog/2014/06/pervasive-internet-surveillance-policy-ripples/> accessed 6 November 2022

Sullivan Danny, ‘Duck Duck Go’s Post-PRISM Growth Actually Proves No One Cares About “Private” Search’ (2013) *Search Engine Land* <http://searchengineland.com/duck-duck-go-prism-private-search-164333> accessed 1 March 2022.

Swire Peter, 'Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall' (18 Oct 2007) <www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony _peterswire_en.pdf> accessed 12 June 2020.

Thibodeau P, 'The Internet of Things Could Encroach on Personal Privacy' (2014) < https://www.computerworld.com/article/2488949/emerging-technology/the-internet-of-things-could-encroach-on-personal-privacy.htm> accessed 2 October 2019

Thompson Ben, 'Digital Advertising in 2022' (*Stratechery*, 8 February 2022) <https://stratechery.com/2022/digital- advertising-in-2022/> accessed 6 November 2022

US Dep't of Justice, 'Justice Department Sues Monopolist Google for Violating Antitrust Laws' (2020), <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws> accessed 2 January 2021.

Valletti T , 'Doubt Is Their Product": The Difference between Research and Academic Lobbying' (*ProMarket,* 28 September 2020) <https://promarket.org/2020/09/28/difference-between-research-academic-lobbying-hidden-funding/> accessed 17 January 2023.

Valletti Tommaso and Caffarra Cristina, 'Google/Fitbit review: Privacy IS a competition issue' (Cepr 2020) < https://cepr.org/voxeu/blogs-and-reviews/googlefitbit-review-privacy-competition-issue> accessed 1 August 2023.

Vestager M, 'A Principles Based approach to Competition Policy' (Keynote at the Competition Law Tuesdays, 22 October 2022)

Vinocur Nicholas, 'Millions of Americans rely on Europe's tough new privacy rules to safeguard their data, but the law's chief enforcer – Ireland – is in bed with the companies it regulates' (*Politico*, 24 April 2019) <https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/> 23 November 2023.

WhatsApp, 'WhatsApp Blog' (2014) <https://blog.whatsapp.com/499/Facebook?> accessed 14 June 2020

'What Is App Tracking Transparency (ATT) and How Does It Affect Mobile Marketing?' (Vungle Blog, 26 May 2021) <https://vungle.com/blog/app-tracking-transparency-att/> accessed 15 April 2023.

Wilson Christine, 'Breaking the Vicious Cycle: Establishing a Gold Standard for Efficiencies' (*Bates White Antitrust Webinar,* 24 June 2020) <https://www.ftc.gov/system/files/documents/public_statements/1577315/wilson_-_bates_white_presentation_06-24-20-_final.pdf> accessed 7 November 2022.

Witt Anne, 'Feedback On The Proposed Guidelines On Exclusionary Abuses By Dominant Undertakings' (EU Commission, 2023) 5 < https://ec.europa.eu/info/law/better-regulation/

have-your-say/initiatives/13796-EU-competition-law-guidelines-on-exclusionary-abuses-by-dominant-undertakings/F3406999_en> accessed 13 August 2023.