THE INTERPLAY BETWEEN

DATA PROTECTION LAW and COMPETITION LAW

in the EUROPEAN UNION:

A SUGGESTION FOR DATA-RELATED CASES

Supervisor: Prof. Eyad Maher Dabbah

Student: 180687769

Word count: 14924

TABLE of CONTENTS

IS THERE AN INTERSECTION BETWEEN DATA PROTECTION LAW and COMPETITION LAW?....4

1.1. Data Protection and Privacy Laws 4

1.2. Competition Law....11

1.3. A Comparison between Data Protection Law and Competition Law 14

1.4. Conclusion 16

WHAT IS THE INTERPLAY BETWEEN DATA PROTECTION LAW and COMPETITION LAW?....18

2.1. Competition Law Approaches Towards Non-Intervention in Data-Related Issues....19

2.2. Competition Law Approaches Towards Intervention in Data-Related Issues....28

2.3. Conclusion 34

HOW SHOULD BE THE INTERPLAY BETWEEN DATA PROTECTION LAW and COMPETITION LAW?....37

3.1. Limitations of Competition Law Towards Data-Related Exploitative Practices 37

3.2. Limitations of Privacy Considerations Towards Data-Related Exploitative Practices..42

3.3. Conclusion 46

OVERALL CONCLUSION and A SUGGESTION FOR DATA-RELATED CASES ...48

BIBLIOGRAPHY....52

TABLE of CASES 57

The significance of personal data processing has been increased exponentially in parallel with the big data technologies. Businesses can offer a range of innovative and customised services as a result of the real time data collection in enormous scales, powerful processors and data algorithms.[1] Most data-driven businesses, search engines or social networking platforms in particular, provide zero-price services in exchange of their personal data, which is then commercialised to target advertisers. Indeed, as Bygrave highlights, "…*these companies know more about us than our partners and closest friends."*[2]

However, these developments have raised significant concerns on both data protection and competition. On the one hand, the collection of data without consent or even without knowledge of the users and misuse of data by third parties, have arisen significant awareness towards data protection.[3] On the other hand, the number of concentrations between big data processors has been increased and the asymmetric power between undertakings and individuals created a take-it-or-leave-it situation over users.

Consequently, fierce debates have started among regulators, legislators and practitioners. Several legislative actions have been taken regarding data protection or privacy[4]. With respect

[1] 'Big Data: Bringing Competition Policy to the Digital Era-OECD' <http://www.oecd.org/daf/competition/big-data-bringing-competition-policy-to-the-digital-era.htm> accessed 12 March 2019.
[2] See the well-known *Target* case, where the father of a teenager in the US, learned that his girl is pregnant, after the data analytics system of a supermarket identified a teenager as pregnant, and sent her advertising coupons on baby clothes and cribs accordingly. Charles Duhigg, 'How Companies Learn Your Secrets' *The New York Times* (16 February 2012) <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> accessed 15 August 2019, Alberto Alemanno, 'Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many' (2018) 9 European Journal of Risk Regulation 183.
[3] Lee A Bygrave, *Data Privacy Law* (1st edn, OUP 2014) 4.
[4] While the term 'privacy' is more akin to American approach, the Europeans prefer data protection. Jeroen Van Den Hoven and others, 'Privacy and Information Technology' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Summer 2018, Metaphysics Research Lab, Stanford University 2018) <https://plato.stanford.edu/archives/sum2018/entries/it-privacy/> accessed 16 August 2019. Similarly, although 'right to data protection' and 'right to privacy' overlap, they do not exactly encounter the same meanings. See Inge Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Berlin Heidelberg 2018) 284

to competition, adoption of new rules has been proposed to be able to adequately evaluate markets and potential infringements. For instance, to capture mergers with a low turnover but a high corporate value like in acquisitions of digital start-ups, merger thresholds are argued to be revised.[5] Even several hypothetical theories of harm have been established basing on collusions between machines which use artificial intelligence tools without human intervention for anticompetitive agreements.[6]

Furthermore, especially with the renowned merger cases such as *Google/DoubleClick*[7] and *Facebook/WhatsApp*[8], the intersection between competition law and data protection law has become a prominent subject. Several claims were put forward ranging from considering data protection issues under competition law assessments to revising competition law regimes to be able to catch digital era's competition and/or data protection problems.[9] Overall, data protection advocates purported larger considerations in competition cases, some of which are meant to break down the existing standards.[10]

In that respect, the majority of studies about the incorporation of data protection concerns in competition law are focused on limited aspects of either data protection law or competition law enforcement. It would be insufficient and misleading to discuss when to intervene in the context of competition law without addressing the substantive standards of both legal regimes.[11]

<http://link.springer.com/10.1007/978-3-662-57646-5_6> accessed 19 June 2019. However, in the context of this study, no distinction is made between the two.

[5] Victoria Moorcroft and Ariane Le Strat, 'The Rise of Big Data: The Intersection between Competition Law and Customer Data' [2018] The Licensing Journal 8.

[6] Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (1st edn, Harvard University Press 2016).

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

[8] *Facebook/WhatsApp* (Case COMP/M.7217) [2014] OJ C297/13.

[9] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties:The Intersection Between Data Protection and Competition in EU Law' [2017] Common Market Law Review 11, 13.

[10] Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer Law International 2016) 283.

[11] Costa-Cabral and Lynskey (n 9) 14.

Therefore this study targets providing a detailed look over the issue of interplay without losing the broader perspective at the same time.

Given above point of views, at an era of information technologies, the interplay between data protection law and competition law have become a major point of focus. Leaving aside merger thresholds or collusions by artificial intelligences, as they are rather straightforward or too hypothetical, how to approach data-related anticompetitive practices[12] remains unsolved. In order to address this controversial issue, the study will first unfold if there is a theoretical intersection between two legal regimes; second, analyse what is the interplay in practice in light of the case law; and third, discuss how this interplay should actually be.[13] It will finally propose a suggestion for the competition law assessment of data-related cases. Though the study focuses on the enforcement standards of the European Union (EU), references will be made to other jurisdictions to provide a comparative analysis.

[12] Unilateral or coordinated effects analyses in the merger investigations are included.
[13] The study excludes the role of big data in relevant market and market power assessments for an in-depth analysis of anticompetitive practices.

PART I

IS THERE AN INTERSECTION BETWEEN DATA PROTECTION LAW and COMPETITION LAW?

Several arguments have been raised for integrating data protection policies with competition law. On the one hand, the European Data Protection Supervisor (EDPS) suggested that data protection rights should be considered within competition law enforcement and market power in digital markets should be regulated accordingly.[14] On the other hand, the European Commission (EC) and national competition authorities heavily discussed on big data and data protection issues when assessing competition law cases.[15]

In order to be able to healthily scrutinise the interplay between data protection and competition laws, it is first necessary to analyse if there is an intersection between the two. The backgrounds, goals, scopes and tools of both legal regimes are crucial factors that pave the way for the interplay. In that respect, this part will unfold the legal concepts of data protection and competition law in the EU respectively and examine their characteristics in a comparable way in order to identify if there is an intersection.

1.1. Data Protection and Privacy Laws

In the international context, for the first time, although not binding, the Universal Declaration of Human Rights (UDHR, 1948) laid down that *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour*

[14] EDPS, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 22 July 2019.
[15] Moorcroft and Strat (n 5).

and reputation. Everyone has the right to the protection of the law against such interference or attacks".[16] International Covenant on Civil and Political Rights (1966), an international treaty that 169 parties are committed to, rule similar provisions.[17] It is self-executing and has the power to influence national laws. Moreover, after the Snowden revelations[18] in 2013, the United Nations endorsed new resolutions regarding the right to privacy in the digital age. They prohibited mass surveillance due to its potential detrimental effects on democracy, freedom of expression and private life.[19]

In Europe, data protection rules are safeguarded under both Council of Europe and the EU. After the adoption of the UDHR, the Council of Europe's European Convention on Human Rights (ECHR, 1950) which is legally binding, affirmed the right to privacy as well.[20] It prohibited public authorities from interfering with the exercise of this right unless based on a legal ground. Although it does not contain a specific provision on data protection, its provision is broadly interpreted to also cover data protection.[21]

Both the UDHR and ECHR, were established well before the era of the information society, internet or even computer. While these inventions provided unique benefits in terms of quality of life, efficiency and productivity, they have also created threats to privacy. Consequently, a new term of privacy, namely 'informational privacy' or 'right to informational self-determination' has been derived to be able to specifically regulate the collection and usage of

[16] Art.12.
[17] Art.17.
[18] Geoff Dyer and Richard McGregor, 'Spying: Too Much Information' (*Financial Times*, 1 November 2013) <https://www.ft.com/content/ce0cd70e-42e5-11e3-8350-00144feabdc0> accessed 12 July 2019; 'The Five Most Important Events of 2013' (*Financial Times*, 29 December 2013) <https://www.ft.com/content/d6449a2a-5dcd-3e5a-ae14-0de7a10f9089> accessed 12 July 2019.
[19] 'Handbook on European Data Protection Law' (*European Union Agency for Fundamental Rights*, 16 May 2018) 22 <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> accessed 20 June 2019.
[20] Art.8.
[21] Graef (n 10) 283–284. See cases *Amann v Switzerland* (2000) ECHR No.27798/95 para.65; *Rotaru v Romania* (2000) ECHR No.28341/95 para.43.

personal information. Data protection legislation has been established eventually in the light of these new terms.[22]

With that regard, first data protection laws in the EU were established during 1970s by Germany and Sweden. Then in 1980, the OECD declared Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[23] It delineated the core principles regarding privacy and personal data protection. A year later, the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) was signed. In the international context, it serves as the unique binding source for data protection laying down the general principles and rules. It covers all data processing activities no matter if realized by public, or private sectors, courts or government agencies.[24]

When it comes to EU specific rules, however, data protection law is a combination of several primary and secondary laws. In that respect, the adoption of the Lisbon Treaty (2009) represents a milestone for two major developments: First, the EU Charter of Fundamental Rights (Charter), which is aimed to incorporate all individual rights in the EU to a single document, upgraded as a binding source with the Lisbon Treaty.[25] Because the Charter requires the EC to *"respect the rights, observe the principles and promote the application thereof in accordance with their respective powers"*[26], it is argued that data protection and privacy became privileged goals, inter alia, over competition law goals.[27] However this type of interpretation has not been

[22] 'Handbook on European Data Protection Law - 2018 Edition' (n 6) 18.
[23]'OECD Guidelines' <https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en> accessed 21 June 2019.
[24] 'Council of Europe Data Protection' <https://www.coe.int/en/web/data-protection/home> accessed 21 June 2019.
[25] 'Why Do We Need the Charter?' (*European Commission*) <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en> accessed 20 June 2019.
[26] Art.51(1).
[27] Costa-Cabral and Lynskey (n 9) 40–41.

confirmed by the courts. Second, it provides a legal basis to enact secondary law on data protection[28]. As a result, the General Data Protection Regulation (GDPR) was ruled in 2016[29], replacing the Data Protection Directive (DPD, 1995) and is being applied since 2018.[30]

It is worth analysing the GDPR specifically as it constitutes the current major omnibus data protection regulation of the EU.[31] The underlying purpose of DPD was to ensure free flow of personal data between member states (MSs)[32]. Since directives do not directly apply to MSs, the effectiveness and dissuasiveness of the DPD had long been criticised.[33] Thus, to accomplish a sufficient and equal level of protection in every point of the union and to modernise the law according to technological developments , an EU level regulation was ruled. In that context, the GDPR is not only established for right based but also economic based goals.[34]

To analyse its intersection with competition law, some substantial aspects of the GDPR are notable. First, the GDPR clarifies previous rights, obligations in the DPD and also principles in the OECD Guidelines and Convention 108[35], but with several changes that adapt itself to technology and the ways that personal data is collected. Thus, it enables a broader scope for privacy enforcement.[36] It defines personal data wider as *"any information relating to an*

[28] Treaty on the Functioning of the European Union (TFEU), Art.16.
[29] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119
[30] 'Handbook on European Data Protection Law' (n 19); Graef (n 10); Costa-Cabral and Lynskey (n 9) 16.
[31] More specific regulations about data protection are also in force like Directive 2009/136/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive), OJ 2002 L337/11 or Directive (EU) 2016/680.
[32] DPD, Article 1(1).
[33] 'Handbook on European Data Protection Law' (n 19) 29–30.
[34] Art.1, GDPR. Accordingly, the European Data Protection Board is established as a body of the Union (Art.68). Moreover an independent supervisory authority (EDPS) has been constituted as secretariat of the Board (Art.75). EDPS operates at the highest level of the EU. ('About' (*European Data Protection Supervisor*, 11 November 2016) <https://edps.europa.eu/about-edps_en> accessed 7 July 2019.)
[35] Kevin Coates, *Competition Law and Regulation of Technology Markets* (1st edn, OUP 2011) 368.
[36] 'Understanding Key Changes from the Data Protection Directive to GDPR | Synopsys' (*Software Integrity Blog*, 18 January 2018) <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/> accessed 21 June 2019; Costa-Cabral and Lynskey (n 2) 16.

identified or identifiable natural person"[37]. The term identifiability broadly referred as designating a person by "all means" reasonably likely to be used.[38] Not necessarily names, identification numbers, but online identifiers like IP addresses, cookies and RFID tags might be deemed as personal data.[39] Sensitive data is deemed to include genetic and biometric data as well.[40]

Second, personal data processing is lawful as long as it relies on at least one of the six legal bases, most notable ones of which are consent, performance of a contract, public or legitimate interests.[41] No hierarchy exists between these bases.[42] The controllers may well rely on the grounds other than consent. However, when the controllers seek consent, terms offered to data subjects are subject to competition or may be improved by competition. For instance, limits and purposes of the processing or security may influence quality, variety and innovation.[43]

Third, the GDPR sets up borderlines between permissible and impermissible processing of individual data.[44] It introduces rights to data subjects and imposes obligations to data controllers/processors. The rights can be restricted against other societal interests such as national security, defence or other important objectives of the EU or an MS (like public health or social security) or the rights and freedoms of the others as far as the restrictions are necessary and proportionate.[45] This indicates that data protection authorities conduct a balance test for which competition authorities may not have enough competence.

[37] Art.4.
[38] Recital 26.
[39] Recital 30.
[40] Art.9.
[41] Art.6.
[42] Costa-Cabral and Lynskey (n 9) 16.
[43] ibid 30–31.
[44] ibid 17.
[45] Art.23.

With regards to the rights, the GDPR addresses the right to data portability[46], which is an entirely new provision that not only strengthens the personal data protection, but also challenges the businesses, especially cloud computing services to be able to facilitate the relevant infrastructure. The provision enables data subjects to receive and/or transmit their personal data that is provided to a controller by consent or contract in a structured, commonly used and machine-readable format. If technically feasible, direct transfer to another controller may be requested. The controllers are encouraged to establish in interoperable formats that enable data portability.[47]

Fierce debates have been raised among businesses about this right's implications on competition in terms of increasing users', customers' or consumers' trust and on competition law in terms of developing appropriate systems to be able to answer data portability requests.[48] This right ensures similar protection with the essential facilities doctrine. Limitations to data portability may result in entry barriers, when combined with network effects. However, the issue is investigated under competition law only when the undertaking is dominant. Whereas, the GDPR provides this protection regardless of the market power of the controllers.[49]

Fourth, although competition law is interpreted as having the strongest enforcement mechanism among consumer protection laws including data protection law, tougher sanctions were brought

[46] Art.20.
[47] Recital 68.
[48] G Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform' (2012) 2 International Data Privacy Law 149, 161–162 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ips009> accessed 22 June 2019; Barbara Engels, 'Data Portability among Online Platforms' (2016) 5 Internet Policy Review 17 <http://policyreview.info/node/408> accessed 22 June 2019; 'EU General Data Protection Regulation-Key Changes' (*DLA Piper Global Law Firm*) <https://www.dlapiper.com/en/europe/focus/eu-data-protection-regulation/key-changes/> accessed 21 June 2019.
[49] Laíse Bornico and Ian Walden, 'Ensuring Competition in the Clouds: The Role of Competition Law?' (2011) 12 ERA Forum 265, 284 <http://link.springer.com/10.1007/s12027-011-0223-y> accessed 30 July 2019.

under the GDPR as well. Prior to the GDPR, the amount of fines have been determined by MSs.[50] Consequently, the protection was fragmented between MSs, which was one of the fundamentals reasons that the DPD was replaced with a regulation. Indeed, that may have stimulated the data protection advocates to propose data protection concerns to be examined under competition law enforcement, which has tougher penalties.

However, after the enactment of the GDPR, data controllers may be penalised up to 10 or 20 million EUR or, in the case of an undertaking, up to 2 or 4% of the total 'worldwide' annual turnover of the preceding financial year depending on the types of infringement.[51,52] Like competition law, the GDPR is currently ranked among the laws having the highest sanctions for noncompliance.[53] Moreover, damages action can be taken against privacy breaches no matter the damage is material or immaterial[54], even mere emotional distress may be deemed sufficient for the liability of the data controllers as can be seen *Google v Vidal-Hall* case in the United Kingdom.[55]

Having analysed the fundamental goals, principles and vehicles of data protection law, the next section will exercise similar points in the context of competition law.

[50] Arts.22-24, DPD. For instance, in the United Kingdom, monetary penalties were 'just' up to £500,000.
[51] Art.83, GDPR.
[52] Oliver Yaros and others, 'European Union:GDPR Fines Lessons From Competition Law' *Mondaq Business Briefing* (12 December 2018).
[53] 'EU General Data Protection Regulation-Key Changes' (n 48).
[54] Art.82, GDPR.
[55] [2015] EWCA Civ 311.

1.2. Competition Law

Competition law in the EU has been primarily developed by the courts. As for the courts, they identified infringements by reference to the union goals.[56] Article 3(3) of the Treaty on the European Union reads the union goals, inter alia, as establishing an internal market and working for the development of the EU on the grounds of balanced economic growth, competitive social market economy, social progress, protection of environment. The Protocol (No 27) on the internal market and competition[57], then, clarifies that the internal market within the meaning of Article 3(3) includes a system ensuring that competition is not distorted. In that respect, by legislation, the EU set multi-type goals with the overriding principle of free internal market.

In practice on the other hand, promoting European integration and protecting competitive process were key objectives. While competition law always has been used as a tool of market integration, protection of competitive process was unclear and evolved over time. First, with influence of ordoliberals, it was defined as approaching towards perfect competition by contesting economic power. Second derivation is ensuring economic freedom.[58] This is meant, for instance, in abuse of dominance context, freedom of SMEs not to be foreclosed from a market.[59] Furthermore, after 2004, a more economics-based approach is announced by the European Commission (EC). Consumer welfare is emphasized as a significant component of the integrated market objective. Attention is devoted to types of conducts that eliminate

[56] Although courts for sometimes referred to examples provided in Article 102 and conducted analogical approach, in general they pursued a teleological approach, i.e. basing the analysis to the union goals. Damian Chalmers, Gareth Davies and Giorgio Monti, *European Union Law: Cases and Materials* (2nd edn, Cambridge University Press 2010) 1008–1009.
[57] Protocol (No 27) on the internal market and competition [2012] OJ C 326/309.
[58] David Gerber, *Global Competition: Law, Markets, and Globalization* (Oxford University Press 2010) 184.
[59] Eleanor Fox, 'Imagine: Pro-Poor(Er) Competition Law' (OECD 2013) DAF/COMP/GF(2013)12 332 <https://www.oecd.org/daf/competition/competition-and-poverty-reduction2013.pdf> accessed 18 March 2019.

competition and ultimately are most harmful to consumers.[60] In other words, after modernisation process, efficiency and consumer welfare became predominant goals.

Yet, 'can consumer welfare goal encompass data protection/privacy' arises as another paramount point to be exercised individually. Indeed, pursuing non-efficiency objectives is not a new debate. [61] It has long been questioned. It is hard to convert non-efficiency concerns such as media pluralism, environmental protection, public health as well as data protection into economic measures. Competition authorities do not have sufficient legal competence and technical expertise. Thus, they are principally regulated by other laws as long as they cannot be transformed into economic efficiency benefits.[62]

Nevertheless, recently, a developmental approach containing non-efficiency goals is contended over the world.[63] Even the EU along with the United States (US) started to argue[64] competition law with respect to their national security or public interests concerns for instance.[65] These arguments are rejected because such instrumentalisation of competition law to political interests may distort the competition.[66] Likewise, data protection advocates endeavour to incorporate data protection with consumer welfare goals.[67] Despite these arguments, enforcement of

[60] Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009] OJ 45/7 (Guidance Paper), paras.1,5.
[61] Daniel Zimmer (ed), *The Goals of Competition Law* (Edward Elgar Publishing 2012).
[62] Costa-Cabral and Lynskey (n 9) 13; Graef (n 4) 124; Coates (n 35) 394.
[63] Mor Bakhoum, 'Reflections on the Concepts of "Economic Freedom", "Free Competition" and "Efficiency" from the Perspective of Developing Countries' in Daniel Zimmer, *The Goals of Competition Law* (Edward Elgar Publishing 2012).
[64] Guy Chazan, 'Altmaier Urges EU to Protect Technology from Chinese Rivals' (*Financial Times*, 17 February 2019) <https://www.ft.com/content/6757ca9a-3048-11e9-8744-e7016697f225> accessed 16 March 2019.
[65] 'Mergers: Commission Prohibits Siemens' Proposed Acquisition of Alstom' (*EC-Press Release Database*, 6 February 2019) <http://europa.eu/rapid/press-release_IP-19-881_en.htm> accessed 17 March 2019; Guy Chazan, 'Germany Backs French Call for Right to Overturn EU Merger Decisions' (*Financial Times*, 19 February 2019) <https://www.ft.com/content/66c932d8-344b-11e9-bb0c-42459962a812> accessed 17 March 2019.
[66] Dina I Waked, 'Antitrust Goals in Developing Countries: Policy Alternatives and Normative Choices' (2015) 38 Seattle University Law Review 945, 974.
[67] EDPS (n 14).

competition law turned out to persistently focus on economic efficiency on behalf of the consumers.[68]

Having regard to the main statute and goals, the EU competition law intervenes in collusions, abuse of dominance position and concentrations that significantly impede effective competition.[69] Article 101 TFEU prohibits any agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect the trade between MSs and which have as their object or effect the prevention, restriction or distortion of competition within the internal market. This provision may be inapplicable provided that the conditions in Article 101(3) are satisfied.

Article 102 (TFEU) prohibits abuse of dominant position including exploitative abuses as well as exclusionary abuses. Albeit, it does not have a provision that enables legal exceptions like in Article 101, to distinguish competitive conducts from anticompetitive ones, a tool of objective justification or efficiencies defence is constituted by case law. However, cases law demonstrated that it is rather hard to meet requirements of objective justification and proportionality.[70]

Concentrations which have a union dimension in contrast, are subject to prior notification according to EU Merger Regulation by reference to turnovers of concentrating undertakings.[71] A merger will raise concerns when it is expected to substantially lessen the competition, i.e. weakens rivalry to the harm of consumers.[72] The EC has wide-range powers from accepting

[68] Graef (n 4) 124.
[69] Graef (n 28) 123.
[70] Maher M Dabbah, *EC and UK Competition Law: Commentary, Cases and Materials* (1st edn, Cambridge University Press 2004) 375.
[71] Council Regulation (EC) 139/2004 [2004] OJ L24/1.
[72] Dabbah (n 70) 529.

commitments put forward by undertakings to remedying those concerns to blocking the transaction entirely.[73]

After underlining the detailed aspects of the EU data protection and competition law, two legal regimes will be compared and contrasted in the next section.

1.3. A Comparison between Data Protection Law and Competition Law

In order to exercise if it is pertinent to incorporate data protection law concerns to competition law assessments in the context of the EU, comparing them in terms of their goals, means and scopes becomes indispensable. Whereas both aim to enhance free market integration, deal with power asymmetries and protect individuals, the means and the scopes of two regimes are different.

In terms of commonalities, firstly element is tackling with power asymmetries. Generally there is an imbalance between individuals and data controllers especially taken into account the digitalisation and cloud computing.[74] Data protection law remedies by requiring legal basis for processing and introducing rights to data subjects against unlawful processing. Similarly, competition law is concerned with undertakings which possess market power and reduce output or capacity, increase prices, decrease quality of products or restrict consumer choice or supress innovation.[75] If individuals lose control over their data, undertakings may strengthen their market power, likewise, increased market power may enable posing unlawful processing. In that respect two laws support each other.[76]

[73] Richard Whish and David Bailey, *Competition Law* (9th edn, OUP 2018) 849.
[74] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 0829/14/EN WP216 23 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 2 March 2019.
[75] Whish and Bailey (n 73) 2.
[76] Costa-Cabral and Lynskey (n 9) 21.

Second, both regimes target similar goals. In addition to market integration both areas of law are enforced for general public. Data protection law directly safeguards natural persons. With the assumption that data subjects are sensitive to privacy issues, data protection may emerge as a factor that boosts competition. Likewise, competition law, safeguards consumers against distortion of competitive process and direct harm through decrease in quantity, quality, variety or innovation.[77] Nevertheless, this similarity aspect involves conflicting assumptions. First, the sensitivity presumption of data subjects does not reflect the current reality[78]. While many users are concerned about privacy of their data, in rare cases they actually act on them.[79] This may create a hurdle and lead to vague assumptions when data privacy concerns are exercised in competition law cases as will be exercised in the consequent parts. Second, there is no clear roadmap to ensure in which circumstances consumer welfare is maximised, for instance, in terms of proper price level that does not exploit the consumers. Competition authorities are deemed ill-placed to determine if price levels are exploitative or not.[80]

In spite of the similarities, data protection and competition law have significant divergences regarding their means and scopes. Firstly, data protection law targets to protect a fundamental right via enabling individuals control over personal data. Accordingly, they can restrict the collection and processing of personal data. Whereas, competition law targets consumers in general rather than individual customers. Besides, generally it protects consumers indirectly via intervening in anticompetitive conducts and mergers which may significantly impede effective competition.[81]

[77] ibid 22. Guidance Paper, para.6.
[78] Costa-Cabral and Lynskey (n 9).
[79] Coates (n 35).
[80] Whish and Bailey (n 73) 2.
[81] Graef (n 10) 333.

Secondly, data protection law pursues a human-rights based approach, while competition law pursues an effect-based approach especially after the modernisation process. Newly introduced right to data portability can illustrate this divergence explicitly. The GDPR provides the right to all individuals if the data is based on consent and processing is carried out by automated means. Whereas, competition authorities may attain data portability as a duty only if the controller is dominant and meets conditions specific to refusal to supply.[82]

Thirdly, the two fields differ in their scopes. The GDPR covers only personal data, whereas competition law may deal with all types of data. To illustrate via data portability, data cannot be requested to transfer unless it is related to identified or identifiable data subjects. Moreover, as opposed to data directly provided by the users, those derived from user behaviour or created by data analytics may fall outside the scope in case of a strict interpretation.[83] In contrast, if the abuse of dominance conditions are satisfied, competition law reaches to a wider scope irrespective of the type of data.[84]

1.4. Conclusion

Overall, there are some commonalities in terms of dealing with market asymmetries, protecting market integration and the general public. However, it may be misleading to acknowledge that they both aim to consumer welfare because data protection assumes that individuals are sensitive about their privacy. Additionally, competition law rarely applies for exploitation as competition authorities are not suitable for determining in which circumstances consumers are being exploited. Despite the commonalities, data protection law protects personal data of

[82] Guidance Paper para.81.
[83] Graef (n 29) 133.
[84] Graef (n 10) 333–34.

‘individuals’ via a human rights based approach, whereas competition law protects ‘consumers in general’ regardless of the type of data via an effects based approach.

With regards to substantive intersections of two laws, Lynskey and Cabral describe their relationship as “family ties” as both are under EU law family and have some similarities. Data protection and privacy may prevail other goals especially after the Lisbon Treaty’s coming into force. Although this argument is open to interpretation of the courts, it is admissible to conclude data protection law intersects competition law in three aspects.

First, conditions offered for consent or other data protection elements can create a competition parameter in terms of quality, choice and innovation. Theoretically, undertakings can both compete on or distort these parameters. Second, data portability creates an overlap despite of the differences in the scopes of application. Third, it is claimed to include data protection/privacy interests in competition law assessments with a wider interpretation of consumer welfare goal. However, for the third aspect it should be noted that ‘consumer law’ is more akin to data protection law as both are concerned with individuals rather than aggregate consumers.[85]

In sum, it is clear that the two regimes intersect each other in theory. To figure out how, the next part will concentrate on the cases in practice.

[85] Costa-Cabral and Lynskey (n 9) 18.

PART II

WHAT IS THE INTERPLAY BETWEEN DATA PROTECTION LAW and COMPETITION LAW?

Data accumulation by a few but large undertakings created concerns about data privacy especially due to world-shaking security incidences, and uninformed data collection/processing via cookies or invalid consent.[86] Several rules and regulations on data protection have brought into force to overcome these issues as referred in the previous part.

Simultaneously discussions on the interplay between privacy-antitrust regimes have been arouse in two major aspects. First, the adequacy and up-to-dateness of competition law especially against digital markets was questioned.[87] Second, many of large online undertakings are two or multi-sided platforms that benefit from network effects. The more users they have, the more users join them. This asymmetric power results in a take-it-or-leave-it approach against users. The users' control over personal data becomes challenging or even deceptive that they cannot negotiate for terms and conditions of use, just accept whatever is offered by those undertakings.[88] Therefore, competition law was regarded as a short-cut remedy for data protection infringements.[89]

However, there is an overflow of literature proposing intervention by competition authorities disregarding its scope. A number of scholars suggested employing competition law tools to

[86] Fabiana Di Porto, 'In Praise of an Empowerment Disclosure Regulatory Approach to Algorithms' (2018) 49 IIC-International Review of Intellectual Property and Competition Law 507 <http://link.springer.com/10.1007/s40319-018-0708-0> accessed 17 July 2019.
[87] Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11 Journal of Intellectual Property Law & Practice 856, 860.
[88] EDPS (n 14) 35.
[89] C Kuner and others, 'When Two Worlds Collide: The Interface between Competition Law and Data Protection' (2014) 4 International Data Privacy Law 247.

prohibit monopolies from directly exploiting individual data and enhance individual choice.[90] By doing so, a number of studies lack the substantial features of either side. For instance, some simply aim to challenge the market positions of dominant undertakings, which may be misleading, as competition law does not prohibit dominance. Whereas some others questioned the over-interventionist role attained for competition law.[91]

Having demonstrated that there is a theoretical intersection between data protection and competition law in the first part, this part aims to illustrate what is the intersection in practice. For that purpose, the proposals for intervention and non-intervention towards privacy-related cases will be analysed respectively, in the light of developments in practice, namely cases and academic studies. Therefore, instead of hypothetical scenarios, theories of harm encountered in practice and how competition law enforcement reacted them will be analysed.

2.1. Competition Law Approaches Towards Non-Intervention in Data-Related Issues

The intersection of competition and data protection law has evolved from the *Asnef-Equifax* case[92] in 2006. The ECJ was referred for an agreement between financial institutions to create a common credit history registry of their customers. In response, the ECJ did not consider the lawfulness of the processing of customer data. It simply declared that 'such data protection issues are not a matter of competition law'. The Advocate General (AG) did not favour inclusion of these issues in the main competition law assessment either.[93] Rather, he suggested informing the borrowers about the processing to allow them to follow which data is being

[90] EDPS (n 14); Marco Botta and Klaus Wiedemann, 'EU Competition Law Enforcement Vis-à-Vis Exploitative Conducts in the Data Economy' [2018] Max Planck Institute for Innovation and Competition Research Paper Series 90.
[91] Marixenia Davilla, 'Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules' (2017) 8 Journal of European Competition Law & Practice 370.
[92] Case C-238/05 *Asnef-Equifax et al v Asociación de Usuarios de Servicios Bancarios* [2006] ECR I-11166, para.63.
[93] ibid, Opinion of AG Geelhoed, para.56.

processed and rectify if it is necessary. However, the EC did not follow the opinion of AG and left the issue to the governors of data protection.[94]

From the wording of the ECJ, commentators rightly inferred that it does not exclude data protection as a whole, but implies that competition law enforcement should pursue its underlying objectives.[95] That can be illustrated with subsequent cases. In *AstraZeneca v. Commission* case[96], the court re-emphasized the necessity of at very least the restriction on competition to be able to pursue an abuse of dominance case.[97] The same approach towards the scope of competition law continued to be reflected in the following cases.

Attention towards the accumulation of data and data privacy have mainly been aroused by merger cases in digital markets. Debates are polarised on whether data accumulation should be regarded as a risk in competition law investigations. This notion was first argued in *Google/DoubleClick* merger[98] in 2008 at which time Google gathered large amounts of individual data as near-monopoly of online search market, and DoubleClick was the pioneer of "ad serving, management and reporting technology for website publishers and advertising companies". The merger meant monitoring what people search for and which websites they click at one hand. In that case personal data in subject was so significant that it could not be ignored.[99]

[94] Gabriela Zanfir-Fortuna and Sinziana Ianc, 'Data Protection and Competition Law: The Dawn of "Uberprotection"' [2018] SSRN Electronic Journal 1, 2 <https://www.ssrn.com/abstract=3290824> accessed 20 July 2019.
[95] Graef (n 10) 334–335.
[96] Case T-321/05, AstraZeneca v. Commission, 2010 E.C.R. II-2830, paras.310-312. Appeal dismissed. Case T-51/89 *Tetra Pak* v *Commission* [1990] ECR II-309, paras.23-24.
[97] Olivia A Altmayer, 'The Tipping Point - Reevaluating The Asnef-Equifax Separation of Competition of Data Privacy Law in The Wake of The 2017 Equifax Data Breach' (2018) 39 International Law 37, 52.
[98] Google/DoubleClick (n 7), paras.4-5, 192, 221-222, 278, 286-289, 329-332, 356-366.
[99] Zanfir-Fortuna and Ianc (n 94) 3–4; Altmayer (n 97) 43.

Therefore, the EC assessed both horizontal and non-horizontal concerns. For the elimination of DoubleClick as a potential efficient rival in intermediation for online advertisement, the EC determined there still remains a sufficient number of competitors. In terms of non-horizontal effects, it assessed foreclosure risks in search advertising and online intermediation services and ad serving markets. It also separately analysed risks due to consolidation of the databases of search behaviour and web browsing behaviour. After a market investigation, it concluded that the merger is unlikely to exclude competitors and significantly impede the effective competition.[100]

The difference of the merger is that for the first time personal data was examined as a separate asset. Many commentators argued that parties possess the most significant constituents of online advertising, transaction would create a position that cannot be achieved by the rivals and consequently would lead to harm to advertisers, publishers and consumers. Contrarily, the advertisers and publishers are not concerned with their data to be accessed by others and search data of the users is accessible via other competitors or third parties, according to investigation.[101] Moreover, contracts of advertisers with DoubleClick prohibit their data to be used in target ads on Google.[102]

Notwithstanding above assessments, the EDPS's arguments go against the grain of the EC. It criticised the EC for not examining effects of the merger on the search market, user data privacy and consumer welfare.[103] The EC, however, distinguished data protection concerns from its analysis. It pinpointed its analysis is without prejudice to data protection and privacy laws. It

[100] Graef (n 10) 288–300.
[101] Google/ DoubleClick (n 108) paras.361-363.
[102] Damien Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' [2013] SSRN Electronic Journal 12–13 <http://www.ssrn.com/abstract=2216088> accessed 22 July 2019.
[103] EDPS (n 14) 29–30.

assessed only data accumulation concerns in terms of network effects leading foreclosure.[104] Similar conclusion was obtained from the same investigation in the US, despite of a dissenting opinion. Commissioner Harbour claimed that greater attention should have been given to network effects and implications for data protection.[105]

Another case where privacy related issues have been brought into debate at least partially is *Tele Atlas/TomTom merger*[106] in 2008. It involved a vertical relationship between navigable digital maps of Tele Atlas and portable navigation devices of TomTom. The upstream market was a duopoly where the only rival was Navteq and TomTom possessed a strong position in the downstream market. The EC was concerned about the risk of a vertical input foreclosure. However, it concluded that it is unlikely due to the existence of Navteq and sales losses in maps could not be compensated by an increase in TomTom devices.

Unlike the expectations, the assessment of the merger was not based on data privacy. In fact, the parties claimed efficiencies as a result of feedback data from TomTom's customer base, which would help Tele Atlas develop its maps further. However, the EC did not appraise if feedback data involves personal data and if the transaction raised privacy concerns. It just considered sensitive data of undertakings rather than individuals.

Some commentators recognised this approach as political instead of representation of a legal attitude towards data protection. They asserted that the EC would not endanger its decision to be dismissed as there was no clear reason to rely on data privacy.[107] Moreover, the EC

[104] Geradin and Kuschewsky (n 102) 12–13; Zanfir-Fortuna and Ianc (n 94) 3–4.
[105] Dissenting Statement of Commissioner Pamela Jones Harbour in the matter of Google/DoubleClick FTC File No.071-0170.
[106] *TomTom/Tele Atlas* (Case COMP/M.4854) [2008] OJ C237/8, paras.193-237.
[107] Zanfir-Fortuna and Ianc (n 94) 6.

elaborated that the product value is influenced by the way user data is used. Albeit the case seems as an example for non-intervention to data protection issues, due to this elaboration, commentators argued that the EC acknowledges data privacy as an element of quality.[108]

Similar efficiency claims can be seen in *Microsoft's acquisition of Yahoo! Search*[109] in 2010. The EC assessed that the transaction would aid the merger in facilitating its algorithm via data from search queries, by which it can obtain more users, and in the end would better compete with Google.[110] Therefore, the EC referred to some underlying notions of the monetization feedback loop theory which involves (i) online platforms can monetize their services better by target advertising when they can access user data, (ii) consequently the demand from advertisers would increase and facilitate competition between platforms. This time, the EC approved the transaction since the merger would further compete with Google. Commentators stipulated if Google were the notifying party instead of Microsoft/Yahoo, the EC would assess the data as an entry barrier. Albeit, the EC evaluated large databases may restrict new entries, again it did not examine data privacy.[111]

With reference to Tomtom/Teleatlas and Microsoft/Yahoo! Search cases, the EDPS proposed that the EC analysed the protection of client confidentiality and incentives of the parties to mitigate concerns of customers.[112] As Costa-Cabral favourably mentions, the analysis of the EC comprised of consumers who are not enjoying confidentiality anymore and does not fully represent individual privacy. Therefore, the analysis was merely limited to privacy as a non-

[108] Graef (n 10) 308–309; Zanfir-Fortuna and Ianc (n 94) 6.
[109] *Microsoft/Yahoo! Search Business*, (Case COMP/M.5727) [2010].
[110] Ben Holles De Peyer, 'EU Merger Control and Big Data' (2017) 13 Journal of Competition Law & Economics 767, 780–781 <https://academic.oup.com/jcle/article/13/4/767/4802444> accessed 20 July 2019.
[111] Anca D Chirita, 'The Rise of Big Data and the Loss of Privacy' in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Berlin Heidelberg 2018) 166 <http://link.springer.com/10.1007/978-3-662-57646-5_6> accessed 19 June 2019.
[112] EDPS (n 14) 30.

price competition parameter.[113] In another way, however, the notion that competition on privacy is beneficial to consumers, is not novel in competition law enforcement and does not necessitate a new interpretation of consumer welfare.[114]

In *Telefonica UK/Vodafone UK/Everything Everywhere* joint venture decision[115], 2012, the parties planned to process data collected via its transaction and advertising services for targeted advertising and analysis of consumer behaviour purposes. Though the EC defined a separate market for data analytics services, it did not refer to data protection obligations[116] and privacy concerns specifically. The EC examined horizontal foreclosure effects rising from incorporation of different kinds of data, including personal, location, response, social behaviour and browsing data. It concluded that the database of joint venture does not amount to unique and essential data; a number of competitors like Google, Apple, Facebook, card issuers, reference agencies or retailers can have access to similar data from a number of channels like utilities providers or internet providers.[117,118]

Similarly, in 2014, the EC cleared the *Facebook/WhatsApp* merger.[119] It did not assess Facebook-Messenger and WhatsApp as close competitors in consumer communications services. Moreover in online advertising services, even if Facebook is assumed to use WhatsApp as an advertising platform, or utilise WhatsApp database for ads displayed on Facebook, there would still remain sufficient alternative suppliers for target advertising and

[113] Francisco Costa-Cabral, 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law' (2016) 23 Maastricht Journal of European and Comparative Law 495, 509 <http://journals.sagepub.com/doi/10.1177/1023263X1602300307> accessed 21 July 2019.
[114] ibid 503.
[115] *Telefónica UK/Vodafone UK/Everything Everywhere/JV* (COMP/M.6314) [2012] OJ C66/5, paras.542 557.
[116] Zanfir-Fortuna and Ianc (n 94) 8–9.
[117] Likewise, in Verizon/Yahoo, data on scrutiny was not characterized as unique. (Case COMP/M.8180), [2016], para.91-93.
[118] Davilla (n 91) 376; Zanfir-Fortuna and Ianc (n 94) 8–9.
[119] Facebook/WhatsApp n (8).

valuable user data for ads. Whereas, Federal Trade Commission (FTC) warned parties to ask for consent for any alteration in processing for the same case in the US. However, benchmarking the US with the EU would be misleading since the FTC is distinguished from the EC in respect that it is responsible both for antitrust and also privacy violations under Section 5 of the FTC Act[120].

The transaction led severe criticisms. Opponents claimed the merger encountered an aggregation of the two parties' databases[121], which possibly would endanger users when processed by big data analytics.[122] Conversely, the EC pinpointed that privacy concerns regarding the transaction is in the very scope of data protection. However, this does not mean refusing any possible links between competition and data protection matters. It, indeed, emphasized competition as a way of better communication services like privacy and security. Some scholars inferred that the EC hinted at data protection requirements as part of its analysis from its assessment that Facebook will need to first change its privacy policy in order to apply target advertising on WhatsApp.[123] For some, the EC acknowledged privacy as a competition parameter and monitored that WhatsApp lost some users after the merger announcement.[124] Some others criticised the decision as it did not analyse a separate market for acquisition of personal data and effects of the merger on competition on privacy. For instance, they criticised

[120] It prohibits "unfair or deceptive acts or practices in or affecting commerce". Although it is questioned if FTC has authority to intervene in privacy-invasions under Section 5, it continues to do so as the courts rejected appeals against its reach. (Gina Stevens, 'The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices Authority' [2014] Congressional Research Service 15, 4.)
[121] At that time encountered 1.3 billion Facebook users, of which 250-350 million were Facebook-Messenger users, and 600 million were WhatsApp users.
[122] Sih Yuliana Wahyuningtyas, 'Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market' (2017) 18 European Business Organization Law Review 785, 790–91 <http://link.springer.com/10.1007/s40804-017-0084-0> accessed 23 July 2019.
[123] Zanfir-Fortuna and Ianc (n 94) 3.
[124] Costa-Cabral and Lynskey (n 9) 25–26.

the decision as not questioning if WhatsApp's privacy policies could change due to Facebook post- transaction.[125]

Moreover, post-merger developments further illustrate how the two regimes complementarily function in the context of their own scope. In 2016, WhatsApp announced it would share user data such as phone numbers and device details with Facebook to be used for better advertising. However, the parties ensured that they would not share their databases when the transaction was notified. Yet, in order for a controller to be able to transfer such data, it needs to rely on a legal basis such as explicit, freely given, specific, informed and unambiguous consent according to the GDPR.

In contrast, WhatsApp failed to provide it, specifically (i) created a false impression that if users do not subscribe in thirty days, they cannot use the service, (ii) imposed a preselected opt-in, (iii) provided opt-out option pages later that users could not figure out they can opt-out, (iv) executed unfair terms of use in the contract. Consequently several cases were held in MSs. For example in 2016, Germany Data Protection Commissioner of Hamburg ordered Facebook to stop collecting and delete user data acquired from WhatsApp. In Italy, in 2017, the Consumer Protection Authority imposed a fine of €3 million.[126]

It should be underlined that these sanctions are concerning data protection law. With regards to competition law, however, the link was misleading information for notification of transaction. The EC conducted a follow-up investigation, detected the user accounts of the two entities can

[125] Graef (n 10) 345–46.
[126] Guy Chazan and Madhumita Murgia, 'Germany Orders Facebook to Stop Collecting WhatsApp Data' (*Financial Times*, 27 September 2016) <https://www.ft.com/content/f6db8738-8497-11e6-8897-2359a58ac7a5> accessed 24 July 2019; Nic Fildes and James Politi, 'WhatsApp Fined €3m over Facebook Data Sharing in Italy' (*Financial Times*, 12 May 2017) <https://www.ft.com/content/2fdb5f34-3728-11e7-bce4-9023f8c0fd2e> accessed 24 July 2019.

be matched contrary to what Facebook claimed during the transaction and fined Facebook with €110 million on that basis.[127]

Some scholars characterised the Facebook/WhatsApp merger together with Google/DoubleClick as missed opportunities to confront modern-day "anti-competitive and strategic practices concerning personal data in digital markets". They argued competition laws are ill-suited for fast moving digital markets.[128] Though, it may be argued that the USA could still not enact a general data protection law covering all its states and markets, and still continue to offer protection under fragmental regulations[129], the EU has a separate omnibus authority for data protection.

Furthermore, the follow-up developments after the merger constitute three paramount consequences in terms of this study. First, had the EC challenged the transaction just for privacy concerns, this would not have only lowered the standards of proof, but also undermined the possibility of data transfer on legitimate grounds. For instance, WhatsApp might have well informed its users and transferred data after a lawful consent. Second, competition law lacks the legal ground and expertise to assess a legal consent or other bases which is in the very scope of data protection law. Third, when a privacy breach raises, this case illustrates each legal regime can intervene in within the reach of their own legal regime effectively and function complementarily.

[127] Altmayer (n 97) 44–45.
[128] Chirita (n 111) 166–167.
[129] Coates (n 35) 388.

2.2. Competition Law Approaches Towards Intervention in Data-Related Issues

A case where the EC explicitly conducted data protection issues in competition law enforcement was *Microsoft/LinkedIn* merger[130] in 2016, though the link was again not privacy but data accumulation. The EC scrutinised several areas in relation to the merger. First, regarding online advertising services, horizontal effects of merging user databases were analysed. More specifically, the risk of linking user's work history, professional connections, search behaviours with advertising services was investigated. The EC cautiously underlined that parties in general and consolidation of data in specific are subject to data protection laws of MSs and the GDPR. Notably, it added that such combinations would be applied based on (lawful) consent as well. Thus, instead of privacy-intrusion, it examined if the merged data leads an entry barrier, but concluded that it would not be the case since rivals can still reach large amounts of data and neither of the two entities transfer user data to third parties.[131]

Second, vertical effects were examined regarding customer relations management and software solutions. In these areas, the EC specifically questioned the risk of foreclosure of rivals from input provided by LinkedIn. Then, not only it concluded that LinkedIn does not provide its data to third parties and its database is not essential, but it also re-emphasized the liability of Microsoft under data protection laws in case it uses the LinkedIn database as a whole.[132]

Finally, conglomerate effects were scrutinised. The risk of Microsoft to 'use its dominant position in operating systems for personal computers and productivity software' to enhance LinkedIn's position regarding professional social networking has led the merger to end up with

[130] *Microsoft/LinkedIn* (Case M.8124) Commission Decision C(2016) 8404 [2016].
[131] ibid paras.177-79, 337-51. Altmayer (n 97) 53–54; Zanfir-Fortuna and Ianc (n 94) 15–16.
[132] ibid paras.246-370. Marixenia Davilla, 'Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules' (2017) 8 Journal of European Competition Law & Practice 370, 374 <https://academic.oup.com/jeclap/article-lookup/doi/10.1093/jeclap/lpx039> accessed 17 July 2019.

commitments. This risk involved the integration of LinkedIn to Microsoft Office, leading entry barriers to LinkedIn's competitors, as well as a decrease in incentives to offer better privacy policies. Thus, the merger was cleared conditionally upon three situations: (i) the LinkedIn software should be removable from Microsoft products, (ii) Microsoft products should be operable with other professional social network services, (iii) and these competitors should be allowed to access "Microsoft Graph" to help drive new subscribers to their own competing social networks.[133] It should be noted that these concerns fundamentally stemmed from Microsoft's market position in another market, not from data accumulation matters.

Inspite of commitments linked to data access issues, Microsoft/LinkedIn is not the first case. In *Thomson/Reuters* merger[134] concerning a consolidation between two suppliers of the financial database, the EC identified the foreclosure risk against desktop product providers. Hence, entities proposed divesture of copies of their databases to third parties. These cases illustrate the extremity of the proposals towards adjustments of competition law specific to big data matters. What was carried out in *Magill*[135], *IMS Health*[136] or *Microsoft*[137] cases, is also well-suited to the cases above.[138]

Although the above cases illustrate somehow an intervention in terms of data protection, albeit they did not encounter what advocates of data protection exactly expected, the newly announced

[133] ibid para.350, Altmayer (n 97) 53–54.
[134] *Thomson/Reuters* (Case COMP/4726) Commission Decision C(2008) 654 [2008].
[135] Joined cases C-241/91 and C-242/91 *Telefis Eireann and Independent Television Publications Ltd v Commission of the European Communities* [1995] ECLI:EU:C:1995:98
[136] Case C-418/01 *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG* [2004] ECLI:EU:C:2004:257
[137] Case T-201/04 *Microsoft* [2007] ECLI:EU:T:2007:289.
[138] Dr Federico Marini-Balestra and Dr Riccardo Tremolada, 'Digital Markets and Merger Control: Balancing Big Data and Privacy against Competition Law - a Comment on the European Commission's Decision in the Microsoft/LinkedIn Merger' [2017] European Competition Law Review 337, 344.

case of *Amazon*[139], may signal an approach in an opposite way. Based on its preliminary findings, the EC started an antitrust investigation for Amazon's use of 'sensitive data' of 'retailers'. Amazon offers two-sided services as online sale of goods as a retailer and hosts its marketplace for independent retailers whose data about products and transactions is being continuously collected on the platform. The investigation will detect if and how Amazon used accumulated data of retailers against competition and towards selection of the retailers to be displayed in the Buy Box[140]. Though the investigation has just started, regardless of its outcome, in case the so-called sensitive data of retailers includes personal data[141], the case will constitute the first comprehensive case of the EC with a competition related theory of harm based on privacy-intrusion. Seemingly, the concerned data is more of commercial data than private data. In that case, the investigation will constitute just another example where data is analysed only for the exclusion of rivals.

Interventions to dominant undertakings in that respect have long been signalled by both the EDPS and the EC Commissioners.[142] They implied the dominant companies might apply for privacy infringements to obtain an advantage against competitors.[143] Graef favoured data protection law can be used as a benchmark to capture new types of infringements in digital markets as well. She argued there would be no reason not to scrutinise a separate competition violation 'when a strong link is established between privacy infringements and dominance'. But notably she also addressed that any violation of data protection by dominant undertakings

[139] Jon Porter, 'EU Opens Amazon Antitrust Investigation' (*The Verge*, 17 July 2019) <https://www.theverge.com/2019/7/17/20696214/amazon-european-union-antitrust-investigation-third-party-seller-marketplace> accessed 23 July 2019.
[140] A tool that allows customers to add items from a specific retailer directly into their shopping carts and is vital for retailers due to its volume of transaction.
[141] The GDPR only applies to personal data which is any information related to an identified or identifiable natural person by reference to inter alia economic identity of these natural persons (Article 4(1), GDPR).
[142] EDPS (n 14); 'European Commission-Press Release-Speech-Competition and Personal Data Protection, Commissioner Joaquín Almunia' <https://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> accessed 17 August 2019.
[143] Graef (n 4) 136.

should not automatically be acknowledged as abuse of dominance. In that respect commercial or individual privacy issues should primarily be handled by consumer and data protection authorities.

Similarly *Facebook* is under scrutiny by the Bundeskartellamt.[144] Facebook collected vast amounts of data by embedding its products (like button, Facebook login option and Facebook Analytics) to third-party websites. As consumers were not adequately informed about the type and extent of their processed data, the consent is found to be invalid. Facebook's privacy infringement consequently led to an abuse of dominance investigation. This opens a gateway to refer data protection principles like data minimisation, purpose limitation as a benchmark in competition law analyses.[145]

However, it should be noted that Amazon and Facebook cases seem to differ in their theories of harm. While the former is concerning commercial data and exclusion of rivals, the latter seems more to examine personal data and direct exploitation of consumers. The Bundeskartellamt included the exclusionary theory of harm on the basis that unfairly accumulated data led to identity-based network effects and user lock-in, which consequently excludes rivals. Nevertheless, this theory is found problematic and unconvincing since foreclosure effect has failed to be established.

[144] 'Bundeskartellamt-Homepage-Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources' <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 25 July 2019.
[145] Graef (n 4) 136.

The EC illustrated its harm theories especially when it diverged from categorical infringements like in Microsoft[146] or Google Android[147]. In Microsoft the EC relied on market surveys and networks effects. In Google Android, it relied on status-quo bias (consumer inertia) of users that make them stick to pre-installed options. Whereas, in the Facebook case foreclosure effects were not based on a clear evidence.[148] Just embedding Facebook products to other web sites, for instance, do not inhibit other social network services from doing the same.[149] Apart from these debates, however, these cases illustrate again that there is no need for a new competition approach specific to data-intensive markets.[150]

Another example of privacy-antitrust interplay with a strong theory of harm can be seen from the Autorité de la concurrence's (French Competition Authority, FCA) *GDF-Suez (ENGIE)* decision in 2017.[151] The case represents an illustration of both the duty to share individual data with competitors and how a competition authority orders to comply with data protection rules. GDF Suez was a formerly monopolist natural gas supplier and settled with the FCA for using customer datasets and infrastructure it obtained via its monopoly status to foster its contacts in other markets (and offer prices outside the scope of public service obligation). The FCA regarded that although datasets containing contact details, technical information and consumption data are not essential assets, GDF-Suez did not obtain it by innovation but merely by its monopolistic status and the dataset created a competitive disadvantage against its

[146] *Microsoft* (Case COMP/C-3/37.792) [2004] OJ L32/23.
[147] *Google Android* Commission Decision AT.40099 [2018].
[148] Vikas Kathuria, 'Greed for Data and Exclusionary Conduct in Data-Driven Markets' (2019) 35 Computer Law & Security Review 89, 100–101 <https://linkinghub.elsevier.com/retrieve/pii/S0267364918303820> accessed 25 July 2019.
[149] Giuseppe Colangelo and Mariateresa Maggiolino, 'Data Accumulation and the Privacy–Antitrust Interface: Insights from the Facebook Case' (2018) 8 International Data Privacy Law 224, 228 <https://academic.oup.com/idpl/article/8/3/224/5198967> accessed 25 July 2019.
[150] Kathuria (n 145) 100.
[151] 'French Competition Authority Fines ENGIE €100 Million for Abusing Its Dominant Position on the French Retail Gas Supply Market' (*Van Bael & Bellis*) <https://www.vbb.com/insights/competition/abuse-of-dominance/french-competition-authority-fines-engie-100-million-for-abusing-its-dominant-position-on-the-french-retail-gas-supply-market> accessed 27 July 2019. FCA regarded the fact ENGIE might not be aware of its obligations immediately after diversification as a mitigating factor for the fines.

competitors. Thus, GDF-Suez was imposed an interim measure to provide its competitors access to datasets[152] it collected before diversification so that its competitors would be able to reach potential customers.[153]

Second aspect of the case is pertinent to the way the FCA ordered an interim measure. First, the FCA referred to the opinion of the French Data Protection Authority (FDPA) about the case. So far this interaction confirms what the EDPS recommended in its preliminary opinion. It underlined that competition, data protection and consumer protection authorities should all coordinate for a more effective enforcement. Nevertheless, the FCA obliged the undertaking to specifically notify customers about the case and ask their consent for sharing their data with third parties and it provided GDF-Suez a draft notification which urges customers to send a letter in thirty days if they do not prefer transfer of their data.

Several arguments were raised against the second aspect. First the way of forcing customers to take action themselves for not giving consent may not be in line with the data protection rights. It would be more appropriate to provide them both with the choices of 'opt-in' and 'opt-out'. In Microsoft or Google cases and Microsoft/LinkedIn merger, the significance of default settings and status-quo bias towards pre-installed options have already been illustrated. Second, there may be other ways of legitimate bases. Third, how to comply with data protection rules is not in the FCA's reach. Consequently, commentators claimed the authorities should have performed a closer cooperation. It would have been more appropriate had the FCA provided a general statement about the need to comply with data protection when granting duty to share

[152] Names, addresses, telephone numbers and consumption profiles.

[153] 'Competition Law and Data' (Autorité de la concurrence and Bundeskartellamt 2016) 31 <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big%20Data%20Papier.html> accessed 27 July 2019.

and left the FDPA to monitor if the remaining steps of GDF-Suez are in line-with data protection.[154]

2.3. Conclusion

In the light of above cases, it is clear that data may not just represent an input but also a separate asset. Moreover, we can observe that the data can take several forms in the context of anticompetitive conducts. It may constitute an entry barrier due to the accumulated big data which risks exclusion of rivals, a privacy-intrusion which risks exploitation of consumers/data subjects or a competition parameter which is considered as an ingredient of quality.

First, in almost all cases exclusionary/foreclosure effects rising due to accumulated data are examined. Data is analysed against creating an entry barrier, or against constituting an essential facility. In that respect, Microsoft/LinkedIn case presents a notable example. It ended up with commitments. However, the risks considered in that case were mainly on the bases of tying/interoperability theories rather than data accumulation/privacy concerns. But it should be noted that this approach is not specific or new to digital markets. For instance in Thomson/Reuters case, the merging databases are divested due to the concerns about data access.

Second, except the cases like Microsoft/LinkedIn, the EC concluded there still remains sufficient competition or alternative channels to reach data. Despite the reactions against big data, the data accumulation cases like Facebook/WhatsApp or Google/DoubleClick mergers were not deemed to close the substantial part of the relevant markets. Therefore, it is unlikely

[154] Graef (n 10) 317.

for data-related transactions to be intervened in unless the data is unique and non-replicable by the rivals.[155]

Third, both the ECJ and EC distinguished data protection concerns, data protection obligations, individual rights, lawfulness of the processing from its analyses either by not mentioning them or explicitly addressing them by not being covered under competition law. In Asnef-Equifax case, the ECJ rightly refused to order the parties to inform their customers about processing. Although the FTC carried out such an approach in Facebook/WhatsApp merger, the structure of data protection and competition authorities are different in the EU. While the FTC covers both antitrust and unfair (including privacy intrusion) practices, in the EU, separate agencies are responsible for these areas. Therefore, competition agencies' may not be competent to order how to comply with data protection rules as illustrated in GDF-Suez case. Instead a more co-operative approach between competition and data protection agencies is suggested.

Fourth, competition rules are criticised as being ill-suited to digitised markets. The suggestion went beyond the value-based merger thresholds, privacy is proposed to be protected under the consumer welfare goal. However, developments after Facebook/WhatsApp transaction illustrate how competition and data protection agencies can catch the infringements while staying limited to their own reach.

Although these criticisms were not materialised EU wide, the Bundeskartellamt's Facebook case signals that exploitation of data subjects may account for abuse of dominance. It attempts to establish an exclusionary theory of harm, but, this is not deemed persuasive as there seems no impact on competitors. In that context, the EC Commissioners indicated that it requires

[155] De Peyer (n 110) 782.

‘restriction on competition/competitors’ as well as ‘consumers’. The newly announced Amazon case also seems to be in line with this notion as it includes creating a disadvantage against third party competitors. Even though it is not clear if the data scrutinised is commercial data of the retailers or personal data, when there is a strong link between data protection and competition law infringements, competition law can apply. In that respect, data protection rules may be used as a benchmark.

Fifth, the EC pointedly addressed in the mergers like Microsoft/LinkedIn, the processing of data can be carried out on a legitimate basis as well as privacy intrusion. Yet, the sensitivity of individuals against privacy differs considerably. For instance in Google/DoubleClick merger, while commentators argued for the privacy of the advertisers/publishers, the EC concluded that they do not worry about transfer of their data.

Sixth, in Tomtom and Yahoo mergers, the EC evaluated privacy as a parameter of competition amongst others like security. But some academics commented that the EC should have analysed the effects of the transaction on privacy as well as other parameters of consumer welfare. Given the above mentioned uncertainty about privacy sensitivity, it is questionable how precise that analysis could be made.

Having analysed the way of interplay between competition and data protection law in the light of data-related cases, the next part is devoted to discuss how this interplay should actually be. As we may envisage that there will be more cases especially about privacy related conducts of dominant undertakings, a closer look to the role of data-related exploitation in competition law is essential.

PART III

HOW SHOULD BE THE INTERPLAY BETWEEN DATA PROTECTION LAW and COMPETITION LAW?

The fundamental reason behind the controversies in the interplay between data protection and competition law is consumer welfare. As the first part illustrated, it is the common goal between two law systems. Data protection advocates favoured, inter alia, Article 102 can be used as a vehicle to promote data protection. Although the article in wording encompasses both exclusionary and exploitative conducts, the second part illustrated that in practice the EC focused on either exclusionary conducts or foreclosure effects. Furthermore, a consistent approach has been established by the ECJ not to intervene in direct exploitation.

Nevertheless, recent cases of especially national competition authorities are more inclined to deal with direct exploitation of consumers in terms of privacy in line with what data protection advocates propose. Therefore, to be able to figure out how the interplay between competition law and data protection law should be, it is necessary to examine the treatment towards exploitative abuses. In that respect, this part will first touch the limitations of competition law, then, that of privacy perception with respect to data-related exploitative practices, finally will suggest a cautious approach for the data-related cases.

3.1. Limitations of Competition Law Towards Data-Related Exploitative Practices

In order to enshrine the limitations of data-related exploitative practices, first the standards of competition law towards exploitation in general need to be analysed. The definition of abuse of dominance is not provided in Article 102, instead, the case law introduced the relevant

concept.[156] In Hoffman La Roche, the ECJ defined it as an objective concept where the dominant undertaking influence the structure of a market since competition is weakened because of its behaviours that cannot account for normal competition.[157] The ECJ further explained abuse as using methods other than those within the scope of competition on merits. Distinguishing permitted unilateral conduct from abusive ones was based on normal competition/competition on merits (or performance).[158]

Nevertheless, the notion of competition on merits is countered by scholars as being impractical and dangerous since it can easily be converted to a market regulation mechanism. They argued that it may lead courts to shape the performance of undertakings according to their choices instead of letting them be shaped by consumers and other market participants.[159] Similarly, some scholars contended that courts relied on competition on merits to ensure fairness. However, it was argued that this approach may not be viable due to its inadequacy of analytical power in terms of justifiability and predictability.[160]

Considering the case law, a "special responsibility" is assigned to dominant firms since the first judgements of the ECJ from the late 1960s to now.[161] Exclusionary practices like refusing to deal, below-cost or selective pricing, exclusive dealing are amounted to abuse of dominance as they distort competition to the detriment of consumers and impede economic freedom of SMEs.[162] In terms of exploitative practices, Article 102(2)(a) TFEU explicitly positions unfair practices as an example of abuse of dominance. However, in *Continental Can*, it is clarified

[156] Chalmers, Davies and Monti (n 56) 1008–1009.
[157] Case C-85/76 *Hoffmann-La Roche & Co. AG v. Commission*, [1979] ECR 461, para.91.
[158] ibid para.177.
[159] Dimitris Riziotis, *Abuse of Dominant Position: New Interpretation, New Enforcement Mechanisms?*, vol 5 (Mark-Oliver Mackenrodt, Beatriz Conde Gallego and Stefan Enchelmaier eds, Springer Science & Business Media 2008) 90.
[160] Chalmers, Davies and Monti (n 56) 1008.
[161] Gerber (n 58) 187. Case C-322/81 *Michelin v Commission* [1983] ECR 3461.
[162] Chalmers, Davies and Monti (n 56) 1008–1009.

that ‘exploitation itself is not sufficient for an abuse, a harm in effective competition is also required’. Yet, though a few, in some cases where markets were not believed to be able to self-correct, action was taken against excessive practices.[163]

Whereas, for more than half a century, the court decisions about exploitative practices are far less in number when compared to exclusionary practices.[164] Similarly the EC prioritised to intervene in exclusionary abuses as they appear to be more common. However, conducts like excessive pricing, which directly exploit consumers are acknowledged to be liable under Article 102 and the EC keeps the interruption as an alternative, especially when the markets cannot be ensured otherwise.[165]

In determining whether a pricing is unfair, the identification of *“whether the dominant undertaking has made use of the opportunities arising out of its dominant position in such a way as to reap trading benefits which it would not have reaped if there had been normal and sufficiently effective competition”* is emphasized.[166] As this definition is deemed quite similar to the definition of dominance, drawing the line between the two is found to be difficult.[167] Thus, prohibition of exploitative practices would mean prohibition of efforts towards profit maximization. This would discourage innovation and investment.[168] Furthermore, a significant issue about the exploitation via privacy is that these conducts are all designed in the context of a product or service which consumers pay for. Nevertheless, in data-related cases, most services are offered for free.

[163] Case 226/84 *British Leyland v Commission* [1986] ECR 3263; Case C-385/07 P *Der Grüne Punkt–Duales System Deutschland v Commission* [2009] para.141; *Deutsche Post AG* (Case COMP/C-1/36.915) [2001] OJ L331/40, para.159 et seq.
[164] Richard Whish, *Competition Law* (5th edn, OUP 2005) 194.
[165] Guidance Paper, para.7.
[166] Case 27/6, *United Brands Company v. Commission* [1976] ECLI:EU:C:1978:22, para.249.
[167] As well known, not the dominance itself but ‘abuse of dominance’ is prohibited,.
[168] Massimo Motta and Alexandre de Streel, *The Pros and Cons of High Prices*, vol 6 (Swedish Competition Authority 2007).

Having analysed the substantial aspects of exploitation abuses in general, the principal argument of the EDPS is to intervene in exploitation of data subjects under the consumer welfare approach.[169] It relied on the EC's prioritisation of consumer welfare in Guidance Paper. However, Guidance Paper has no binding power. The EC is bound by case law of the ECJ. Besides, the ECJ based its decisions primarily on competitive structure and market integration. The ECJ seldom referred to consumer welfare. Thus, if the EC handles consumer welfare broader to include data protection concerns, it will still need to demonstrate harm on competition before the courts.[170]

Second, the ECJ did not require a causality link between dominance and abuse, the dominant undertakings have special responsibility for distortion of competition regardless of the fact that conduct strengthens market power. One may infer, thus, there is no need to associate data protection infringement with market power.[171] However, commentators claim that the same assumption should not be sufficient for exploitative conducts, otherwise any infringement of law would mean abuse of dominance as well.[172]

Third notion put forward is that other laws like intellectual property law or national laws also had a normative influence on competition law enforcement.[173] The joint report of French and German competition authorities cited *Allianz Hungaria* case[174], to lay down infringements of other rules can be referred to the assessment of competition law restrictions. It also exemplified how cultural diversity is applied for the evaluation of a merger in *Universal/EMI* case[175]. There

[169] EDPS (n 14).
[170] Costa-Cabral (n 112) 503–512.
[171] Costa-Cabral and Lynskey (n 9) 35.
[172] Dr Thomas Höppner, 'Data Exploiting as an Abuse of Dominance: The German Facebook Decision | Lexology' (4 March 2019) <https://www.lexology.com/library/detail.aspx?g=242876ec-4401-4771-80ce-480623c6423e> accessed 2 August 2019.
[173] Altmayer (n 97) 45–46.
[174] Case C-32/11 *Allianz Hungária Biztosító and Others* [2013] OJ C141/3.
[175] *Universal Music Group/EMI Music* (Case COMP/M.6458) [2012] OJ C220/15, para.49.

is no point to argue this notion. As illustrated in the second part, the EC already considered privacy matters where relevant. However, these examples do not involve exploitative abuses of dominance, and should not be used to loosen the established standards.[176]

Furthermore, the report proposes excessive trading conditions as a new type of exploitation despite the fact that it acknowledges the practical difficulties of excessive pricing. It justifies this intervention with the fact that the users do not usually read the terms and conditions.[177] While competition law does not intervene in excessive pricing, which directly affects consumers, intervention for terms that consumers do not even prefer to read should be approached in extreme caution. Consumers generally prefer lower prices[178], whereas, it is hard to predict privacy attitude of consumers as will be discussed in the next section.

Contrary to above arguments, scholars identified these rare conditions as markets characterised by high and non-transitory entry barriers, super-dominance, absence of sector-specific regulation. Some academics also added hindering innovation of new products/services with particular caution not to discourage patent owners.[179] Comparing these conditions with the recent cases, the first obvious result is that the ECJ applies competition law regardless of regulation of the market with a specific law.[180] Indeed that is another reason why data protectionists claim to justify intervention against exploitation.[181]

[176] 'Competition Law and Data' (n 147) 22;
[177] ibid 25.
[178] except for giffen goods.
[179] David S Evans and A Jorge Padilla, 'Excessive Prices: Using Economics to Define Administrable Legal Rules' (2005) 1 Journal of Competition Law & Economics 97 <http://academic.oup.com/jcle/article/1/1/97/848949/Excessive-Prices-Using-Economics-to-Define> accessed 17 August 2019.
[180] C-280/08 *Deutsche Telekom AG v Commission* [2010] ECR I-9555.
[181] Kuner and others (n 89) 248.

However, this notion does not fully represent the standards established by the ECJ. First, in the *United Brands* case[182], it rejected excessive pricing claims because the EC failed to demonstrate that pricing had no reasonable relation to the economic value of the product. Whereas, it confirmed the discriminatory pricing between MSs, which is not surprising considering the per se prohibition of restricting the trade between MSs. This approach is still being pursued, indeed, with a more stricter way. In *MEO* case[183] in 2018, the ECJ not only further confirmed that in principle exploitative discrimination is unlikely to take place, but also required demonstration of the competitive disadvantage to establish an abuse. Consequently, the scope of justification for exploitation cases became even more restricted.[184]

Adjusting these standards to exploitation of data protection interests raises further concerns. How competition authorities will/can prove excessive privacy is one of these. If the ECJ continues the standards in MEO case, how the effects on data subjects will be illustrated is another concern. The individual behaviour towards privacy is hardly predictable as will be discussed in the next section. The conducts under Article 102 are forbidden only if the harm outweighs the efficiencies.[185] However, a balance between benefits and harm of the 'privacy' would be even more difficult to attain.

3.2. Limitations of Privacy Considerations Towards Data-Related Exploitative Practices

In addition to limitations of the competition law enforcement towards privacy exploitation, there are several constraints on the side of consumer behaviour towards privacy itself. First, contrary to the above-mentioned over-protectionist approach, Fuller criticises the EU privacy

[182] United Brands (n 166), paras.232-268.
[183] Case C-525/16, *MEO–Serviços de Comunicações e Multimédia SA v. Autoridade da Concorrência* [2018] ECLI:EU:C:2018:270.
[184] Botta and Wiedemann (n 90) 12–17.
[185] Whish and Bailey (n 73) 218.

control rules in the digital era as a whole. He underlines if personal data is the 'price' of access to digital platforms, then, any control that provides users not to supply personal data while at the same time utilising the website, is not different than 'price control'. Referring to the E-Privacy Directive, he explains mandating opt-in is different from mere consent as it forces entities not to exclude users even if they reject to opt-in. Tie-in sales, investment flights and altered exchange characteristics are some of the consequences of these rules.[186]

Second, the privacy paradox entails another constraint. Many data subjects are concerned about protection of their personal data, whereas, they do not take action accordingly. They do not even devote an effort to read or comprehend the terms and conditions or privacy policies. Firstly, privacy is a personal and diverse concept. While a data subject is unwilling to share data, another may be indifferent. Secondly, user behaviour alters in reference to context of the data they provide. Thirdly, some of the internet users are not aware of personal data protection rules and in which ways their data is being utilised like in target ads/tailored services etc.[187]

Arguments in favour of pursuing data-related exploitation cases, nonetheless, involve assumptions towards consumer behaviour. Coates emphasizes the competition law cannot decide which products/services are better/worse for consumers. What they actually should be concerned about are the competitive conditions, i.e. transactions are carried out voluntarily and appraised according to willingness to pay. With that notion, sensitive consumers will seek for companies with better protection, or make a trade between privacy and innovation.[188]

[186] Caleb S Fuller, 'Privacy Law as Price Control' (2018) 45 European Journal of Law and Economics 225 <http://link.springer.com/10.1007/s10657-017-9563-6> accessed 3 August 2019.
[187] Botta and Wiedemann (n 90) 25.
[188] Coates (n 35) 394.

Third, a study of NBER conducted in 2017[189], further revealed the results of privacy paradox. According to the study, first, students disclosed personal data in return for a small incentive (slice of pizza), although they indicated that privacy is significant for them. This illustrates zero price services are sufficient to gain the willingness of users for sharing personal data. Based on this result, one inevitably questions the viability of abuse of dominant cases due to imposing unfair trading conditions. Some commentators even argue that privacy lacks sufficient characteristics in that regard to be a competition parameter.[190]

Contrary to limitations due to privacy considerations, scholars favour competition intervention against targeted advertising. Chirita claimed that the consumers mostly do not know if their data is being processed, if so which data, by whom, how, for what purposes and to whom it is being shared/sold.[191] However, that is the very basic function of the data protection law. As provided in the first section, it is the GDPR that exactly encounters to answer these questions and more specifically to single out privacy misuse. Moreover, as she herself emphasizes, the ECJ declared that data protection law applies irrespective of the fact that processing led to inconvenience of individuals.[192]

Moreover, she contends as this is not the issue of individuals one by one, but a public concern to which only competition law can provide remedy not the consumer laws.[193] That notion totally dismisses not only the above-mentioned inconsistencies in privacy behaviours by generalising

[189] Susan Athey, Christian Catalini and Catherine Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' [2017] NBER Working Paper Series 34.
[190] Stefano Lucchini and others, 'Online Digital Services And Competition Law: Why Competition Authorities Should Be More Concerned About Portability Rather than About Privacy' (2018) 9 Journal of European Competition Law & Practice 563, 564 <https://academic.oup.com/jeclap/article/9/9/563/5067527> accessed 4 August 2019.
[191] Chirita (n 111) 167.
[192] Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* [2014] ECLI:EU:C:2014:238, para.33.
[193] Chirita (n 111) 168.

the attitude of consumer behaviours but also benefits of data accumulation. She criticised the EC cases for not analysing thorough economics of privacy. Yet, in some cases the EC rightly projected potential efficiencies of data accumulation in particular better targeted ads.[194] Moreover, the OECD identifies several potential gains from data-driven innovation. Improved quality, newly developed services, better understanding consumer needs, more useful results in web searches via machine learning algorithms, social benefits like reduced traffic congestion via the tracking of mobile devices are just some of them.[195]

Finally, there is a majority of literature with the focus on concerns about the big data and how data is converted to economic benefits by large undertakings. Attention should first be given to studies, which indicate there is empirical ground that large online platforms collect more data than smaller ones.[196] Second, although they propose competition intervention against these issues, they do not consider which standards of proof can be relied on. At least Chirita proposes intervention should be based on identifiable economic "harm to consumers of digital products or services as a result of exploitation of the consumers naïve trust and confidence".[197] Even the privacy is a currency of the new age, taking difficulties of identification of excessive pricing into account, one inevitably questions how can competition law detect a rather variable concept and its harm on consumers.

[194] See (n 106) and (n 109) in part II.
[195] 'Big Data: Bringing Competition Policy to the Digital Era-OECD' (n 1) 7.
[196] Chirita (n 111) 172.
[197] ibid 159.

3.3. Conclusion

In sum, the competition law approach towards data-related exploitation cases has a determinative role in the interplay between data protection and competition law. While Article 102 constitutes a controversial area of competition law, it is pertinent to say exploitation is even more controversial in the application of Article 102.[198]

The ECJ favoured not to intervene in exploitation unless exceptional circumstances occur since the early times of enforcement. Yet, recent cases also required proof of competitive disadvantage created by exploitation. Moreover, academics found competition law investigations in exploitation cases dangerous as they are hard to detect, justify, and predict, impede innovation and investment.

Although, one may not counter-argue utilising data protection law in competition assessments, as is the case with other laws as well, what data protection advocates propose goes well beyond this notion. Not necessitating a causal relationship between dominance and abuse in exploitation cases, may lead to false intervention.

Besides, the behaviour of consumers towards privacy is inconsistent. It does not only change according to individual in subject, one individual may reveal different outcomes when faced with different types of data, different environments, different incentives or costs. Yet, they are willing to share their data in return for zero-price services. In addition, data accumulation has a number of pro-competitive aspects as well. It provides several data-driven innovation benefits to consumers.

[198] Whish and Bailey (n 80) 849.

Therefore, unawareness or disinterest of the consumers should not be a ground for competition law intervention. Instead promoting data protection rules and facilitating privacy awareness among consumers would be a better and safer solution. Yet, the data protection authorities are the agencies that have the exact ability to counter the privacy misuse and other data related violations. Competition authorities do not have the same competence with data protection authorities to inspect harm on data subjects or remedy data protection issues.

OVERALL CONCLUSION and A SUGGESTION FOR DATA-RELATED CASES

This study examined the interplay of data protection and competition laws in the EU. Opinions are polarised on data accumulation and privacy protection against large undertakings. A number of commentators proposed competition law as a vehicle to fight with data accumulation, privacy-invasion or asymmetric power of undertakings over users. However, there is an overflow of literature that lacks standards of either of the two legal regimes, which may undermine the case law established over the years. Thus, the study aimed to provide a substantial analysis of the two laws to map if there is an intersection, if so in what ways and how the interplay between two laws exactly should be.

First step was to explore if there is an intersection in theory based on the backgrounds, goals, scope and tools of these law systems. Though there are some similarities with regards to goals, the difference in their scopes and tools should not be disregarded. In fact, both law systems are under EU law systems and thus, naturally have family ties. Relying on the obligation of the EC to respect and promote Charter rights, some commentators also argued data protection law may prevail competition law. Yet, this interpretation has not been confirmed by the courts. Moreover, data portability/duty to access or competition on privacy parameters create theoretical intersections even though a practical example still does not exist.

The most controversial part amongst these is the so called intersection in the consumer welfare goal. Commentators rely on this overlap to favour competition law intervention towards data protection issues. However, while competition law targets consumers as a whole, data protection law protects individuals with the assumption of all individuals are privacy sensitive.

Whereas, competition law targets economic efficiency which indirectly increases consumer welfare.

Second, after exploration of theoretical overlaps, the study questioned how this intersection is realised in practice. In the light of the case law, the study indicated that data may be handled as an asset as well as an input. The reluctance of the EC and ECJ should not be interpreted as rejection of data protection issues as a whole, rather A*snef-Equifax* case was a highlight of the underlying goals of the competition law. It necessitated at very least 'restriction on competition' for abuse of dominance investigations.

Concerns on data accumulation were aroused especially via merger cases in digital markets. The EC assessed data as a separate asset in Google/DoubleClick or *Telefonica UK/Vodafone UK/Everything Everywhere* cases. In either way, it exercised only foreclosure risks and left privacy concerns to data protection authorities despite fierce objections. Considering clearances in renowned Google/DoubleClick or Facebook/WhatsApp mergers, prevention of data-related transactions seems unlikely unless the data in subject is unique and non-replicable.

In contrast, there were some mergers that ended up with commitments due to foreclosure risks. Again the concern in this case was due to tying/interoperability risks arising from Microsoft's market position instead of data accumulation/privacy risks. It should be noted that this approach is not novel. Thomson/Reuters case is another example of divesture due to data accessibility risks rising from merging databases.

Several criticisms were put forward about the ill-placement of competition law to catch new infringements in digital markets. Nevertheless, above-mentioned merger cases indicate how

existing rules can remedy possible exclusion risks. Moreover, post Facebook/WhatsApp merger developments illustrate how data protection and competition authorities can detect infringements though respecting the reach of their scope. Otherwise, competition authorities risk forbidding lawful processing. GDF-Suez case illustrates how incompetent the competition authorities may be against imposing substantial data protection obligations.

The EC Commissioners implied to intervene in when dominant undertakings use privacy infringements to gain disadvantage against competitors as signalled in the EC/ECJ cases. However, recent cases of Amazon and Bundeskartellamt's Facebook facilitate the debates on intervention towards exclusionary versus exploitative conducts.

The third part delved into limitations in terms of competition law and privacy considerations towards data-related exploitative practices with that regard. On the one side, the ECJ intervened in direct exploitation only in rare conditions. Recently, MOE case illustrated even stricter standards of proof as it required the proof of competitive disadvantage. Exploitation investigations are approached with caution. They are hard to detect and justify. Competition authorities may interrupt competitive practices creating false positives and discouraging investment and innovation.

On the other side, consumers do not have a consistent attitude towards privacy. While privacy sensitivity differs according to individuals, individuals themselves may reveal divergent attitudes according to varying types of data, environments, incentives or costs. Yet, many consumers are willing to share data in return of zero-price services. Additional to these factors, taking into account the benefits of data accumulation like in increasing quality, facilitating

innovative products, assumption of all consumers are privacy sensitive in competition enforcement, may in fact be detrimental to the consumer welfare.

In conclusion, the study acknowledges both legal regimes have some theoretical intersections without dispute. Moreover, data protection law may definitely be utilised in competition assessments, as is the case with other laws. Data of course would be addressed as an asset and accordingly foreclosure affects would be scrutinised where relevant. Data protection/privacy may encounter a competition parameter though currently it is still emerging.

Nevertheless, competition law should not be used as a vehicle just for populist concerns. From the studies it is pertinent to conclude that the privacy awareness is still evolving. Data protection laws are just updated for the newly developed technologies and authorities are strengthened with more deterrent sanctions. The next step would be to raise awareness among the individuals to facilitate awareness.

The study does not aim to take a blind eye towards new developments. Indeed, it appreciates potential damages of data accumulation/privacy intrusion as well as their benefits. However, it aims to devote the same caution for established standards over years' experience. When comparing both, taking also into account there is no clear study that measures their balance, the study chooses a cautionary approach.

Competition law cannot decide which products/services are better or worse for consumers. Similarly it should not decide if privacy is desirable or if services provided in return for private data are harmful for consumers. As a result, competition law intervention against data protection issues should always be based on a strong link to competition or competitive process.

BIBLIOGRAPHY

'About' (*European Data Protection Supervisor*, 11 November 2016) <https://edps.europa.eu/about-edps_en> accessed 7 July 2019

Alemanno A, 'Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many' (2018) 9 European Journal of Risk Regulation 183

Altmayer OA, 'The Tipping Point - Reevaluating The Asnef-Equifax Separation of Competition of Data Privacy Law in The Wake of The 2017 Equifax Data Breach' (2018) 39 International Law 37

Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 0829/14/EN WP216 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 2 March 2019

Athey S, Catalini C and Tucker C, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' [2017] NBER Working Paper Series 34

Bakhoum M, 'Reflections on the Concepts of "Economic Freedom", "Free Competition" and "Efficiency" from the Perspective of Developing Countries' in Daniel Zimmer, *The Goals of Competition Law* (Edward Elgar Publishing 2012)

'Big Data: Bringing Competition Policy to the Digital Era-OECD' <http://www.oecd.org/daf/competition/big-data-bringing-competition-policy-to-the-digital-era.htm> accessed 12 March 2019

Bornico L and Walden I, 'Ensuring Competition in the Clouds: The Role of Competition Law?' (2011) 12 ERA Forum 265 <http://link.springer.com/10.1007/s12027-011-0223-y> accessed 30 July 2019

Botta M and Wiedemann K, 'EU Competition Law Enforcement Vis-à-Vis Exploitative Conducts in the Data Economy' [2018] Max Planck Institute for Innovation and Competition Research Paper Series 90

'Bundeskartellamt-Homepage-Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources' <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 25 July 2019

Bygrave LA, *Data Privacy Law* (1st edn, OUP 2014)

Chalmers D, Davies G and Monti G, *European Union Law: Cases and Materials* (2nd edn, Cambridge University Press 2010)

Chazan G, 'Altmaier Urges EU to Protect Technology from Chinese Rivals' (*Financial Times*, 17 February 2019) <https://www.ft.com/content/6757ca9a-3048-11e9-8744-e7016697f225> accessed 16 March 2019

Chazan G, 'Germany Backs French Call for Right to Overturn EU Merger Decisions' (*Financial Times*, 19 February 2019) <https://www.ft.com/content/66c932d8-344b-11e9-bb0c-42459962a812> accessed 17 March 2019

Chazan G and Murgia M, ‘Germany Orders Facebook to Stop Collecting WhatsApp Data’ (*Financial Times*, 27 September 2016) <https://www.ft.com/content/f6db8738-8497-11e6-8897-2359a58ac7a5> accessed 24 July 2019

Chirita AD, ‘The Rise of Big Data and the Loss of Privacy’ in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Berlin Heidelberg 2018) <http://link.springer.com/10.1007/978-3-662-57646-5_6> accessed 19 June 2019

Coates K, *Competition Law and Regulation of Technology Markets* (1st edn, OUP 2011)

Colangelo G and Maggiolino M, ‘Data Accumulation and the Privacy–Antitrust Interface: Insights from the Facebook Case’ (2018) 8 International Data Privacy Law 224 <https://academic.oup.com/idpl/article/8/3/224/5198967> accessed 25 July 2019

‘Competition Law and Data’ (Autorité de la concurrence and Bundeskartellamt 2016) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big%20Data%20Papier.html> accessed 27 July 2019

Costa-Cabral F, ‘The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law’ (2016) 23 Maastricht Journal of European and Comparative Law 495 <http://journals.sagepub.com/doi/10.1177/1023263X1602300307> accessed 21 July 2019

Costa-Cabral F and Lynskey O, ‘Family Ties:The Intersection Between Data Protection and Competition in EU Law’ [2017] Common Market Law Review 11

‘Council of Europe Data Protection’ <https://www.coe.int/en/web/data-protection/home> accessed 21 June 2019

Dabbah MM, *EC and UK Competition Law: Commentary, Cases and Materials* (1st edn, Cambridge University Press 2004)

Davilla M, ‘Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules’ (2017) 8 Journal of European Competition Law & Practice 370

De Peyer BH, ‘EU Merger Control and Big Data’ (2017) 13 Journal of Competition Law & Economics 767 <https://academic.oup.com/jcle/article/13/4/767/4802444> accessed 20 July 2019

Di Porto F, ‘In Praise of an Empowerment Disclosure Regulatory Approach to Algorithms’ (2018) 49 IIC-International Review of Intellectual Property and Competition Law 507 <http://link.springer.com/10.1007/s40319-018-0708-0> accessed 17 July 2019

Duhigg C, ‘How Companies Learn Your Secrets’ *The New York Times* (16 February 2012) <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> accessed 15 August 2019

Dyer G and McGregor R, ‘Spying: Too Much Information’ (*Financial Times*, 1 November 2013) <https://www.ft.com/content/ce0cd70e-42e5-11e3-8350-00144feabdc0> accessed 12 July 2019

EDPS, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 22 July 2019

Eleanor Fox, 'Imagine: Pro-Poor(Er) Competition Law' (OECD 2013) DAF/COMP/GF(2013)12 <https://www.oecd.org/daf/competition/competition-and-poverty-reduction2013.pdf> accessed 18 March 2019

Engels B, 'Data Portability among Online Platforms' (2016) 5 Internet Policy Review 17 <http://policyreview.info/node/408> accessed 22 June 2019

'EU General Data Protection Regulation-Key Changes' (*DLA Piper Global Law Firm*) <https://www.dlapiper.com/en/europe/focus/eu-data-protection-regulation/key-changes/> accessed 21 June 2019

'European Commission-Press Release-Speech-Competition and Personal Data Protection, Commissioner Joaquín Almunia' <https://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> accessed 17 August 2019

Evans DS and Padilla AJ, 'Excessive Prices: Using Economics to Define Administrable Legal Rules' (2005) 1 Journal of Competition Law & Economics 97 <http://academic.oup.com/jcle/article/1/1/97/848949/Excessive-Prices-Using-Economics-to-Define> accessed 17 August 2019

Ezrachi A and Stucke ME, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (1st edn, Harvard University Press 2016)

Fildes N and Politi J, 'WhatsApp Fined €3m over Facebook Data Sharing in Italy' (*Financial Times*, 12 May 2017) <https://www.ft.com/content/2fdb5f34-3728-11e7-bce4-9023f8c0fd2e> accessed 24 July 2019

'French Competition Authority Fines ENGIE €100 Million for Abusing Its Dominant Position on the French Retail Gas Supply Market' (*Van Bael & Bellis*) <https://www.vbb.com/insights/competition/abuse-of-dominance/french-competition-authority-fines-engie-100-million-for-abusing-its-dominant-position-on-the-french-retail-gas-supply-market> accessed 27 July 2019

Fuller CS, 'Privacy Law as Price Control' (2018) 45 European Journal of Law and Economics 225 <http://link.springer.com/10.1007/s10657-017-9563-6> accessed 3 August 2019

Geradin D and Kuschewsky M, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2216088> accessed 22 July 2019

Gerber D, *Global Competition: Law, Markets, and Globalization* (Oxford University Press 2010)

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

Graef I, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Berlin Heidelberg 2018) <http://link.springer.com/10.1007/978-3-662-57646-5_6> accessed 19 June 2019

'Handbook on European Data Protection Law' (*European Union Agency for Fundamental Rights*, 16 May 2018) <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> accessed 20 June 2019

Höppner DT, 'Data Exploiting as an Abuse of Dominance: The German Facebook Decision | Lexology' (4 March 2019) <https://www.lexology.com/library/detail.aspx?g=242876ec-4401-4771-80ce-480623c6423e> accessed 2 August 2019

Kathuria V, 'Greed for Data and Exclusionary Conduct in Data-Driven Markets' (2019) 35 Computer Law & Security Review 89 <https://linkinghub.elsevier.com/retrieve/pii/S0267364918303820> accessed 25 July 2019

Kerber W, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11 Journal of Intellectual Property Law & Practice 856

Kuner C and others, 'When Two Worlds Collide: The Interface between Competition Law and Data Protection' (2014) 4 International Data Privacy Law 247

Lucchini S and others, 'Online Digital Services And Competition Law: Why Competition Authorities Should Be More Concerned About Portability Rather than About Privacy' (2018) 9 Journal of European Competition Law & Practice 563 <https://academic.oup.com/jeclap/article/9/9/563/5067527> accessed 4 August 2019

Marini-Balestra DrF and Tremolada DrR, 'Digital Markets and Merger Control: Balancing Big Data and Privacy against Competition Law - a Comment on the European Commission's Decision in the Microsoft/LinkedIn Merger' [2017] European Competition Law Review 337

'Mergers: Commission Prohibits Siemens' Proposed Acquisition of Alstom' (*EC-Press Release Database*, 6 February 2019) <http://europa.eu/rapid/press-release_IP-19-881_en.htm> accessed 17 March 2019

Moorcroft V and Strat AL, 'The Rise of Big Data: The Intersection between Competition Law and Customer Data' [2018] The Licensing Journal 8

Motta M and de Streel A, *The Pros and Cons of High Prices*, vol 6 (Swedish Competition Authority 2007)

'OECD-Guidelines' <https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en> accessed 21 June 2019

Porter J, 'EU Opens Amazon Antitrust Investigation' (*The Verge*, 17 July 2019) <https://www.theverge.com/2019/7/17/20696214/amazon-european-union-antitrust-investigation-third-party-seller-marketplace> accessed 23 July 2019

Riziotis D, *Abuse of Dominant Position: New Interpretation, New Enforcement Mechanisms?*, vol 5 (Mark-Oliver Mackenrodt, Beatriz Conde Gallego and Stefan Enchelmaier eds, Springer Science & Business Media 2008)

Stevens G, 'The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices Authority' [2014] Congressional Research Service 15

'The Five Most Important Events of 2013' (*Financial Times*, 29 December 2013) <https://www.ft.com/content/d6449a2a-5dcd-3e5a-ae14-0de7a10f9089> accessed 12 July 2019

'Understanding Key Changes from the Data Protection Directive to GDPR | Synopsys' (*Software Integrity Blog*, 18 January 2018) <https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/> accessed 21 June 2019

Van Den Hoven J and others, 'Privacy and Information Technology' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Summer 2018, Metaphysics Research Lab, Stanford University 2018) <https://plato.stanford.edu/archives/sum2018/entries/it-privacy/> accessed 16 August 2019

Wahyuningtyas SY, 'Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market' (2017) 18 European Business Organization Law Review 785 <http://link.springer.com/10.1007/s40804-017-0084-0> accessed 23 July 2019

Waked DI, 'Antitrust Goals in Developing Countries: Policy Alternatives and Normative Choices' (2015) 38 Seattle University Law Review 945

Whish R, *Competition Law* (5th edn, OUP 2005)

Whish R and Bailey D, *Competition Law* (9th edn, OUP 2018)

'Why Do We Need the Charter?' (*European Commission*) <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en> accessed 20 June 2019

Yaros O and others, 'European Union:GDPR Fines Lessons From Competition Law' *Mondaq Business Briefing* (12 December 2018)

Zanfir G, 'The Right to Data Portability in the Context of the EU Data Protection Reform' (2012) 2 International Data Privacy Law 149 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ips009> accessed 22 June 2019

Zanfir-Fortuna G and Ianc S, 'Data Protection and Competition Law: The Dawn of "Uberprotection"' [2018] SSRN Electronic Journal 1 <https://www.ssrn.com/abstract=3290824> accessed 20 July 2019

Zimmer D (ed), *The Goals of Competition Law* (Edward Elgar Publishing 2012)

TABLE of CASES

The European Court of Human Rights

Amann v Switzerland (2000) ECHR No.27798/95

Rotaru v Romania (2000) ECHR No.28341/95

The European Court of Justice

27/6, United Brands Company v. Commission [1976] ECLI:EU:C:1978:22

C-85/76 Hoffmann-La Roche & Co. AG v. Commission, [1979] ECR 461

C-322/81 Michelin v Commission [1983] ECR 3461

226/84 British Leyland v Commission [1986] ECR 3263

C-241/91 and C-242/91 Telefis Eireann and Independent Television Publications Ltd v Commission of the European Communities (Magill) [1995] ECLI:EU:C:1995:98

C-418/01 IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG [2004] ECLI:EU:C:2004:257

C-238/05 Asnef-Equifax et al v Asociación de Usuarios de Servicios Bancarios [2006] ECR I-11166

C-238/05 Asnef-Equifax et al v Asociación de Usuarios de Servicios Bancarios [2006] ECR I-11166, Opinion of AG Geelhoed

C-385/07 P Der Grüne Punkt–Duales System Deutschland v Commission [2009]

C-280/08 Deutsche Telekom AG v Commission [2010] ECR I-9555

C-32/11 Allianz Hungária Biztosító and Others [2013] OJ C141/3.

C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] ECLI:EU:C:2014:238

C-525/16, MEO–Serviços de Comunicações e Multimédia SA v. Autoridade da Concorrência [2018] ECLI:EU:C:2018:270

The General Court

T-51/89 Tetra Pak v Commission [1990] ECR II-309

T-201/04 Microsoft [2007] ECLI:EU:T:2007:289.

T-321/05, AstraZeneca v. Commission, 2010 E.C.R. II-2830

The European Commission

Deutsche Post AG (Case COMP/C-1/36.915) [2001] OJ L331/40

Microsoft (Case COMP/C-3/37.792) [2004] OJ L32/23.

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

TomTom/Tele Atlas (Case COMP/M.4854) [2008] OJ C237/8

Thomson/Reuters (Case COMP/4726) Commission Decision C(2008) 654 [2008]

Microsoft/Yahoo! Search Business, (Case COMP/M.5727) [2010]

Telefónica UK/Vodafone UK/Everything Everywhere/JV (COMP/M.6314) [2012] OJ C66/5

Universal Music Group/EMI Music (Case COMP/M.6458) [2012] OJ C220/15

Facebook/WhatsApp (Case COMP/M.7217) [2014] OJ C297/13

Verizon/Yahoo (Case COMP/M.8180) [2016]

Microsoft/LinkedIn (Case M.8124) Commission Decision C(2016) 8404 [2016]

Google Android Commission Decision AT.40099 [2018]

Other Jurisdictions

Dissenting Statement of Commissioner Pamela Jones Harbour in the matter of Google/DoubleClick FTC File No.071-0170 (Federal Trade Commission)

Google v Vidal-Hall [2015] EWCA Civ 311 (Court of Appeal, the United Kingdom)