DOCTOR OF LEGAL STUDIES

Imposing data sharing among private actors: a tale of evolving balances

Tombal, Thomas

Award date:
2021

Awarding institution:
University of Namur

Academic year 2020-2021

IMPOSING DATA SHARING AMONG PRIVATE ACTORS

A TALE OF EVOLVING BALANCES

Thesis presented in view of obtaining
the title of doctor of law
at the University of Namur
by Thomas TOMBAL
Namur, 7 September 2021

Members of the Jury:

Prof. Cécile de Terwangne (UNamur), Promoter
Prof. Alexandre de Streel (UNamur), Co-Promoter
Prof. Marc Nihoul (UNamur), President
Prof. Benoît Michaux (UNamur)
Prof. Giorgio Monti (Tilburg University)
Prof. Dr. Heike Schweitzer (Humboldt-Universität zu Berlin)

Acknowledgments

As the journey of my doctoral research is coming to an end, I would like to take a moment to thank all the people that have either helped or supported me in my endeavours. While the PhD process might sometimes be described as a solitary adventure, the truth is that without the help of all of these formidable people, the road would have been much more complicated. As so many of them have, each in their own way, helped me to carry this project over the line, I apologize in advance for anyone that I might have forgotten.

Firstly, I would like to thank all the people that directly assisted me in improving this manuscript.

In this regard, I would like to thank Prof. Dr. Heike Schweitzer and Prof. Dr. Giorgio Monti for giving me the honour of accepting to be part of my jury and for taking the time to read my work. Your fresh look on the manuscript and the insightful remarks that you have provided to me have pushed me to challenge myself and to go the extra-mile, in order to improve my text. The same goes for Prof. Dr. Benoît Michaux, whose role has evolved during the process of the research, but who has always been supportive and available when I needed his enlightened opinion, which also contributed to the enrichment of my findings.

I would also like to thank my two promoters, Prof. Dr. Cécile de Terwangne and Prof. Dr. Alexandre de Streel, as the lively and enriching exchanges that we have had during the whole doctoral process have shaped the final result of my research, which you undeniably contributed to improve, as you never stopped pushing me to refine my text. I would also like to thank you for all the precious professional and personal advices that you have provided to me over the years.

More generally, I would like to thank Prof. Dr. Séverine Dusollier, Prof. Dr. Michal Gal, Prof. Dr. Reto Hilty, Prof. Dr. Ioannis Lianos, Prof Dr. Yves Poullet, Dr. Inge Graef, Bertin Martens, Nestor Duch-Brown; Dr. Luc Desaunettes, Dr. Heiko Richter and the other people I met at the Max Planck Institute for Innovation and Competition in Munich; and all the other people that I have had the pleasure to exchange opinions with about my doctoral research, and whose advise has helped me to better shape my ideas.

Secondly, I would like to thank all of the people that I have had the chance to collaborate with during the last five years, as the pleasure of working with them has given me the motivation to push forward and to reach my goals.

In this regard, I would like to thank Prof. Dr. Marc Nihoul and Prof. Dr. Hervé Jacquemin for all the support that they have provided to me in their respective roles, which enabled me to complete my doctoral journey with serenity. Your availability to answer all the questions I had has been precious.

I would also like to thank my partners on the FLEXPUB and DIGI4FED research projects, which were conducted in parallel to this doctoral research, for the fascinating interdisciplinary exchanges that we have had.

I thank my colleagues and friends from the Law Faculty of the University of Namur and from the CRIDS, for their camaraderie and the countless laughs and good moments that we have shared, and which allowed me to enjoy writing this thesis in a convivial environment.

I also thank the support staff of the Faculty and of the CRIDS, whose assistance has not only been vital for the different steps of this thesis, but also in my daily life as a researcher.

Third, I would like to thank my family and my friends for providing me with the love and affection that I needed to see the finish line.

In particular, I would like to thank my sister, Marie, and my brother, Martin, for always being there for me when I needed them. I am truly blessed that you are not only my siblings, but also two friends for life.

I would also like to thank my parents, Anne and Bertrand, for their unconditional support and for all of the sacrifices that you have made, each in your own way, in order to give us the best life possible. I know that we are not the most expressive people when it comes to sharing our feelings, but you have always made me feel loved and protected. I can never thank you enough for that.

Last but not least, I would like to thank my partner in life and my best friend, Cecilia. Without this doctoral research I wouldn't have met you, and without you I would have struggled a lot more to finalise this thesis. You calm me down when I am stressed, you cheer me up when I'm down, you give me faith when I doubt myself and you always push me to do more and to get out of my comfort zone. In short, you make me a better man, and having you in my life makes me the luckiest men on earth.

Table of contents

Introduction

1. Data is often presented as the new oil of our modern economy. It is the fuel of information and knowledge creation in an increasingly connected world. In the context of this doctoral thesis, "data" is defined in a broad sense, on the basis of the definitions provided in the European Commission's proposals for a Data Governance Act and for a Digital Markets Act, and means "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording".[1]

The European economy runs on data, which has become an essential resource for economic growth, job creation and societal progress[2], and the value of the data market is expected to reach between 432 and 827 billion euros by 2025.[3] Such numbers do not come as a surprise, given that the amount of data generated increases exponentially. Indeed, our increased reliance on electronic networks generates troves of data, as every action taken on these networks leaves "footprints" in the shape of data. This growth will not slow down any time soon, as the emergence of the "Internet of Things" (*IoT*)[4] will contribute to the increase of this phenomenon. One might simply think of data that is (or will be) generated by smart cars, smart houses, smart farming, etc.

While the economic value deriving from the processing of these data seems obvious, determining the legal framework to be applied to it is, on the contrary, a complex task. This stems from the fact that data is a complex good, towards which many natural or legal persons can potentially claim a right or interest. For instance, the data generated by an autonomous vehicle is relevant for multiple categories of stakeholders, such as vehicle manufacturers, car dealers, spare parts manufacturers, authorised and independent garages and repairers, developers of infotainment software used in vehicles, vehicle users, and possibly also public authorities for the optimisation of road traffic management. This example illustrates the inherent complexity of this resource, which will often be at the crossroads of multiple claims and rights aimed at controlling, accessing, or benefiting from the data processing.

2. This highlights the need for a clear legal framework, especially as the data markets are still emerging.[5] Moreover, the lack of a clear legal environment may contribute to insufficient data

---

[1] Article 2.1 of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final; Article 2.19 of the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Building a European Data Economy*", Brussels, 10 January 2017, COM(2017) 9 final, p. 2.

[3] International Data Corporation and the Lisbon Council, "The European Data Market Study Monitoring Tool – Final Study Report", June 2020, SMART 2016/0063, available at http://datalandscape.eu/, p. 9.

[4] "The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data" (https://en.wikipedia.org/wiki/Internet_of_things).

[5] M. Barbero, D. Cocoru, H. Graux, A. Hillebrand, F. Linz, D. Osimo, A. Siede and P. Wauters, "Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability", 25 April

sharing, possibly stifling innovation and creating entry barriers for new market entrants[6], and possibly impairing access to information or our societies' ability to tackle environmental, health or mobility challenges.[7] In the context of this thesis, "data sharing" is defined in a broad sense, on the basis of the definition provided in the European Commission's proposal for a Data Governance Act.[8] Namely, it is the act through which one or several data holder(s)[9] provide(s) access to its(their) data to one or several data recipient(s), directly or through an intermediary, for the purpose of joint or individual use of the shared data, on the basis of voluntary agreements or of compulsory rules.

3. It should be outlined from the outset that the legal framework pertaining to (compulsory) data sharing is clearer when it comes to the sharing of data between governments and businesses ("G2B data sharing"). Indeed, in 2003, the European legislator adopted the Public Sector Information (PSI) Directive, which invited public sector bodies to open their public sector information for re-use.[10] However, given that the public sector bodies had the choice, rather than the obligation, to open their data, only few of them did so. To remedy that weakness, the PSI Directive was amended in 2013 to force public sector bodies to make their public sector information re-usable for commercial or non-commercial purposes, for free or with charges limited to the marginal costs incurred for their reproduction, provision and dissemination.[11] More recently, in June 2019, the European legislator adopted a recast version of the PSI Directive, which will have to be transposed in all Member States by July 2021.[12] This recast brings substantial modifications, which will be outlined further.[13] Finally, in November 2020, the European Commission also proposed a Data Governance Act, which notably aims at laying down the conditions for the re-use of certain categories of data held by

---

2018, available at https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and, p. 31.

[6] Communication from Commission, "*Building a European Data Economy*", *op. cit*., p. 3.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", 19 February 2020, COM(2020) 66, p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *Study on Behalf of the European Consumer Organisation (BEUC)*, 2019, available at https://www.beuc.eu/publications/beuc-x-2018_121_data_access_and_control_in_the_area_of_connected_devices.pdf, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *IIC*, 2020, Volume 51, Issue 8, p. 942.

[8] "Data sharing means the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary" (Article 2.7 of the Proposal for a Data Governance Act).

[9] The more generic term of "data holder" is used in the context of this thesis, rather than "data owner", as the issue of data "ownership" is widely debated (see Part I, Chapter 2, Section B, b)). For a proposed definition of a "data holder", see Article 2.5 of the Proposal for a Data Governance Act: "a legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control".

[10] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ L 345/90*, 31 December 2003.

[11] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, *OJ L 175/1*, 27 June 2013, Articles 3.1 and 6.1.

[12] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019.

[13] See Part III, Chapter 3, Section B, a), 1.

public sector bodies.[14] This string of legislations is motivated by the fact that public sector data are highly valuable resources that can be used to foster accountability and transparency, and to foster the European economy by generating digital innovation and preventing the distortion of competition in the internal market.[15]

4. Contrary to G2B data sharing, the field of (compulsory) business-to-business data sharing ("B2B data sharing") is still in the early phases of its construction. In the context of this thesis, the term "business" should be understood broadly, and is not limited to undertakings pursuing profit. It also covers, for instance, data sharing with non-profits pursuing societal goals.[16] Rather, it should be understood as being distinct from business-to-government (B2G) data sharing.[17] In this regard, B2B data sharing can pursue economic goals but also societal and "empowerment" goals.[18]

As underlined by the European Commission, "data sharing between companies has not taken off at sufficient scale. This is due to a lack of economic incentives (including the fear of losing a competitive edge), lack of trust between economic operators that the data will be used in line with contractual agreements, imbalances in negotiating power, the fear of misappropriation of the data by third parties, and a lack of legal clarity on who can do what with the data".[19] These factors can lead to market failures, such as the lack of incentives to collect data, uncertainties in terms of risks, high transaction costs for sharing and missing markets, and asymmetries of information distorting decision-making.[20]

One way to address these market failures is through the adoption of legal instruments promoting *voluntary* data sharing, which will tend to focus more on data governance and technical issues (standardisation, interoperability[21], etc.), in order to create more favourable

---

[14] Articles 1.1.a) and 3 to 8 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final.

[15] See Recitals, 3, 7, and 11 of the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019.

[16] On these societal goals, see Part I, Chapter 2, Section C, a).

[17] This thesis will therefore not focus on the data sharing obligations that are imposed on businesses to the benefit of the public sector (e.g. banks are compelled to share financial information with public authorities in the context of the fight against money laundering). See however Part III, Chapter 3, Section B, a), 2.

[18] See Part I, Chapter 2, Section B, c) and Section C.

[19] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 7.

[20] See point 78. For a broader analysis of all of the potential types of data market failures, see M. Stucke and A. Grunes, *Big Data and Competition Policy*, Oxford, Oxford University Press, 2016; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability: case studies and data access remedies", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era – Final report*"*, 2019, available at http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing: an economic and legal analysis", *EU Science Hub*, 2020, available at https://ssrn.com/abstract=3658100; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *CERRE Report*, March 2019, available at http://www.crid.be/pdf/public/8377.pdf; B. Martens, "An economic perspective on data and platform market power", *JRC Digital Economy Working Paper 2020-09*, February 2021, available at https://www.researchgate.net/publication/349179464.

[21] Interoperability is defined as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the

conditions for the market actors to remedy, or at least reduce, these market failures themselves.[22] For instance, the European Commission has adopted a Communication "Towards a common European data space", containing key principles for *voluntary* B2B data sharing.[23] It has also created a "Support Centre for Data Sharing"[24], with the aim of putting in place a series of measures facilitating (voluntary) data sharing, in particular by providing examples of good practice, standard contractual clauses or existing contract models.[25] More recently, it has adopted a proposal for a Data Governance Act that notably aims at promoting *voluntary* data sharing services by intermediaries[26], as well as *voluntary* data sharing in the common good ("data altruism").[27] The underlying idea behind all these instruments is that, in light of the proportionality principle[28], it is preferable to first attempt to create a clear framework to incentivise the market actors to share data on their own initiative, rather than to compel them to do so. In this perspective, the European Commission seems to repeat the approach that it adopted for G2B data sharing, as the PSI Directive did not contain any *compulsory* G2B data sharing obligation either in its first version of 2003.[29]

Yet, such *voluntary* data sharing initiatives may not always be sufficient to address the above-mentioned issues, and legislators could be tempted to go a step further, by imposing *compulsory* business-to-business ("B2B") data sharing in some "specific circumstances".[30] These specific circumstances can either be economic or societal.[31] For example, they might be justified if, as it is currently the case, a small number of large firms hold a significant part of the world's data, as this might diminish the incentives of smaller data-driven firms to emerge,

---

organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems" (Decision 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector, *OJ L 318/1*, 4 December 2015, article 2.1).

[22] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 28. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability: Towards a Governance Framework*", CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/.

[23] See point 64. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Towards a common European data space*", Brussels, 25 April 2018, COM(2018) 232 final, p. 10. See also Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication "*Towards a common European data space*", Brussels, 25 April 2018, SWD(2018) 125 final.

[24] See https://eudatasharing.eu/homepage

[25] See point 65. Commission Staff Working Document establishing a guidance on sharing private sector data, *op. cit.*, p. 6.

[26] See point 78. See Articles 9 to 14 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*, p. 11-12.

[27] See point 93. See Articles 15 to 22 of the Proposal for a Data Governance Act.

[28] Article 5.4 of the Treaty on European Union, *OJ C 326/13*, 26 October 2012; Protocol (No 2) on the application of the principles of subsidiarity and proportionality, *OJ C 326/206*, 26 October 2012

[29] See points 3 and 385.

[30] See, *inter alia*, M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*

[31] See *infra* Part I, Chapter 2, Section B, c) and Section C.

grow and innovate, due to high entry barriers.[32] The high degree of market power deriving from this "data advantage" could also affect the contestability of some markets.[33] Moreover, some platforms have acquired significant scale, effectively allowing them to act as "private gatekeepers", and *compulsory* B2B data sharing is being discussed as a potential remedy to ensure that their systemic role will not endanger the fairness and openness of the markets.[34] On the other hand, this data concentration phenomenon[35] could also possibly impair access to information and our societies' ability to tackle environmental, health or mobility challenges.[36] In this regard, the European Commission has suggested that it would explore legislative options in order to promote a wider (compulsory) sharing and availability of data, in order to ensure "contestability, fairness and innovation and the possibility of market entry, as well as public interests that go beyond competition or economic considerations".[37]

It must nevertheless be outlined here that *voluntary* and *compulsory* data sharing should not be seen as two extremes on the regulatory intervention scale. Rather, there are links to be made between these two approaches, which complement each other. Indeed, if the step has to be taken from *voluntary* to *compulsory* data sharing regulatory initiatives, the latter should not reinvent the wheel and should build on the former. Indeed, the data governance principles and the technical provisions contained in *voluntary* initiatives are equally relevant for, and should support, these *compulsory* initiatives. For instance, the key principles for *voluntary* B2B data sharing contained in the Communication "Towards a common European data space" could be integrated, in the future, in *compulsory* B2B data sharing instruments. Moreover, the national authorities that the European Commission's proposal for a Data Governance Act suggests to appoint, in order to supervise *voluntary* B2B data sharing with trusted data intermediaries, could also be appointed as the regulatory authorities for (some) *compulsory* data sharing regulatory initiatives.[38] This is because these national authorities will arguably have expertise with the governance, pricing and technical mechanisms used for *voluntary* data sharing, which are, in essence, the same as those that could be used for *compulsory* data sharing. Furthermore, the work made by the "Support Centre for Data Sharing", mentioned above, and the European Data Innovation Board – which is a formal expert group that should support the European Commission's work on technical standardisation and interoperability to facilitate

[32] See Part I, Chapter 2, Section B, c), 3. Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 3.
[33] *Ibid*., p. 8.
[34] Communication from the Commission, "*Shaping Europe's digital future*", *op. cit*., p. 8.
[35] See Part I, Chapter 2, Section B, c), 3.
[36] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 942.
[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Shaping Europe's digital future*", Brussels, 19 February 2020, COM(2020) 67, p. 9; Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 5 and 14.
[38] See points 219 and 416. See Recitals 22 to 34 and Articles 13 and 23 to 25 of the Proposal for a Data Governance Act.

voluntary data sharing –[39], would also be a precious resource for *compulsory* data sharing initiatives.

5. Despite this complementarity, the choice has been made, in this thesis, to focus on *compulsory* B2B data sharing regulatory initiatives, because if the legislator decides to take this step forward in the degree of its intervention, this will require the prior consideration of a certain number of fundamental economic and societal balancing exercises. The focus of this thesis will be to highlight the nature of these balancing exercises and to provide insights on how they could potentially be addressed. This doctoral thesis will thus be structured around the following research question: "***What are the economic and societal balancing exercises underlying compulsory B2B data sharing?***".

More concretely, and without entering into too much detail at this stage, this thesis will focus on three balancing exercises, namely the need to balance the benefits stemming from compulsory B2B data sharing initiatives with: i) the economic interests of the data holder;[40] ii) personal data protection considerations;[41] and the long-term and collective costs that (some of) these initiatives could entail in terms of individual autonomy.[42] This focus can be explained by the evolution of the doctoral research, which has paralleled the evolution of the policy discussions on compulsory B2B data sharing since 2016, which marked the beginning of the research.

Indeed, while the focus of the research and of these policy discussions was originally set on whether it would be relevant to create an IP-like "data producer's right"[43], both have shifted away from developments pertaining to "property" on data, towards legal reflections revolving around notions of data "control" and "access".[44] However, as will be outlined throughout the thesis, what has remained constant in the policy discussions is the large emphasis on the need to ensure that these initiatives do not excessively distort the economic interests of the data holders, whether in the context of competition law remedies or of *ex ante* legislations imposing data sharing, as their incentives to collect and process data must be preserved. Accordingly, the first ambition of this thesis was to adopt an analytical approach, in order to shed more light on how these economic interests of the data holders are factored in the existing compulsory B2B data sharing initiatives, and to provide some insights on how these interests could be factored in future initiatives.

---

[39] See point 309. See Recitals 40 and 41 and Articles 26 and 27 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit*., p. 54.
[40] See, inter alia, Part I, Chapter 2, Section B, c), 5; Part II, Chapter 2, Section A, a); Part II, Chapter 2, Section C; Part III, Chapter 1; Part III, Chapter 3, Section B; and Part III, Chapter 4, Section A.
[41] See, inter alia, Part II, Chapter 2, Section A, b); Part II, Chapter 2, Section C; Part III, Chapter 2; Part III, Chapter 3, Section B; and Part III, Chapter 4, Section A.
[42] See, inter alia, Part I, Chapter 2, Section C, b); and Part II, Chapter 2, Section A, c).
[43] See Part I, Chapter 2, Section B, b), 2.
[44] See Part I, Chapter 2, Section B, b), 3.

Then, it quickly became apparent that, as many of the data that would be shared in the context of these initiatives could be deemed as being personal data[45], it is essential for these compulsory B2B data sharing initiatives to factor personal data protection considerations. However, as the research progressed, it became striking that while legislators and policy makers seem to be aware of the necessity to consider this issue, they usually simply indicate that "where data qualifies as personal data, the data protection framework, in particular the [General Data Protection Regulation (GDPR)[46]], will apply"[47], without providing detailed indications on how this could be articulated in practice. Accordingly, the second ambition of this thesis was to adopt a normative approach in order to fill this gap, by attempting to clarify the core elements that must be factored in this balancing exercise, and by attempting to provide insights on how this delicate articulation can be solved.

Finally, as will be outlined below[48], the doctoral research led to the observation that, up to now, the European legislator seemed to favour (some forms of) data portability models when adopting compulsory B2B data sharing initiatives. Yet, it is worrying to observe that while legislators and policy makers heavily focus on the positive aspects of these types of initiatives, they seem to completely overlook the long-term and collective costs that they could entail in terms of personal autonomy and informational self-determination. Accordingly, the third ambition of this thesis was, once again, to adopt a normative approach in order to fill this gap, by attempting to raise awareness about the crucial need to take these risks into consideration, and by attempting to provide insights on how this delicate balance between short-term individual benefits, on the one hand, and long-term and collective risks, on the other hand, can be addressed.

6. In order to answer the above-mentioned research question, it is first necessary to explain the fundaments of (data) sharing, which will be the aim of **Part I of this thesis**. To do so, the concept of *data* (What?) will first be specified and **Chapter 1** will suggest a data typology. Then, the rationale for (data) sharing (Why?) will be analysed. In this regard, **Chapter 2** will first revert to the more standard discussions on whether a resource should be shared. Then, it will be questioned whether the findings made in the realm of (in)tangible resources can be translated to the realm of data. It will be outlined that the rationale for data sharing can be economic, societal or based on "empowerment" considerations. **Chapter 3** will then present a typology of data sharing models and initiatives (How?). To this end, this chapter will first take

---

[45] "Any information relating to an identified or identifiable natural person (data subject)" (Article 4.1 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4 May 2016).

[46] *Ibidem*.

[47] Communication from Commission, "*Building a European Data Economy*", *op. cit*., p. 9. See also Recital 28 of the Proposal for a Digital Governance Act: "This Regulation should be without prejudice to the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation. Where the data sharing service providers are data controllers or processors in the sense of Regulation (EU) 2016/679 they are bound by the rules of that Regulation"; and Article 7.1 of the proposal for a Digital Markets Act: "The gatekeeper shall ensure that these measures are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety".

[48] See Part I, Chapter 3, Section A, c) and Part II.

a more practical approach, and will present the most common *conceptual models of data sharing*. Then, it will take a more abstract approach, by focussing on the underlying objectives pursued by *compulsory B2B data sharing initiatives*. Indeed, it would be ill-advised to consider *compulsory* data sharing as a goal in itself.[49] Rather, it should only be used as a mean to achieve determined objectives. In this regard, while the debates at the European level usually crystallise around economic objectives (contestability of data markets, social welfare deriving from data sharing and re-use…), societal objectives could also be pursued through the imposition of compulsory B2B data sharing (tackling environmental challenges, contributing to healthier and more sustainable societies, improving mobility…).[50] Moreover, compulsory B2B data sharing can also be used as a mean to empower individuals[51], as illustrated by the personal data portability right granted by Article 20 of the GDPR.[52] Considering these distinct objectives will lead to the identification of two main categories of compulsory B2B data sharing initiatives, which will guide the rest of the analysis in the thesis. These are ***"empowerment" initiatives imposing B2B data sharing***, on the one hand, and ***economic or societal initiatives imposing B2B data sharing***, on the other hand. Importantly, it must be clarified from the outset that while these two main categories of compulsory B2B data sharing initiatives pursue different objectives, synergies can be found between these two types of initiatives, which explains why they are both addressed in this thesis.[53]

7. Part II of the thesis will be devoted **to *"empowerment" initiatives imposing B2B data sharing*. Chapter 1** will first present the main data sharing initiatives aiming at empowering individuals, which are essentially structured around (some forms of) data portability rights.[54] In this regard, it will be outlined that these empowerment initiatives can pursue two different types of sub-objectives. On the one hand, empowerment initiatives can pursue the objective of allowing the exercise of fundamental rights, such as the right to personal data protection and informational self-determination.[55] On the other hand, empowerment initiatives can be adopted to address specific market failures, through the strengthening of the individuals' control on their data.[56] However, the effectiveness of these data sharing initiatives is being criticised[57], leading to a growing call for the introduction of a "continuous portability" right.[58] Moreover, a brief digression will be made about a more recent phenomenon, namely the

---

[49] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.
[50] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 942.
[51] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 10.
[52] See Part II of the thesis.
[53] See point 130.
[54] See Part II, Chapter 1, Sections A and B.
[55] See Part II, Chapter 1, Section A.
[56] See Part II, Chapter 1, Section B.
[57] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *CERRE Report*, 2020, available at https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy.
[58] *Ibidem*; Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 20. See Part II, Chapter 1, Section C.

adoption of several regulatory initiatives aiming at "empowering" specific (small) business users.[59]

Chapter 2 will focus on the key balancing exercises for these types of initiatives. Firstly, there is a need to balance the benefits that the specific individual will derive from the data sharing, on the one hand, and the potential effects that this might entail on the rights and freedoms of third parties, on the other hand. More concretely, a balance must be found between the benefits of the data sharing for the specific individual and the business interests of the data holder, and the data sharing must comply with the other data subjects' right to personal data protection.[60] Secondly, there is a need to balance the potential short-term gains that are promised to individuals via these "empowerment" initiatives with the potential long-term costs for these individuals in terms of control, autonomy and self-determination; and to balance the individual's potential gains from data sharing with the potential collective costs for other individuals.[61] Moreover, the matter of the competitive effects of these types of initiatives will also be addressed. On that basis, some insights on how these types of initiatives could be constructed will be formulated.

8. Part III of the thesis will be devoted to ***economic or societal initiatives imposing B2B data sharing***. In this Part, several key balancing exercises will also be discussed. The first three Chapters will be dedicated *to economic initiatives imposing B2B data sharing*. **Chapter 1** will first analyse whether the existing competition law balances pertaining to refusals to share a resource (essential facilities doctrine, abuse of economic dependence and input foreclosure), aiming at finding a balance between the benefits and costs of access/sharing in terms of incentives for each of the parties[62], remain appropriate in light of data's characteristics, or whether the results of these balancing exercises need to be adapted in order to better fit the characteristics of the data markets. This fits in a broader discussion pertaining to whether competition law needs to be adapted in order to better fit the digital environment.[63]

---

[59] See Part II, Chapter 1, Section D. See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018; Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019.

[60] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11-12.

[61] See Part I, Chapter 2, Section C, b) and Part II, Chapter 2, Section A, c).

[62] P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *Antitrust Law Journal*, 2008, n° 75, p. 616-620.

[63] See (EU) J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit*.; (Germany) H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *Report by the Commission "Competition Law 4.0" for the German Federal Ministry for Economic Affairs and Energy*, 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competitionframework.pdf? blob=publicationFile&v=2; (Germany) H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, Baden-Baden, Nomos, 2018 (also available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtigeunternehmen.html (an executive summary in English is available at https://ssrn.com/abstract=3250742)); (France) Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf; (BeNeLux) J. Steenbergen, M. Snoep and P.

Then, **Chapter 2** will discuss another balancing exercise entailing stronger societal considerations, namely the articulation between competition law and data protection law. In fact, it will be outlined that this articulation generates two core issues. First, there are growing concerns that the GDPR might limit competition and increase concentration in personal data and data-related markets.[64] Second, the GDPR must also be taken into consideration by a competition authority wishing to impose a data sharing remedy when (some of) the data at hand are personal data.[65]

Because of the complexity to solve the balancing exercises outlined in Chapter 1 and 2, growing discussions have emerged about alternative solutions than resorting to competition law for imposing B2B data sharing.[66] Accordingly, **Chapter 3** will discuss the creation of potential *ex ante* legislations imposing B2B data sharing for economic purposes. In essence, such *ex ante* legislations could be sectoral or could have a more general horizontal scope. Each of these options, which are not necessarily exclusive from one another, entail their own balancing exercises, which will need to be considered by the European legislator.

While the policy discussions pertaining to these economic initiatives are quite advanced, the reflections around the creation of *societal initiatives imposing B2B data sharing* are, on the other hand, still scarse. Yet, as they could have a significant role to play in achieving societal goals[67], they will be addressed in a shorter prospective **Chapter 4**, which will not aim for exhaustivity on this growingly important topic, but will rather have as main objective to

---

Barthelmé, "Joint memorandum of the Belgian, Dutch and Luxembourg competition authorities on challenges faced by competition authorities in a digital world", 2 October 2019, available at https://www.belgiancompetition.be/en/about-us/publications/joint-memorandum-belgian-dutch-and-luxembourg-competition-authorities; (UK) J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel; (UK) UK Competition & Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study; (USA) Stigler Committee on Digital Platforms, "Final Report*"*, September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report; (Australia) Australian Competition and Consumer Commission, "Digital Platforms Inquiry – Final Report", 26 July 2019, available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report. For a comparative analysis of some of these reports, see W. Kerber, "Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia", September 2019, available at https://ssrn.com/abstract=3469624; and S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", 31 March 2020, available at https://ssrn.com/abstract=3565491.

[64] M. Gal and O. Aviv, "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*, September 2020, Volume 16, Issue 3, p. 349-391; T. Zarsky, "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review*, 2017, Vol. 47, No. 4(2), p. 995-1020; T. Zarsky, "The Privacy–Innovation Conundrum", *Lewis & Clark Law Review*, 2015, Vol. 19, No. 1, p. 115-168; D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech", *TILEC Discussion Paper DP 2020-012*, May 2020, available at https://ssrn.com/abstract=3598130; G. Johnson and S. Shriver, "Privacy & market concentration: Intended & unintended consequences of the GDPR", March 2020, available at https://ssrn.com/abstract=3477686.

[65] T. Tombal, "The GDPR: A Shield to a Competition Authority's Data Sharing Remedy?", *Deep Diving into Data Protection*, J. Herveg (coord.), Bruxelles, Larcier, 2021, p. 67-94.

[66] See Part III, Chapter 1, Section E, b). See Communication from the Commission, "*Shaping Europe's digital future*", *op. cit*., p. 9; Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 3, 5 and 14.

[67] See Part I, Chapter 2, Section C, a).

launch avenues of exploration on why such initiatives could be envisaged and on how they could be constructed in the future.

9. Finally, the **Conclusion** of this thesis will come back on the fundaments of data sharing outlined in Part I, before synthesising the key balancing exercises that will have been emphasised in Part II and III, as well as the insights made in this thesis in order to address them.

Part I. The fundaments of (data) sharing: What, Why and How?

10. As outlined in the introduction, the main research question of this doctoral thesis is "***What are the economic and societal balancing exercises underlying compulsory B2B data sharing?***". In the context of this thesis, "data sharing" is defined as the act through which one or several data holder(s) provide(s) access to its(their) data to one or several data recipient(s), directly or through an intermediary, for the purpose of joint or individual use of the shared data, on the basis of voluntary agreements or of compulsory rules.[68] It does not only cover transfers of data from one party to another, but also data pooling initiatives, where different parties aggregate their data together in order to extract (economic and/or societal) value from the access to increased resources. A more extensive list of the various models of data sharing, considered in this thesis, are presented in Chapter 3, Section A.

To answer this main research question, the concept of *data* first needs to be specified (**What?**). This will be done in **Chapter 1**, where a data typology, to be used for the remainder of the thesis, will be proposed. Then, the rationale for (data) sharing will be analysed (**Why?**). In this regard, **Chapter 2** will first look back at the rationale for sharing "traditional" tangible or intangible resources, before turning to the same question for data. Finally, **Chapter 3** will present a typology of data sharing models and initiatives (**How?**). Here, two main categories of *compulsory B2B data sharing initiatives* will be identified on the basis of the rationale for data sharing that will have been outlined in the previous Chapter, namely, *"empowerment" initiatives imposing B2B data sharing*, on the one hand, and *economic or societal initiatives imposing B2B data sharing*, on the other hand.

[68] This definition is based on Articles 2.7 of the Proposal for a Data Governance Act; and Article 2.19 of the Proposal for a Digital Markets Act.

Chapter 1. Sharing what? A typology of data

11. Data is not a homogeneous good. It can be described on the basis of numerous typologies (public sector data v. private sector data; proprietary data v. public domain data; closed data v. open data…).[69] As, for the sake of concision, it would not be possible to delve into all of the possible typologies of data, this thesis will focus on two fundamental typologies. The first one pertains to the form of the data along the value chain (Section A). The second one pertains to the classic dichotomy between personal and non-personal data, which is broadly relied upon in the European legal framework (Section B).[70] On the basis of this analysis, a data typology will be suggested, which will be relied upon in the remainder of the thesis (Section C).

Section A. Form of the data along the value chain

12. Data comes into multiple forms and shapes, which evolve along the data value chain.[71] First, data is collected from users, extracted from sensors[72], or generated by the data holder itself (e.g. a football match calendar or a television programme). At this stage, it is considered as raw (or unstructured) data. This raw data can be collected/extracted/generated either as the object of the data collector's core economic activity (e.g. data collected by Facebook about its users in order to finance its activity by making profit through the sale of (personalised) advertising space) or as a by-product of this activity (e.g. data generated by sensors in a car assembly line).[73] This is also described as active or passive data collection/extraction/generation.[74] In many cases, firms will first start to collect/extract/generate data passively, as a by-product of their core economic activity, but once they realise the value that such data can have, they will tend to move towards more active approaches.[75]

Accordingly, in practice, it might be extremely difficult to determine whether a specific dataset has been collected/extracted/generated as a by-product or as the object of the data collector's core economic activity. Indeed, this notion of "core economic activity" is evolutive. For instance, Bayer-Monsanto, historically considered as an agriculture and

---

[69] See for instance OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019, available at https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm, p. 25-31.

[70] For a criticism of this broad reliance on the personal versus non-personal data dichotomy, see: I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, September 2018, available at http://ssrn.com/abstract=3256189.

[71] On the steps of this data value chain, see M. Gal and D. Rubinfeld, "Data Standardization", *New York University Law Review*, 2019, Vol. 94, Number 4, p. 746-747. See also OECD, *Consumer Data Rights and Competition - Background note*, June 2020, DAF/COMP(2020)1, available at http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm, p. 14-15; OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications, 2015, available at https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm, p. 32.

[72] M. Gal and D. Rubinfeld, "Data Standardization", *op. cit.*, p. 746.

[73] *Ibidem*; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 357; OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 15.

[74] OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 15.

[75] *Ibid*., p. 15-16. For an example in the retail business, see J. Turow, *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, New Haven, Yale University Press, 2017.

bioengineering firm, seems to be "heading towards becoming an information broker".[76] Therefore, while the datasets generated through the use of its agricultural and bioengineering products would have likely been considered, in the past, as by-products of its core economic activity, the same conclusion might not necessarily be reached today. In fact, it could maybe even be argued that generating this agricultural data is part of its new core economic activity, which is to become a major agricultural data broker, and that it only sells agricultural and bioengineering products in order to generate more data. In the same vein, car manufacturers might attempt to argue that, in the near future, with the advent of autonomous cars, they will strive towards becoming "mobility data companies" rather than simple "car builders". Accordingly, data generated by these autonomous cars might no longer be considered as by-products generated by these car manufacturers' core economic activity (building and selling cars), but might rather be considered as part of their new core economic activity (becoming leading mobility data companies that only sell cars in order to generate more data).

13. Second, this raw (unstructured) data is structured, interpreted and organised, transforming it into information (structured data).[77] In a joint study, the French and German competition authorities (the *Autorité de la Concurrence* and the *Bundeskartellamt*) distinguish between structured and semi-structured data.[78] The former follow "a model that defines a number of fields, what type of data these fields contain and how they relate to each other", while the latter "does not conform to a predefined model but certain elements or fields therein can be identified through a marker-type system".[79] This structuration of data increases the possibilities to extract value from the data, as they can more easily be processed and used than raw (unstructured) data.[80]

14. Third, this information (structured data) is analysed, transforming it into knowledge (analysed data) which can be used for prediction or decision-making.[81] To conduct these analyses, *Big Data*[82] analytics are increasingly called upon. They are characterised by the *four Vs*, namely "the **V**olume of data collected, the **V**ariety of sources, the **V**elocity with which the

---

[76] I. Carbonell, "The ethics of big data in big agriculture", *Internet Policy Review*, 2016, Issue 5(1), available at https://policyreview.info/articles/analysis/ethics-big-data-big-agriculture, p. 5.

[77] M. Gal and D. Rubinfeld, "Data Standardization", *op. cit.*, p. 746; R. Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, London, Sage Publications, 2014, p. 10 *et seq.*; M.J. Adler, *A Guidebook to Learning: For a Lifelong Pursuit of Wisdom*, London, Macmillan, 1986; L. Floridi, *Information: A Very Short Guide*, Oxford, Oxford University Press, 2010; H. von Baeyer, *Information: The New Language of Science*, Canbridge, Harvard University Press, 2003; D. Weinberger, *Too Big to Know*, New York, Basic Books, 2011; D. McCandless, "Data, information, knowledge, wisdom", 29 November 2010, available at http://www.informationisbeautiful.net/2010/data-information-knowledge-wisdom/.

[78] Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data", 10 May 2016, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf, p. 6.

[79] *Ibidem*.

[80] *Ibidem*.

[81] M. Gal and D. Rubinfeld, "Data Standardization", *op. cit.*, p. 746; R. Kitchin, *The Data Revolution*, *op. cit.*, p. 10 *et seq.*; M.J. Adler, *A Guidebook to Learning*, *op. cit.*; L. Floridi, *Information: A Very Short Guide*, *op. cit.*; M. Zelany, "Management support systems: towards integrated knowledge management", *Human Systems Management*, 1987, Volume 7, p. 59-70; D. Weinberger, *Too Big to Know*, *op. cit.*; D. McCandless, "Data, information, knowledge, wisdom", *op. cit.*

[82] ""Big data" is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software" (https://en.wikipedia.org/wiki/Big_data).

analysis of the data can unfold, and the **V**eracity of the data which could (arguably) be achieved through the analytical process" (emphasis in the text).[83] These *four Vs* subsequently increase the **V**alue that can be derived from the data analysis.[84] According to the OECD, "the value of data is mainly reaped at two moments: first when data are transformed into knowledge (gaining insights), and then when they are used for decision-making (taking action). Decisions taken can in turn lead to more or different data generated and thus trigger a new data value cycle".[85]

Naturally, some data holders can skip the above-mentioned data value chain by directly acquiring structured or analysed data from third parties, such as data brokers. In that case, they directly acquire information (structured data) or knowledge (analysed data) rather than raw (unstructured) data.

15. While it might seem somewhat artificial, the above-mentioned typology based on the form of the data along the value chain has an importance in practice, because the true value of data does not generally derive from the raw data as such, but rather from the information and knowledge that can be extracted from it.[86] Indeed, as elegantly put by Mayer-Schönberger and Padova, data "is like a single puzzle piece that taken by itself offers little value, but when combined with others to complete an image is turned into something precious".[87]

---

[83] T. Zarsky, "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review*, 2017, Vol. 47, No. 4(2), p. 998-999.
[84] M. Gal and D. Rubinfeld, "Data Standardization", *op. cit.*, p. 744; OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 10.
[85] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 32.
[86] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 342. However, this does not mean that raw data does not have any value at all, as a third party may prefer to have access to raw data, in order to create its own structured data (information) that better corresponds to its needs, rather than to information that has been structured differently by the data holder.
[87] V. Mayer-Schönberger and Y. Padova, "Regime change? Enabling Big Data through Europe's new Data Protection Regulation", *Columbia Science & Technology Law Review*, Vol. XVII, 2016, p. 320.

Section B. Personal and non-personal data: a porous boundary

16. Data can also be classified as personal or non-personal. Personal data are defined in the General Data Protection Regulation (hereafter "GDPR") as "any information relating to an identified or identifiable natural person (data subject)".[88] Information can relate to an identified or identifiable natural person either in content, purpose, result or impact.[89] According to the GDPR, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.[90] In order to determine whether a person is identifiable, account must be taken of all the reasonable means likely to be used, either by the data controller[91] or by a third party, to identify, directly or indirectly, the person.[92] In other words, a person is identifiable if it can be singled out.[93] To ascertain the likeliness of the reidentification of the person, account must be taken of a series of objective factors, such as the costs of, and the amount of time required for, the reidentification, in light of the available technology and technological developments at the time of the processing.[94]

---

[88] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4 May 2016, article 4.1. See also Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, CM/Inf(2018)15-final, article 2.a.

[89] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, p. 9-12; Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, WP 223, 16 September 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p. 10-11; Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *Council of Europe Treaty Series n° 223*, Strasbourg, 10 October 2018, available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a, p. 3-4; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union, 2018, p. 83-93; C. de Terwangne, "Définitions clés et champ d'application du RGPD", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 60-63; I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy" *op. cit*., p. 5; ECJ, *Peter Nowak v Data Protection Commissioner*, 20 December 2017, C-434/16, EU:C:2017:994, § 35.

[90] Article 4.1 of the GDPR.

[91] "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4.7 of the GDPR).

[92] Recital 26 of the GDPR.

[93] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, *op. cit*., p. 12-15; Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, *op. cit*., p. 10-11; Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251 rev.01, 6 February 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, p. 6-8; Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *op. cit.*, p. 3-4; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, *op. cit*., p. 83-93; C. de Terwangne, "Définitions clés et champ d'application du RGPD", *op. cit.*, p. 63-64; I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy", *op. cit*., p. 5; C. de Terwangne, "La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel", *Quelle protection des données personnelles en Europe?*, C. Castets-Renard (dir.), Bruxelles, Larcier, 2015, p. 84-85.

[94] Recital 26 of the GDPR.

17. In the context of its guidelines on the right to data portability enshrined in Article 20 of the GDPR[95], the Article 29 Working Party (today the European Data Protection Board – EDPB) has identified three categories of personal data.[96]

The first category of personal data is "data actively and knowingly provided by the data subject".[97] This includes, but is not limited to, any information provided by completing an online registration form, posts on social media, etc. This category is also sometimes referred to as "volunteered data".[98] Yet, this latter terminology can be somewhat misleading, as it seems to imply that the data subject has always taken the initiative to provide the data "willingly". However, in some cases, the data subject has no other choice than to actively provide the data, even if she is not "willing" to do so (e.g. bank customers are legally obliged to disclose some information to their bank). Accordingly, a less ambiguous term such as "actively provided data" is preferable to describe this first category.

The second category of personal data is "observed data provided by the data subject by virtue of the use of the service or the device".[99] Examples include the search history of a data subject, the history of the websites she has visited, traffic and location data generated by the use of a mobile application, or other types of data, such as the average pulse rate or the number of steps taken by a data subject, which would be collected by a connected watch. For these observed data, a further distinction can be made between first party and third party observed data.[100] First party observed data are data collected directly by the controller from its users, on the basis of their use of the controller's product or service (e.g. the search queries typed by users and collected by Google).[101] Third party observed data, on the other hand, are data collected indirectly from the users, on the basis of their use of the product or service of a third party, via a range of different technologies such as "cookies" (e.g. the data collected by Google through third party tracking cookies on a range of websites not operated by Google).[102]

The third category of personal data is "inferred data and derived data created by the data controller on the basis of the data "provided by the data subject"".[103] This refers to data resulting from a subsequent analysis carried out by the controller on the basis of data provided (actively or observed) by the data subject. Examples are user profiles created by the controller on the basis of the analysis of data provided by the data subjects, or the results of an assessment of the data subject's health based on the health data collected by her smart watch.[104] This is also sometimes presented as "second generation data", which is created,

---

[95] On this right, see Part II, Chapter 1, Section A.
[96] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233, p. 9-11.
[97] *Ibid*., p.10.
[98] OECD, *Enhancing Access to and Sharing of Data, op. cit.*, p. 30.
[99] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10.
[100] OECD, *Consumer Data Rights and Competition, op. cit.*, p. 16-18.
[101] *Ibid*, p. 16.
[102] *Ibidem*. See also V. Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Common Market Law Review*, 2020, Vol. 57, p. 162.
[103] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10.
[104] *Ibidem*.

inferred or derived from "first generation data".[105] These types of data will often be the most valuable for data holders, as this is where the real added-value of their service must be found.[106] The difference between derived and inferred data relies on the type of analytics used to generate them. Indeed, according to the United Kingdom's Information Commissioner's Office (the UK's data protection authority), derived data "is produced from other data in a relatively simple and straightforward fashion, e.g. calculating customer profitability from the number of visits to a store and items bought", while inferred data "is produced by using a more complex method of analytics to find correlations between datasets and using these to categorise or profile people, e.g. calculating credit scores or predicting future health outcomes. Inferred data is based on probabilities and can thus be said to be less 'certain' than derived data".[107]

A fourth category of personal data can be added, namely "acquired data", which is personal data obtained from third parties on the basis of a voluntary data sharing mechanism (e.g. data acquired from data brokers)[108], or on the basis of a compulsory data sharing mechanism. Indeed, as it will be outlined further in this thesis, some well-identified data recipients have a right to acquire some data from well-identified data holders, provided that certain specific conditions are met. For instance, the revised Directive on payment services in the internal market (PSD2)[109] grants to the providers of payment initiation service and the providers of account information service[110] the right to acquire the payment account information[111] of the users of their services (the consumers), if the latter have explicitly consented to it.[112]

Distinguishing between these categories of personal data is relevant, as the individuals' level of awareness about the processing of their personal data will be different for each category, which in turn has an impact on the control they have on "their" personal data.[113] Indeed, individuals will likely be aware of, and more comfortable with, the processing of actively provided or first party observed data. On the other hand, the collection of third party observed

---

[105] R. Kemp, "Legal Aspects of Managing Data (White Paper)", October 2019, available at http://www.kempitlaw.com/legal-aspects-of-managing-data/, p. 8.

[106] Primary and observed data can, however, also be of great value, especially when the costs of data collection are very high and/or when the data is difficult to collect (e.g. satelite imagery). On this point, see also points 303 and 304.

[107] Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection", 4 September 2017, available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, p. 12-13.

[108] OECD, *Enhancing Access to and Sharing of Data, op. cit.*, p. 31. See Part I, Chapter 3, Section A for a presentation of the most common conceptual models that can be used for such voluntary data sharing.

[109] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015. See Part II, Chapter 1, Section B, b).

[110] Respectively defined as "a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider" and as "an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider" (Directive 2015/2366, articles 4.15 and 4.16).

[111] Defined as "account held in the name of one or more payment service users which is used for the execution of payment transactions" (Directive 2015/2366, article 4.12).

[112] Directive 2015/2366, arts. 64-67.

[113] OECD, *Consumer Data Rights and Competition, op. cit.*, p. 17.

data, the generation of inferred or derived data and the acquisition of personal data will be more obscure to them, and will affect the sense of control that they have on the types of data processing for which they are used.[114]

18. Non-personal data, on the other hand, are usually residually defined as all data other than personal data[115], either because they have never been personal data in the first place (such as industrial data generated by the "Internet of Things" (*IoT*)[116], e.g. sensors installed on industrial machines that provide data on maintenance needs), or because they have been anonymised[117] (e.g. through mathematical and statistical operations) and therefore no longer qualify as personal data because the data subject is no longer identifiable.[118] In this regard, anonymised data should not be confused with pseudonymised data, which remain personal data subject to the GDPR, given that the data subject can still be re-identified by using additional information.[119] Importantly, determining whether specific data should be considered as anonymised or pseudonymised will always be function of the specific circumstances of each individual case.[120]

19. This choice of a residual definition for non-personal data has been criticised, as it presumes that the scope of what constitutes personal data can be clearly defined.[121] Yet, in practice, it might not be easy to determine whether specific data should be considered as personal or not. This is due to the broad definition of personal data, making it a dynamic, fluid and open-ended concept, as the possibilities of re-identification evolve with the technology,

---

[114] *Ibidem*.
[115] See for instance Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018, article 1.
[116] See footnote 4.
[117] The ISO 29100 standard defines anonymisation as the : "process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" (ISO 29100:2011, point 2.2, available at https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en).
[118] Recital 26 of the GDPR; Communication from the Commission to the European Parliament and the Council, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", Brussels, 29 May 2019, COM(2019) 250 final, p. 6. On anonymisation, see Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, *op. cit.*, p. 21; Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP 216, 10 April 2014, available at https://www.pdpjournals.com/docs/88197.pdf, p. 5-11; Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *op. cit.*, p. 4; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, *op. cit.*, p. 93-94; C. de Terwangne, "Définitions clés et champ d'application du RGPD", *op. cit.*, p. 64-65.
[119] Recital 26 of the GDPR. On pseudonymisation, see Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, *op. cit.*, p. 18-20; Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, *op. cit.*, p. 10-11 and 20-23; Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *op. cit.*, p. 4; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, *op. cit.*, p. 94-95; C. de Terwangne, "Définitions clés et champ d'application du RGPD", *op. cit.*, p. 64-65.
[120] Communication from the Commission, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", *op. cit.*, p. 6.
[121] L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability", *EDPL*, 2020/1, p. 88-89; I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy", *op. cit.*, p. 4-6.

increasing over time the scope of what should be considered as personal data.[122] Indeed, "technological and other developments may change what constitutes "unreasonable time, effort or other resources" (…) to re-identify the data subject".[123]

This has led some authors to call for a new taxonomy of data, because it is impossible to govern and regulate personal data and non-personal data separately, in light of the constant flow between each category.[124] Moreover, the above dichotomy is also complex to apply in practice because, in most cases, datasets will be "mixed", i.e. composed of both personal and non-personal data, in light of technological developments such as the *IoT* or *Big Data* analytics.[125] Additionally, if these mixed datasets are "inextricably linked", the GDPR will have to be applied to the entirety of the dataset, even if personal data only represent a small part of it.[126] Although this concept of "inextricably linked" is not defined, it should be understood as encompassing situations where it would be impossible, economically inefficient, or technically infeasible to separate the personal data from the non-personal data in the set.[127] The changing nature of the data and a significant decrease in the value of the dataset, if separated, could lead to such situations.[128] In sum, because most of the datasets are mixed and "inextricably linked", there is a risk that "in the near future everything will be or will contain personal data, leading to the application of data protection to everything".[129]

20. This is even more so if one considers the constant development of *Big Data* analytics. Indeed, *Big Data* analytics allow the gathering of data at unprecedented scale, as the time and cost required to do so has been drastically reduced by technological evolutions.[130] In turn, this increases the possibility to do cross analysis on multiple data sets, to which it was previously more difficult to have access. This consequently exacerbates the risk of direct or indirect re-identification of a data subject on the basis of these data, whether by the controller or by a third party. In doing so, data considered at a time "T" as non-personal may thus, on the basis

---

[122] OECD, *Enhancing Access to and Sharing of Data, op. cit.*, p. 26; L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU", *op. cit.*, p. 88-90; I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy", *op. cit.*, p. 4.

[123] Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *op. cit.*, p. 4.

[124] L. Taylor, "Hacking a path through the Personal Data Ecosystem", December 2013, available at https://linnettaylor.wordpress.com/2013/12/12/hacking-a-path-through-the-personal-data-ecosystem/. See also I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy", *op. cit*.

[125] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", Brussels, 29 May 2019, COM(2019) 250 final, p. 4 and 7; I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy", *op. cit.*, p. 6.

[126] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018, article 2.2; Communication from the Commission, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", *op. cit.*, p. 9.

[127] Communication from the Commission, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", *op. cit.*, p. 10.

[128] *Ibidem*.

[129] N. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, 2018, Vol. 10, Issue 1, p. 40.

[130] V. Mayer-Schönberger and Y. Padova, "Regime change?", *op. cit.*, p. 317-318.

of technological developments in data analytics capabilities, become personal data at time "T+1".

For example, at the end of the 1990s, a researcher in the United States managed to re-identify more than 80% of the people whose data were contained in a database of a private company operating in the health sector, even though these data were supposed to be anonymised.[131] In fact, while the names of these people had been deleted, the database still contained medical information as well as the postal code, gender, and full date of birth. Yet, the latter three pieces of information were also included in the registers of electoral lists, which were accessible to the public, enabling the researcher to cross-reference these data, to identify 80% of the persons contained in the file and to obtain information on their health status. This example illustrates that the risk of re-identification increases with the development of new technologies and increasing access to large data sets.[132] Therefore, what is presented as anonymisation techniques are, in fact, often merely pseudonymisation techniques.[133] Yet, as already outlined, pseudonymised data remain personal data subject to the GDPR, given that the data subject can still be re-identified.[134]

[131] L. Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality", *Journal of Law, Medicine & Ethics*, 1997, Vol. 25, Issues 2 & 3, p. 98-110; Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, *op. cit*., p. 33-34.

[132] For other examples, see M. Barbaro and T. Zeller, "A Face is exposed for AOL searcher no. 4417749", *The New York Times*, 9 August 2006, available at https://www.nytimes.com/2006/08/09/technology/09aol.html; P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, Volume 57, 2010, p. 1716-1722; J. Pearson, "Yahoo's Gigantic 'Anonymized' User Dataset Isn't All That Anonymous", 14 January 2016, available at https://www.vice.com/en/article/yp3d8v/yahoos-gigantic-anonymized-user-dataset-isnt-all-that-anonymous; L. Rocher, J. Hendrickx and Y.-A. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, 2019, Vol. 10, n°3069, available at https://www.nature.com/articles/s41467-019-10933-3.

[133] "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Article 4.5 of the GDPR). See also Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, *op. cit*., p. 8.

[134] Recital 26 of the GDPR.

Section C. Proposed data typology

21. Because this boundary between personal and non-personal data is porous and often difficult to establish in practice, this thesis will suggest an alternative data typology, following a common holistic approach for both personal and non-personal data[135], which will nevertheless take personal data protection considerations into account when relevant.[136] This proposed typology will then be relied upon in the remainder of the thesis.

Indeed, when looking at the four categories of personal data presented above (actively provided, observed, inferred/derived, and acquired data)[137], these categories can also be applied to non-personal data. Indeed, while objects cannot "knowingly" provide data about themselves, as they have no conscience (e.g. a machine in an assembly line does not decide to provide data about its wear and tear to the manufacturer), non-personal data can be actively and knowingly provided by an anonymous person (e.g. votes in an election, answers to a survey, etc.). It can also be actively created by the data holder itself (e.g. a football match calendar or a television programme). Furthermore, non-personal data collected via *IoT* sensors or via the observation of electronic operations can be considered as "observed data" (e.g. weather, humidity or pesticides level data collected by "smart tractors"; or wear and tear data collected by a sensor on an industrial machine in a car assembly line). Moreover, "inferred/derived non-personal data" can be generated on the basis of these actively provided and observed data, as insights are drawn from their analysis (e.g. the weather/humidity data can be analysed to infer when it will be optimal to plant a specific type of seed; or the wear and tear data of the assembly line machine can be analysed in order to derive when the next maintenance operation will need to be planned). In this regard, personal data that has become non-personal because it has been anonymised shall be considered as derived data, as it is a second generation of data that derives from mathematical operations conducted on the first generation of personal data. Additionally, non-personal data can also be acquired from third parties (acquired data), such as data brokers (e.g. farmers could acquire, from agriculture data brokers, data about the level of efficiency of specific pesticides against specific diseases or insects).

These four categories of data (actively provided, observed, inferred/derived, and acquired data) can in fact be classified in three broader categories of data, namely i) "primary data", ii) "inferred/derived data", and iii) "acquired data". Indeed, actively provided and observed data can be classified in a common group of "primary data". Inferred/derived data are a second generation of data drawn, by the data holder itself, from the analysis of this first generation of primary data. The data holder could also opt to acquire primary or inferred/derived from third parties, such as data brokers ("acquired data"). The distinction between these three broader categories of data (primary data, inferred/derived data and acquired data) will be relevant when considering (future) data sharing obligations imposed by the EU legal framework.

---

[135] For a call to follow such a holistic approach see I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy" *op. cit.*, p. 14-18.
[136] See, for instance, Part III, Chapter 2 "Articulation between data protection and competition law".
[137] See point 17.

22. When integrating the forms of data along the value chain in the equation, it can be assumed that primary data (actively provided and observed) will generally be raw (unstructured), semi-structured or structured data (information). This will notably be the case for personal data collected through an online form or through the observation of individuals' behaviour on the internet, and for non-personal IoT data collected by sensors on "smart" agricultural or industrial machinery. Moreover, depending on the circumstances of the case, this primary data can either be the object of the data collector's core economic activity or a by-product of this activity.[138] Taking the non-personal IoT data examples mentioned above, it could be argued that collecting weather, humidity or pesticides level data may constitute the core economic activity of the provider of smart farming equipment, while the wear and tear data collected by a sensor on an industrial machine in a car assembly line could be considered as a by-product of the data collector's core activity, which is to manufacture cars.

Inferred/derived data, on the other hand, will generally be considered as analysed data (knowledge), as it is a second generation of data drawn from the analysis of the first generation of primary data. For instance, data collectors will be able to draw profiles of individuals and to infer knowledge about their preferences, on the basis of the primary personal data that has been collected about them (their age, sex or country of residence; the websites they have visited; the music they listen to; the videos they have watched, etc). Similarly, data collectors will be able to generate knowledge/insights on the basis of the primary non-personal that they have collected. For instance, the analysis of truck tyres' sensor data and the combination of this information with data about the weight of the loads that has been put in those trucks could allow transport service providers to infer knowledge about the optimal load weight for a specific type of truck, in order to reduce tyre degradation and to increase the durability of those tyres. Finally, "acquired data" could either be raw (unstructured) data, information (structured data) or knowledge (analysed data).

23. Although this suggested typology follows a common holistic approach for both personal and non-personal data, it must be outlined from the outset that the remainder of the thesis will focus more on behavioural or consumer data than on non-personal IoT data. This is mainly because the two gaps that this thesis aims to fill through a normative approach precisely pertain to such behavioural/consumer data.[139] Moreover, most of the European policy discussions pertaining to compulsory B2B data sharing relate to large data actors that draw a "data advantage" from their privileged access to, and control of, consumer/behavioural data.[140] In fact, even the European policy discussions on IoT data mostly focus on consumer/behavioural data, rather than on purely industrial non-personal IoT data, as illustrated by the recent preliminary report of the European Commission on its "Consumer

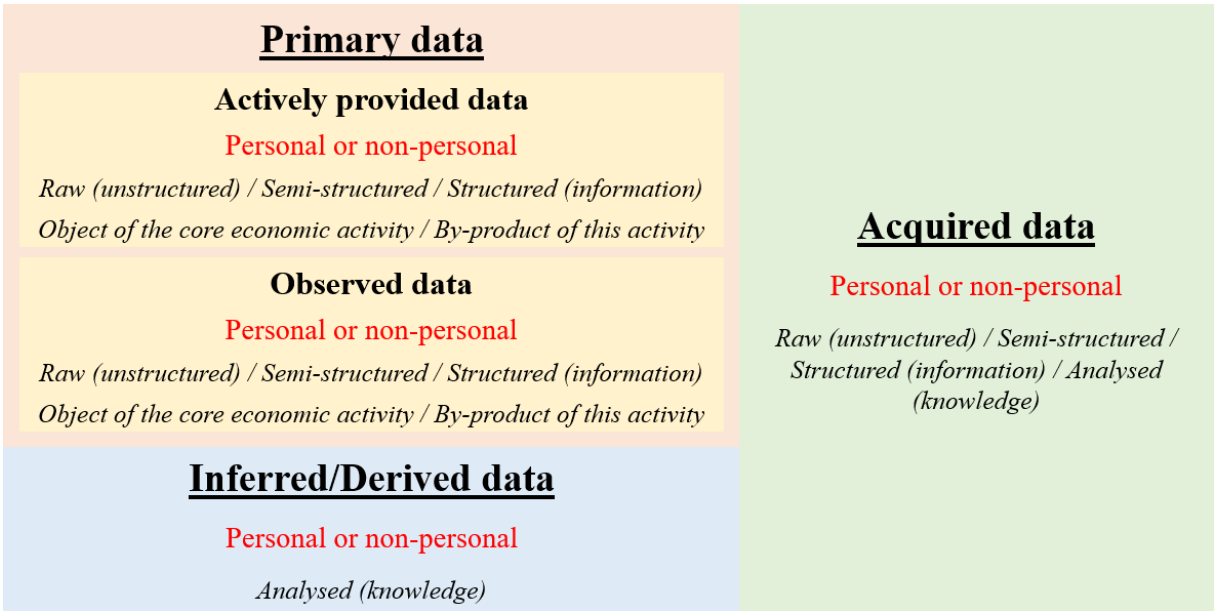
[138] See point 12. M. Gal and D. Rubinfeld, "Data Standardization", *op. cit.*, p. 746; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 357; OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 15.
[139] See point 5.
[140] See Part I, Chapter 2, Section B, c); Part II, Chapter I; Part III, Chapters 1 and 3. See, for instance, the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final.

Internet of Things sector inquiry".[141] Indeed, this sector inquiry focusses on four consumer IoT segments, namely the manufacture of smart home devices and of wearable devices, and the provision of voice assistants and of consumer IoT services (such as search or health services). This focus can be explained by the fact that consumer/behavioural data are at the core of certain online markets such as search, social networks or e-commerce, and constitute a fundamental resource to compete on these markets. Accordingly, the issue of the (lack of) access to such data is particularly sensitive.

On the other hand, IoT non-personal data have received much less policy attention, especially since the option to create a "data producers right" on non-personal machine generated data has been abandoned.[142] A potential explanation for this is that such data is often generated as a by-product of other industrial activities, and that, as a result, they might not be perceived as creating as many data access issues. While this could change in the future with the growth of the IoT, notably in the context of societal initiatives imposing B2B data sharing[143], this also explains why the focus of this thesis is mostly set on consumer/behavioural data, rather than on IoT non-personal data.

24. Finally, it must be admitted that the classification suggested above may not always be perfectly applicable. Nevertheless, this simplified classification has the merit to offer a clear data typology for the remainder of the thesis. For clarity purposes, this typology is summarised in Figure 1 below.

Figure 1: Proposed data typology



[141] Commission Staff Working Document, Preliminary Report – Sector inquiry into consumer internet of things, Brussels, 9 June 2021, SWD(2021) 144 final.
[142] On this topic, see Part I, Chapter 2, Section B, b), 2.
[143] See Part I, Chapter 2, Section C, a); and Part III, Chapter 4.

Chapter 2. Why sharing? The rationale for (data) sharing

25. In order to answer the main research question of this doctoral thesis ("***What are the economic and societal balancing exercises underlying compulsory B2B data sharing?***"), it is necessary to focus on fundamental considerations pertaining to the rationale for data sharing. Said otherwise, what could justify the imposition of data sharing obligations?

Before attempting to answer this question, it is worth reverting to more classical discussions on whether a resource should be shared. Indeed, such type of discussions have not emerged with data. Finding a balance between granting exclusive ownership/property rights to the few, on the one hand, and providing access to and sharing resources with the many, on the other hand, has also always been a challenge, whether this related to tangible or intangible resources. Therefore, **Section A** will shed light on the **balance between the exclusive use of, and the access to/sharing of, tangible and intangible resources,** and on the various critics pertaining to how it has been addressed. On that basis, the **economic and societal rationale for sharing intangible resources** will be presented. The reason why this thesis will focus solely on intangible resources for this last aspect is because they share a key characteristic with data, namely their non-rivalrous nature, while tangible resources, on the other hand, are rivalrous.[144]

Then, the thesis will turn, in **Sections B and C,** towards the analysis of the same **balance in the realm of data**. **Section B** will focus on the **economic rationale for data sharing**. To do so, **data's characteristics** will first be presented. Moreover, the question of **whether data are subject to (intellectual) property rights** will be tackled. Then, this thesis will dive deeper in the analysis of the **economic rationale for data sharing**, as it is not a goal in itself and as a balance must be found between exclusive use of and access to/sharing of data.[145]

Section C will be dedicated to **the societal and the "empowerment" rationale** for data sharing. On the one hand, data sharing could support **broader societal objectives**.[146] On the other hand, data sharing is increasingly presented as a **way to empower individuals**, by giving them more control on "their" data.[147] Regarding these **"empowerment" initiatives**, it will be outlined that one should not be blinded by their benefits and that great attention should also be paid to the **long-term and collective risks that they could entail in terms of personal autonomy and (informational) self-determination**.

---

[144] See points 33 and 52.
[145] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing: an economic and legal analysis", *EU Science Hub*, 2020, available at https://ssrn.com/abstract=3658100, p. 5.
[146] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", 19 February 2020, COM(2020) 66.
[147] *Ibid*., p. 10. See also p. 20-21.

Section A. To share or not to share resources: a balance between exclusive use and access/sharing

26. Since the dawn of humanity, dividing resources between the various members of a group has always been a challenge. This Section will first address the debates pertaining to the sharing of tangible resources, before moving on to intangible resources. Then, an attempt at the identification of some rationales for sharing resources will be made.

a) Balance between exclusive use of and access to/sharing of tangible resources

1. The tragedy of the commons

27. In the realm of tangible resources, exclusive property has, for centuries, been invoked as an efficient solution to avoid overuse of resources leading to their depletion.[148] One of the most emblematic pleas in this regard is Hardin's paper in *Science* titled "The Tragedy of the Commons".[149] Hardin's starting point, as a biologist working on the issue of Earth's "population problem" (i.e. overpopulation), is that, because the population naturally tends to grow exponentially, while the amount of tangible resources in a specific territorial area are finite[150], the per capita share of the available resources will necessarily steadily decrease.[151]

Questioning Adam Smith's theory of the "invisible hand", following which decisions taken individually by people having their own interest and gain in mind actually lead to benefits for the whole society[152], Hardin argues that allowing people to act as they please and to consume freely commonly shared tangible resources would inevitably lead to a "tragedy of the commons".[153] In perhaps the most notorious extract of his paper, Hardin explains how, according to him, this "tragedy" unfolds:

> "Picture a pasture open to all. It is to be expected that each herdsman will try to keep as many cattle as possible on the commons. Such an arrangement may work reasonably satisfactorily for centuries because tribal wars, poaching, and disease keep the numbers of both man and beast well below the carrying capacity of the land. Finally, however,

---

[148] W. Blackstone, *Commentaries on the Laws of England*, Book 2, Chapter 1, Oxford, Oxford University Press, 1771, available at https://avalon.law.yale.edu/18th_century/blackstone_bk2ch1.asp; R.-J. Pothier, "Traité de la propriété", *Œuvres de R.-J. Pothier*, D. Ainé (ed.), tome V, Bruxelles, Tarlier, 1831; B. Windscheid, *Lehrbuch des Pandektenrechts*, 3 volumes, Frankfurt am Mein, Rutten & Loening, 1891; J. Bonnecase, *Précis de droit civil*, 2e éd., Paris, Rousseau, 1938, t. I; R. Schlatter, *Private Property: the History of an Idea*, New Brunswick, Rutgers University Press, 1951; G. Hardin, "The Tragedy of the Commons", *Science*, December 1968, Vol. 162, Issue 3859, p. 1243-1248; P. Ehrlich, *The Population Bomb*, New York, Ballantine Books, 1968; D. Feeny, F. Berkes, B. McCay and J. Acheson, "The Tragedy of the Commons. Twenty-Two Years Later", *Human Ecology*, 1990, Volume 18, Issue 1, p. 1-19; M. Kramer, *John Locke and the Origins of Private Property*, Cambridge, Cambridge University Press, 1997; T. Merrill, "Property and the Right to Exclude", *Nebraska Law Review*, Volume 77, Issue 4, 1998, p. 730-755; P. Gansey, *Thinking About Property: From Antiquity to the Age of Revolution*, Cambridge, Cambridge University Press, 2007; B. Frischmann, A. Marciano and G. Ramello, "Retrospectives: Tragedy of the Commons After 50 Years", *Journal of Economic Perspectives*, 2019, Volume 33, Issue 4, p. 211-228.

[149] G. Hardin, "The Tragedy of the Commons", *op. cit.*, p. 1243-1248.

[150] It must be outlined from the outset that Hardin's starting point focusses on depletable finite resources and that, accordingly, his reasoning cannot be translated to the use of non-depletable tangible resources such as the energy that can be derived from the sun or the wind.

[151] G. Hardin, "The Tragedy of the Commons", *op. cit.*, p. 1243.

[152] A. Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, London, 1776.

[153] G. Hardin, "The Tragedy of the Commons", *op. cit.*, p. 1244.

comes the day of reckoning, that is, the day when the long-desired goal of social stability becomes a reality. At this point, the inherent logic of the commons remorselessly generates tragedy.

As a rational being, each herdsman seeks to maximize his gain. Explicitly or implicitly, more or less consciously, he asks, "What is the utility to me of adding one more animal to my herd?" This utility has one negative and one positive component.

1) The positive component is a function of the increment of one animal. Since the herdsman receives all the proceeds from the sale of the additional animal, the positive utility is nearly +1.

2) The negative component is a function of the additional overgrazing created by one more animal. Since, however, the effects of overgrazing are shared by all the herdsmen, the negative utility for any particular decision-making herdsman is only a fraction of -1.

Adding together the component partial utilities, the rational herdsman concludes that the only sensible course for him to pursue is to add another animal to his herd. And another; and another.... But this is the conclusion reached by each and every rational herdsman sharing a commons. Therein is the tragedy. Each man is locked into a system that compels him to increase his herd without limit in a world that is limited. Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons. Freedom in a commons brings ruin to all".[154]

Moving away from this bucolic narrative, Hardin outlines that the tragedy of the commons equally applies to more contemporary issues such as overfishing or pollution.[155] For him, such a scenario could only be averted by granting private property rights or through governmental regulation, even if such a legal system is itself not perfect and potentially unjust.[156] This is because, for him, "[t]he alternative of the commons is too horrifying to contemplate. Injustice is preferable to total ruin".[157]

28. Hardin's paper had a huge impact as it became *Science*'s most-cited article ever, and his depiction of the "tragedy of the commons" was relayed by numerous economists, social scientists and politicians in order to justify the need for strong private property.[158] In fact, it has been reformulated by some as a prisoner's dilemma game[159], outlining "the paradox that

---

[154] *Ibidem*.
[155] *Ibid*., p. 1245.
[156] *Ibid*., p. 1245-1247.
[157] *Ibid*., p. 1247.
[158] D. Bollier and S. Helfrich, *Free, Fair and Alive. The Insurgent Power of the Commons*, Gabriola Island, New Society Publishers, 2019, p. 16.
[159] See R.M. Dawes, "The commons dilemma game: An N-person mixed motive game with a dominating strategy for defection", *Organ. Res. Inst. Res. Bull*., 13(2), 1973, p. 1-12. The prisoner's dilemma game describes a situation in which two rational individuals might prefer to act in their own interest rather than to cooperate with each other, even if it would be in their best interest to cooperate (see https://en.wikipedia.org/wiki/Prisoner%27s_dilemma).

individually rational strategies lead to collectively irrational outcomes".[160] Moreover, a closely related view was developed by Olson in his book "The Logic of Collective Action".[161] He indicated that "unless there is coercion or some other special device to make individuals act in their common interest, rational, self-interested individuals will not act to achieve their common or group interests".[162] According to Ostrom, these three models (the tragedy of the commons, the prisoner's dilemma and the logic of collective action) are closely related because the free-rider problem lies at the heart of each of them.[163] As she explains, "whenever one person cannot be excluded from the benefits that others provide, each person is motivated not to contribute to the joint effort but to free-ride on the efforts of others. If all participants choose to free ride, the collective benefit will not be produced".[164] As will be outlined below, this free-rider problem is also a key concern raised in the debates pertaining to compulsory B2B data sharing.[165]

29. As a result of these three models, the decline of the commons and the ever-growing importance of private property have led to a steep increase in the quantity and concentration of capital.[166] To some extent, this is not surprising because, in our Western societies, "the right to exclude is the essential feature of owning property, and every limit is at most exceptional and temporary".[167] This paradigm of modern private property finds its roots in our history, going back to the concept of *dominium* in Roman law and culminating in the definition of property in the Napoleonic Code of 1804[168] and in the German private law Code of 1896.[169] Its justification is traditionally rooted in the pursuit of social stability (Grotius[170] and Hobbes[171]) and of individual liberty (Locke[172]), and, more recently, in the pursuit of wealth maximisation through an efficient allocation of resources (Posner[173]).[174] In this regard, the Napoleonic Code understands property above all as an individual relationship to goods,

---

[160] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge, Cambridge University Press, 1990, p. 5.
[161] *Ibidem*.
[162] M. Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*, Harvard University Press, 1965, p. 2.
[163] E. Ostrom, *Governing the Commons, op. cit.*, p. 6.
[164] *Ibidem*.
[165] See below point 55.
[166] U. Mattei and A. Quarta, *The Turning Point in Private Law. Ecology, Technology and the Commons*, Cheltenham, Edward Elgar, 2019, p. 3.
[167] *Ibid*., p. 12.
[168] "Property is the right to enjoy and dispose of things in the most absolute manner, as long as one does not make use of them in a manner prohibited by laws or regulations" (author's own translation from article 544 of the Belgian Civil Code of 21 March 1804).
[169] U. Mattei and A. Quarta, *The Turning Point in Private Law, op. cit.*, p. 14; 21. See also R.-J. Pothier, "Traité de la propriété", *op. cit.*; B. Windscheid, *Lehrbuch des Pandektenrechts*, *op. cit*.; J. Bonnecase, *Précis de droit civil*, *op. cit*.; R. Schlatter, *Private Property: the History of an Idea*, *op. cit*.; P. Gansey, *Thinking About Property: From Antiquity to the Age of Revolution*, *op. cit*.
[170] H. Grotius, *De Iure Belli ac Pacis*, 1625.
[171] T. Hobbes, *Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil*, 1651.
[172] J. Locke, *Two Treatises of Government: In the Former, The False Principles, and Foundation of Sir Robert Filmer, and His Followers, Are Detected and Overthrown. The Latter Is an Essay Concerning The True Original, Extent, and End of Civil Government*, London, Awnsham Churchill, 1690.
[173] R. Posner, *Economic Analysis of Law*, Boston, Little Brown, 1973.
[174] B. Lomfeld, "Fondements de la propriété (Théories de la propriété)", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 566-569.

and regimes of collective property are only considered as temporary and marginal situations.[175] The essence of the property right as enshrined in the Code is thus the power to exclude.[176]

This dominant legal approach to the idea of "property as exclusion" has a significant political impact, as it determines the default rules of our legal system, namely that the exclusive property model should be the norm, unless there are legally established reasons to depart from it.[177] Such departure from the "exclusivity norm" can, for instance, be observed for *res nullius*, which are goods that are not owned by anyone[178], or for *res communes omnium*, which belong to everyone because it is not necessary to appropriate them in order to be able to use them (e.g. air or light).[179] Consequently, this dominant legal approach also has an impact on the rationale for sharing because, in our social construct, "exclusive ownership" or "exclusive property" is generally the default model, while models based on sharing/access are less common.

2. Reconsidering (the tragedy of) the commons

30. While Hardin's analysis has had a tremendous impact, it is, to some extent, flawed.[180] This is because what Hardin depicts as a commons is in fact not a commons, but "a free-for-all in which nothing is owned and everything is free for the taking".[181] Rather, the notion of "commons" refers to "a form of community management or governance of a shared resource [i.e. one that is produced, used, and/or consumed by multiple actors, either concurrently or sequentially][182]. Governance involves a group or community of people who share access to and/or use of the resource and who manage their behaviour via an established set of formal and informal rules and norms".[183]

The same argument is made by Ostrom, whose body of work has shed a whole new light on the commons.[184] She points out that the world is more complex than the presentation that is made of it by the three models mentioned above (the tragedy of the commons, the prisoner's

---

[175] A. Chaigneau, "Propriété collective", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 955.
[176] G. Salord, "Propriété commune", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 961; Y. Emerich, "Propriété exclusive ou exclusivité", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 980-981; I. Durant, *Droit des biens*, Bruxelles, Larcier, 2017, p. 156.
[177] U. Mattei and A. Quarta, *The Turning Point in Private Law, op. cit.*, p. 13.
[178] *Res nullius* are however "open to exclusive rights" and are thus a "property-to-be and anyone who uses it first, by taking hold thereof will thereby gain an exclusive right of property" (S. Dusollier, "The commons as a reverse intellectual property - from exclusivity to inclusivity", *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 266).
[179] J. Bart, "Res communes omnium, res nullius, res publicae, res universatis", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 1052; I. Durant, *Droit des biens, op. cit.*, p. 20-21 and 180; Article 714 of the Napoleonic Code.
[180] D. Bollier and S. Helfrich, *Free, Fair and Alive, op. cit.*, p. 16.
[181] *Ibidem*.
[182] M. Madison, "Tools for Data Governance", *Technology and Regulation*, 2020, p. 33, fn 32.
[183] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *Legal Studies Research Paper Series: Working Paper No. 2018-39*, December 2018, available at http://ssrn.com/abstract=3300348, p. 3.
[184] E. Ostrom, *Governing the Commons, op. cit.*

dilemma and the logic of collective action[185]).[186] Admittedly, these models could be true in certain scenarios, namely "when conditions in the world approximate the conditions assumed in the models, observed behaviours and outcomes can be expected to approximate predicted behaviours and outcomes".[187] However, without being inherently wrong, these models rely on extreme assumptions rather than on general theories.[188] Ostrom, in fact, goes on to demonstrate that some groups of individuals can break free from the commons dilemma when managing "common-pool resources"" (hereafter "CPR").[189]

In her work, Ostrom defines a CPR as "a natural or man-made *resource system* that is sufficiently large as to make it costly (but not impossible) to exclude potential beneficiaries from obtaining benefits from its use".[190] Resource systems are "stock variables that are capable, under favourable conditions, of producing a maximum quantity of flow variable without harming the stock or the resource system itself".[191] It is crucial to distinguish these resource systems from the *resource units*, which are "what individuals appropriate or use from resource systems".[192] The process of withdrawing resource units from a resource system is called "appropriation", and "as long as the average rate of withdrawal does not exceed the average rate of replenishment, a renewable resource is sustainable over time".[193]

31. This concept of "appropriation" is fundamental to understand, as it distinguishes a CPR from a public good, which nobody is prevented from using.[194] Indeed, it is only the resource system, and not the resource units withdrawn from the system, that are jointly used (everyone is free to fish, but once a fish is caught, it is appropriated by that person).[195] This is an important finding because it contrasts with the classic "open/closed binary", which limits individuals to two choices: either they retain private ownership or they give it away.[196] As pointed out by Bollier and Helfrish:

> *"*Given this binary, it is not surprising that many people conflate "openness" with the commons, and conclude that its general, defining feature is that everything is free for the taking, at no cost. This is absolutely not true. The point of a commons is to maximize shared control and benefits, a goal that requires thoughtful rules for access and use. Openness can work only when the resource being used is nonrivalrous – i.e., it is not depleted when used and shared, such as digital information. (...) But for rivalrous natural resources that can be used up, successful commons set limits on usage, restrict access at certain periods of time, or for certain people, etc".[197]

---

[185] See point 28.
[186] E. Ostrom, *Governing the Commons, op. cit.*, p. 183.
[187] *Ibidem*.
[188] *Ibidem*.
[189] *Ibid*., p. 21.
[190] *Ibid*., p. 30.
[191] *Ibidem*.
[192] *Ibidem*.
[193] *Ibidem*.
[194] *Ibid*., p. 32.
[195] *Ibid*., p. 31.
[196] D. Bollier and S. Helfrich, *Free, Fair and Alive, op. cit.*, p. 71.
[197] *Ibid*., p. 71.

Therefore, sharing should not be confused with absolute openness. Rather, "open" and "closed" are merely two extremes of a wider spectrum of possible sharing and access rules.[198] This is clearly outlined in Ostrom's design principles of enduring and self-governing CPR institutions, which notably rely on clearly defined boundaries and on appropriation rules.[199]

32. In light of the above, it becomes clear that concepts such as "property" or "ownership", on the one hand, and "sharing" or "commons", on the other hand, should not be opposed so strongly. Indeed, commons can be subject to ownership, as illustrated by numerous examples provided by Ostrom[200], and can thus be subject to a form of appropriation or reservation, but, importantly, this does not lead to the exclusion of others.[201] Rather, commons are a form of ownership that organise the collective and shared use of a resource.[202] To some extent, they reflect a form of "inclusive property", as opposed to "exclusive property", which can be defined as a "legal relationship between a person and a good, which is characterised, on the one hand, by the absence of a power to exclude – numerous people being included in the use of the good –; and, on the other hand, by the necessarily collective use of the good, as opposed to the individualism of use generally permitted by exclusive property".[203] Commons, and other forms of sharing, are thus situated somewhere along a continuum between absolute exclusive property/ownership, on the one hand, and the absence of any form of property/ownership (public good/free-for-all), on the other hand.

Without entering into too much detail, as this is not the core focus of the thesis, it is worth mentioning several forms of property/ownership that can be found along this continuum. One example is collective property, where individuals having exclusive property over a specific good are required to cooperate in order to preserve and maintain a resource of which their good is a sub-part (e.g. an apartment in a building), or where separate individuals having exclusive property over goods decide to group them together in order to pursue a common goal through the collective management of the grouped goods.[204] Another example is common property, where a plurality of people share an ownership right on a resource.[205] The difference between common and collective property is that, in the former case, a same right on a resource is shared between multiple individuals, while in the latter case each individual

---

[198] *Ibid*., p. 69.
[199] E. Ostrom, *Governing the Commons, op. cit.*, p. 90.
[200] See, for instance, the examples of the village of Törbel in Switzerland (E. Ostrom, *Governing the Commons, op. cit.*, p. 61-65), of the Hirano, Nagaike and Yamanoka villages in Japan (*ibid*., p. 65-69), and of the huerta irrigation institutions in Spain (*ibid*., p. 69-82), which testify of the "side-by-side existence of private property and communal property in settings in which the individuals involved have exercised considerable control over institutional arrangements and property rights" (*ibid*., p. 61).
[201] S. Dusollier, "Du commun de l'intelligence artificielle", *Penser le droit de la pensée. Mélanges en l'honneur de Michel Vivant*, Paris, Dalloz, 2020, p. 116.
[202] *Ibidem*.
[203] S. Dusollier et J. Rochfeld, "Propriété inclusive ou inclusivité", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 986 (author's own translation). On this concept of "inclusive property", see also S. Dusollier, "The commons as a reverse intellectual property - from exclusivity to inclusivity", *op. cit.*, p. 258-281; and G. Van Overwalle, "Inventing Inclusive Patents: From Old to New Open Innovation", *Kritika: Essays on Intellectual Property*, P. Drahos, G. Ghidini and H. Ullrich (ed.), Vol. 1, Cheltenham, Edward Elgar, 2015, p. 206-277.
[204] See A. Chaigneau, "Propriété collective", *op. cit.*, p. 954-957.
[205] See G. Salord, "Propriété commune", *op. cit.*, p. 960-964.

has its own exclusive right on a good that forms a sub-part of a resource managed collectively.[206] Importantly, such common property does not prevent the possibility to exclude third parties from using the resource, but the difference with exclusive property, as it is traditionally conceived, is that in this case, the power to exclude belongs to a group of people and not to a single individual (exclusivity must not be confused with individuality).[207] However, in its most extreme form, collective property belongs to everyone (*res communes omnium*), in which case no one can be excluded from the use of the resource (e.g. air or light).[208] A last interesting example is the concept of "Common goods" (*beni comuni*) in Italy, which has been developed by Mattei, Reviglio and Rodotà.[209] These are "things that are functional to the exercise of fundamental rights and to a free development of human beings (…) [such as] rivers, streams, spring waters, lakes and other waters; the air; national parks as defined by the law; forests and wooden areas; mountain areas at a high altitude, glaciers and perpetual snows; seashores and coasts established as natural reserves; protected wildlife; archaeological, cultural and environmental goods".[210] According to these authors, the legal system should safeguard these resources, should guarantee their collective fruition to benefit the future generations, and should ensure that everyone is entitled to the jurisdictional protection of these resources.[211]

b) Balance between exclusive use of and access to/sharing of intangible resources (information and knowledge)

33. In transitioning from considerations on sharing *tangible* resources to considerations pertaining to the sharing of *intangible* resources, it is important to point out that a large share of Ostrom's research on the commons focused on *tangible* (natural/biophysical) resources, which fit Ostrom's definition of a CPR.[212] *Intangible* resources, such as information and knowledge, on the other hand, do not fit this definition because, by essence, they are non-rivalrous, non-excludable and non-depletable.[213] This has led to the development of "knowledge commons", which are "an institutional approach (commons) to governing the production, use, management, and/or preservation of a particular type of resource (knowledge)".[214]

Intangible resources are non-rivalrous because their consumption by one person does not diminish the amount of the resource that can be consumed by others (multiple people can use

[206] *Ibid*., p. 961.
[207] *Ibid*., p. 962-964.
[208] J. Bart, "Res communes omnium, res nullius, res publicae, res universatis", *op. cit.*, p. 1052; I. Durant, *Droit des biens*, *op. cit*., p. 20-21.
[209] U. Mattei, E. Reviglio and S. Rodotà (eds.), *Invertire la rotta. Idee per una riforma della proprietà pubblica*, Bologna, Il Mulino, 2007; U. Mattei, E. Reviglio and S. Rodotà (eds.), *I beni pubblici. Dal governo democratico dell'economia alla riforma del codice civile*, Rome, Accademia Nazionale dei Lincei, 2010.
[210] F. Cortese, "What are common goods (beni comuni)? Pictures from the Italian debate", *Revista da Faculdade de Direito da UFMG – N° Especial 2nd Conference Brazil-Italy*, 2017, p. 125-126.
[211] *Ibid*., p. 126.
[212] M. Madison, "Tools for Data Governance", *op. cit.*, p. 35.
[213] *Ibidem*.
[214] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 2.

the resource at the same time).[215] Tangible resources, on the contrary, are rival because their use by one person prevents others from using them at the same time (if a person drives a car, nobody else can drive that car at the same time). Moreover, intangible resources are, by essence, non-excludable because "it is either impossible to exclude non-payers (free-riders) from using the [resource], or the costs for such exclusion are so high that it would be inefficient to exclude".[216] Indeed, in light of their intangible nature, information and knowledge do not have physical boundaries and their duplication can be made at very low cost, having as a consequence that the "marginal costs of exclusion are often greater than the marginal costs of provision, so it is inefficient to spend resources to exclude non-payers".[217] Finally, intangible resources are non-depletable because their use does not affect their existence, although it may affect their value.[218]

1. The underproduction problem

34. Although intangible resources have different characteristics than tangible resources[219], legal scholars have often assimilated the above-described "tragedy of the commons" metaphor to problems pertaining to the creation and circulation of intangible resources such as information and knowledge.[220] This is because intangible resources are conventionally conceived as (free-for-all) public goods, due to their non-excludable and non-rivalrous nature.[221] Yet, assimilating such a metaphor to the realm of intangible goods presents an inherent problem, as it pertains to depletable resources, while, as indicated above, information and knowledge are non-depletable.[222]

Therefore, the basic social dilemma to be solved will not be a classic "tragedy of the commons" overconsumption problem.[223] Rather, it is a free-rider dilemma leading to an underproduction problem, as the prospect of free-riders may discourage the creators from producing intangible resources, in light of their potential inability to generate returns on investments.[224] As will be outlined below, this free-rider problem is also a key concern raised in the debates pertaining to compulsory B2B data sharing.[225]

Because this leads to an underproduction – rather than an overconsumption – issue, the key concern is not to regulate the use of the resource, but rather to ensure that it is created in the

---

[215] M.A. Carrier, "Limiting copyright through property", *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 196.
[216] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age: The limits of the analysis*, London, Routledge, 2013, p. 59.
[217] *Ibidem*. It is key to mention here that in some cases the costs of exclusion may be lower than the costs of provision, making the access to the information excludable. See point 41.
[218] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34.
[219] It should however be noted that some tangible resources, such as the energy that can be derived from the sun or the wind, are non-depletable and, therefore, have similar characteristics than intangible resources (non-excludable and non-rivalrous).
[220] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34.
[221] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 5.
[222] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34.
[223] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 9-10.
[224] *Ibidem*; N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 60.
[225] See below point 55.

first place.[226] Legal scholars' solution to this problem has been the creation and assignment of marketable exclusive property rights on these intangible resources, namely intellectual property rights such as patents or copyright.[227]

35. Naturally, one might question whether it makes sense to apply the concept of "property" to both tangible and intangible resources, notably in light of the non-rivalrous and non-depletable nature of intangible resources, which is an essential difference with tangible resources.[228] In this regard, it should be reminded here that the dominant legal paradigm for tangible goods is the idea of "property as exclusion".[229] Such a paradigm can indeed, as a matter of legal technique, be translated to intangible goods through the assignment of exclusive (intellectual) property rights. As summarised by Dreier, the common point between "property" on tangible and intangible resources "is the aim of providing the legal basis to enable the right holder to exclude others from using the particular [resource] in question. (…) In other words, if any similarity attaches, it is only at the level of the formulation of the exclusivity of rights".[230] Whether this importation of the "property as exclusion" paradigm from tangible to intangible goods is justified is another question, to which this thesis now turns.

2. The advent of intellectual property (IP) rights as a solution to the underproduction problem

36. As outlined above, the allocation of exclusive (intellectual) property (IP) rights has been the legal scholars' response to the underproduction problem of intangible resources. Such a response did not emerge out of the bloom. It is the result of a balancing exercise between the need to incentivise the creation of intangible goods in order to avoid the underproduction problem, on the one hand, and the importance of ensuring the largest dissemination of information and knowledge for the benefit of society, on the other hand.[231] Indeed, the non-

---

[226] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34.
[227] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 5.
[228] T. Dreier, "How much "property" is there in intellectual property? The German civil law perspective", *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 127.
[229] See point 29.
[230] T. Dreier, "How much "property" is there in intellectual property?", *op. cit.*, p. 127.
[231] See, *inter alia*, N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age*, *op. cit.*; D. Halbert, *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*, Westport, Quorum books, 1999; P. Chrocziel and W. Prinz zu Waldeck und Pyrmont, "Introduction", *Intellectual Property and Competition Law*, P. Chrocziel, M. Lorenz and W. Prinz zu Waldeck und Pyrmont (ed.), Alphen aan den Rijn, Kluwer, 2016, p. 1-32; P. Régibeau and K. Rockett, "The relationship between intellectual property law and competition law: an economic approach", *The Interface between Intellectual Property Rights and Competition Policy*, S. Anderman (ed.), Cambridge, Cambridge University Press, 2007, p. 505-552; A. Flanagan and M. Montagnani, "Intellectual property law: economic and social justice perspectives: introduction", *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. x-xviii; G. Ramello, "Intellectual property, social justice and economic efficiency: insights from law and economics", *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. 1-23; F. Morando, "Copyright default rule: reconciling efficiency and fairness", *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. 24-43; S. Sandeen, "The value of irrationality in the IP equation", *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. 44-65; D.

rivalrous nature of information and knowledge implies that there is no social loss associated with their usage, because others are not deprived from using them as well.[232] Because everyone can use information and knowledge simultaneously, it is in the general interest to ensure that it is used by as many people as possible, as this will nurture the human capital that will subsequently contribute to the production of more information and knowledge.[233] In more economic terms, the consumption of information and knowledge generates positive externalities, and "there is a benefit in their widest possible usage in order to maximize welfare in society and as a basis for further innovation".[234]

One important aspect of this balancing exercise must be underlined from the outset, namely that exclusive intellectual property rights are not granted on information/knowledge as such, but rather solely on the concrete way in which they have been expressed by the IP right holder. For instance, a copyright holder is only granted exclusive rights pertaining to the specific material form in which the work has been fixed.[235] The ideas underlying the work, on the other hand, are not protected.[236] This idea/expression dichotomy is fundamental and well-established.[237] Similarly, a patent holder is only granted exclusive rights on the concrete product or process that she has invented, which must be specified in the forms of "claims" that define the invention for which the patent is sought and determine the scope of the exclusive rights, and not on the idea(s) underlying the invention.[238] This balance is fundamental, as it does not prevent the wide dissemination of information and knowledge as

---

Voorhoof, "Freedom of expression and the right to information: Implications for copyright", *Research Handbook on Human Rights and Intellectual Property*, C. Geiger (ed.), Cheltenham, Edward Elgar, 2015, p. 331-353; L. Helfer, "Mapping the interface between human rights and intellectual property", *Research Handbook on Human Rights and Intellectual Property*, C. Geiger (ed.), Cheltenham, Edward Elgar, 2015, p. 6-15; B. Martens, "An economic perspective on data and platform market power", *JRC Digital Economy Working Paper 2020-09*, February 2021, available at https://www.researchgate.net/publication/349179464.

[232] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age*, *op. cit.*, p. 61.

[233] *Ibidem*.

[234] *Ibidem*. See also P. Régibeau and K. Rockett, "The relationship between intellectual property law and competition law", *op. cit.*, p. 509.

[235] Berne Convention for the Protection of Literary and Artistic Works, 9 September 1886, as amended on 28 September 1979, article 2.2. See also Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ L 122/42*, 15 May 1991, article 1.2.

[236] Agreement on Trade-Related Aspects of Intellectual Property Rights, contained in Annex 1C to the Agreement establishing the World Trade Organisation (WTO), Marrakesh, 15 April 1994, article 9.2; See also Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ L 122/42*, 15 May 1991, article 1.2.

[237] See, inter alia, F. De Visscher et B. Michaux, *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000, p. 9; B. Michaux, "Diffusion du savoir: droit d'auteur et Internet", *L'Europe des droits de l'homme à l'heure d'Internet*, Q. Van Enis et C. de Terwangne (dir.), Bruxelles, Larcier, 2019, p. 492-493; E. Derclaye, "Introduction", *Research Handbook on the Future of EU Copyright*, E. Derclaye (ed.), Cheltenham, Edward Elgar, 2009, p. 3; T. Aplin, "Subject matter", *Research Handbook on the Future of EU Copyright*, E. Derclaye (ed.), Cheltenham, Edward Elgar, 2009, p. 50, 59 and 64; A. Quaedvlieg, "Overlap/relationships between copyright and other intellectual property rights", *Research Handbook on the Future of EU Copyright*, E. Derclaye (ed.), Cheltenham, Edward Elgar, 2009, p. 493; R. Burrel and A. Coleman, *Copyright Exceptions: The Digital Impact*, Cambridge, Cambridge University Press, 2005, p. 20-24.

[238] Agreement on Trade-Related Aspects of Intellectual Property Rights, contained in Annex 1C to the Agreement establishing the World Trade Organisation (WTO), Marrakesh, 15 April 1994, article 27.1; Code de droit économique, article XI.3; M. Fisher, *Fundamentals of Patent Law: Interpretation and Scope of Protection*, Oxford, Hart Publishing, 2007, p. 1; M. Buydens, *Droits des brevets d'invention*, 2e éd., Bruxelles, Larcier, 2020, p. 87-89.

such, which is in the general interest and generates positive externalities. Accordingly, when, in the following lines, this thesis refers to intellectual property rights on information and knowledge, this must be understood within the limits formulated in this paragraph.

37. The paragraphs above reflect the dominant approach to the justification of the creation and allocation of IP rights, namely the *incentive theory*.[239] This economic discourse of the *incentive theory* became globally dominant over the years as it was perceived as more objective than alternative theories, such as the *natural rights* theory[240] (human beings have an unconditional "ownership" right on the result of their labour and there is a moral duty to protect their creations) and the *reward* theory[241] (a creator/inventor should be rewarded for contributing to the public knowledge by disclosing a creation/invention). Indeed, the latter theories were seen as more relativist due to their reliance on moral considerations.[242] On the contrary, the incentive theory is not concerned with the more ethical question of whether "the scope of the granted rights is "just" in respect of the contribution made by the [creator/inventor]".[243] Rather, the incentive theory is purely utilitarian in the sense that it provides that IP rights are granted "to incentive certain desirable behaviour that would otherwise not occur".[244]

This theory is the direct result of the "underproduction" problem presented above[245], as it alleges that without (intellectual) "property" rights, information and knowledge would not be produced, due to the fear of free-riding.[246] As explained by Elkin-Koren and Salzberger, this theory "views information [and knowledge] as public goods that bring about a market failure, and thus require central intervention by granting IP rights. The goal, according to this approach, is to design laws, which will maximize society's welfare or wellbeing".[247]

38. One of the core assertions behind the incentive theory is that IP rights are the cheapest and most effective way for society to incentivise these desired behaviours of creation/invention.[248] Yet, IP rights come at a cost, as they create monopolies on, and barriers to, access to pre-existing creations/inventions, which can themselves stifle future creation and innovation.[249] In a way, the "public good" market failure is thus replaced by a "monopoly" market failure.[250] This creates an inherent paradox because, in order to generate more knowledge for the public

---

[239] A. Flanagan and M. Montagnani, "Intellectual property law: economic and social justice perspectives", *op. cit.*, p. xi.
[240] See J. Locke, *Two Treatises of Government, op. cit*.; P. Chrocziel and W. Prinz zu Waldeck und Pyrmont, "Introduction", *op. cit.*, p. 3-4; G. Spina Ali, "Intellectual Property and Human Rights: A Taxonomy of Their Interactions", *IIC*, 2020, Volume 51, Issue 4, p. 417.
[241] See P. Chrocziel and W. Prinz zu Waldeck und Pyrmont, "Introduction", *op. cit.*, p. 4.
[242] P. Chrocziel and W. Prinz zu Waldeck und Pyrmont, "Introduction", *op. cit.*, p. 4.
[243] *Ibid*., p. 5.
[244] *Ibidem*.
[245] See point 34.
[246] See, in this regard, N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 59-60.
[247] *Ibid*., p. 11.
[248] *Ibid*., p. 57.
[249] *Ibidem*.
[250] *Ibid*., p. 88.

good, which is the ultimate goal of IP rights, exclusive rights are allocated to generate incentives to create/invent, but these rights limit the access to existing knowledge.[251]

IP policies thus struggle with a balancing act between "the social welfare costs of monopolistic exclusive rights and the social welfare gains from the innovation incentive effects".[252] Accordingly, the incentive theory treats IP rights "as an inevitable evil that must be limited to the scope [and length] necessary for serving its goal".[253] Indeed, if the incentivising regime is misconstrued and does not limit sufficiently the scope and length of these IP rights, this might inflate the price of future creations/inventions, or may even prevent their creation altogether, as it will be too costly to build on this pre-existing material and knowledge protected by IP rights.[254] In such a scenario, the benefits derived from the incentive effects might even be discounted by the increase in the information/knowledge production costs.[255]

39. This creates a challenge, for legislators, to find the right balance between these various competing interests in order to maximise the public good through a broad access to information and knowledge, while protecting the incentives of the creators/inventors, through the appropriate determination of the subject matter, the scope, the length of and the limitations to IP rights.[256] This inherent tension between incentivising creation and granting the widest possible public access to information and knowledge is reflected in the various international and European instruments where intellectual property is enshrined as a human right.[257] Indeed, these instruments aim at protecting the creators'/inventors' fundamental rights over their creations/inventions and at providing the necessary economic incentives for a thriving cultural diversity and scientific innovation, while primarily recognising the general public's right to benefit from cultural and scientific progress.[258] In this regard, the European Court of Human Rights has outlined in two judgments of 2013[259] that the application and enforcement of intellectual property rights had to be balanced with the right to freedom of information

---

[251] *Ibid*., p. 87-88.
[252] B. Martens, "An economic perspective on data and platform market power", *op. cit.*, p. 23.
[253] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age*, *op. cit.*, p. 61.
[254] *Ibid*., p. 62.
[255] G. Ramello, "Intellectual property, social justice and economic efficiency", *op. cit*., p. 13.
[256] P. Chrocziel and W. Prinz zu Waldeck und Pyrmont, "Introduction", *op. cit.*, p. 8.
[257] Article 27 of the Universal Declaration of Human Rights, signed in Paris on 10 December 1948; Article 15.1.b) and c) of the International Covenant on Economic, Social and Cultural Rights, 16 December 1966; Article 1 of Protocol n° 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Paris on 20 March 1952; Article 17.2 of the Charter of Fundamental Rights of the European Union, *OJ C 326/391*, 26 October 2012. See G. Spina Ali, "Intellectual Property and Human Rights", *op. cit.*, p. 411–445.
[258] G. Spina Ali, "Intellectual Property and Human Rights", *op. cit.*, p. 414-417. See also L. Helfer, "Mapping the interface between human rights and intellectual property", *op. cit.*, p. 12-13.
[259] ECtHR, *Ashby Donald and Others v. France*, 10 January 2013, App. No. 36769/08; ECtHR, *Neij and Kolmisoppi v. Sweden*, 19 February 2013, App. No. 40397/12.

enshrined in Article 10 of the European Convention on Human Rights[260], which also encompasses a right of access to information.[261]

3. Questioning the underproduction problem and the IP answer to it

40. IP rights have thus been created in order to solve the alleged "underproduction" problem of intangible goods presented above[262], according to which information and knowledge would not be produced, due to the fear of free-riding, unless exclusive (intellectual) "property" rights are granted on these intangible resources in order to incentivise their creation.[263] However, the existence of this "underproduction problem", and/or of the appropriateness of the IP answer to it, are being questioned.

i. Is there really an underproduction problem?

41. The rationale behind the underproduction problem is the "public good market failure", namely that, because intangible goods are non-rivalrous and non-excludable, this will lead to their underproduction. However, as pointed out by Madison *et al*., "knowledge-generating institutions based on successful coordination and collaboration among knowledge producers and users have existed for centuries, often despite the absence of IP rights owned by individual creators or inventors".[264] For instance, they outline that "universities have long served as knowledge-generating and knowledge-sustaining institutions despite faculty researchers often exercising few conventional market-based IP interests".[265]

In spite of this finding, the narrative of the underproduction problem remains strongly used by right holders as a rhetorical justification for the superiority of the rationale of exclusion over the rationale of access/sharing, especially in the advent of digital technologies that facilitate the reproduction and dissemination of their creations/inventions.[266] Yet, these technological changes that have occurred, mostly in the digital environment, could actually be used to formulate a contradictory argument to that of the right holders. Indeed, although these evolutions enable easier reproduction and dissemination of creations/inventions, they also enable much easier and cheaper technical exclusion of the access to them, which could thus question the "public good market failure" premise, as large fractions of information and knowledge may now be made excludable through technical, as well as contractual, means.[267]

---

[260] D. Voorhoof, "Freedom of expression and the right to information", *op. cit.*, p. 331; L. Helfer, "Mapping the interface between human rights and intellectual property", *op. cit.*, p. 7.
[261] ECtHR, *Youth Initiative for Human Rights v. Serbia*, 25 June 2013, App. No. 48135/06, §§ 20 and 24; D. Voorhoof, "Freedom of expression and the right to information", *op. cit.*, p. 337. See also C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 555-579.
[262] See point 34.
[263] See, in this regard, N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 59-60.
[264] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 5.
[265] *Ibidem*.
[266] T. Dreier, "How much "property" is there in intellectual property?", *op. cit.*, p. 132; J. Waldron, "From Authors to Copiers: Individual Rights and Social Values in Intellectual Property", *Chi.-Kent L. Rev*., 1993, Vol. 68, p. 851.
[267] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 77.

This could be especially problematic if the access to information or knowledge that are not covered by exclusive IP rights is technically or contractually excluded (e.g. information and knowledge falling out of the scope of these rights;[268] or information and knowledge falling within the scope of the exceptions to these rights).[269]

42. Alternatively, even if these technological developments were not deemed to be sufficient to tackle the non-excludability issue, some authors have outlined that monetary incentives, deriving from the granting of exclusive IP rights, are not the only way to stimulate creation/innovation.[270] For them, the assumption that monetary incentives are necessary to induce creation/innovation relies on shaky grounds, as there is limited empirical evidence to support the claim that people will not create/invent if they are not promised some financial profits in return.[271] In fact, some empirical evidence suggests that monetary incentives may actually sometimes undermine people's motivation to create/invent.[272] Such studies show that offering monetary rewards may make people less creative as their free-choice is undermined due to performance constraints[273], or could reduce the quality of their work[274].[275] Moreover, it is practically impossible to determine the desirable or optimal level of incentives that should be aimed for, and, consequently, it is extremely complex to tailor IP rights perfectly (in terms of scope, duration, exceptions, etc.) in order to achieve this optimum.[276]

Rather, these authors outline that there are also many non-monetary motivations that incentivise people to create/invent, such as the natural drive to create/invent, the need to express ideas or talents and to be acknowledged for it, or the wish to gain recognition among peers or the general public.[277] These can be intrinsic (self-oriented) motivations and/or social motivations (other-oriented).[278] To give a famous example, when Dr. Jonas Salk was asked in 1955 who owned the patent to the polio vaccine that he had just co-created, he answered: "Well, the people I would say. There is no patent. Could you patent the sun?[279]".[280]

---

[268] On this limit, see point 36. See also A. Quaedvlieg, "Overlap/relationships between copyright and other intellectual property rights", *op. cit.*, p. 493.
[269] On this issue for the *sui generis* database right, see points 58 to 60.
[270] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 11; see also A. Flanagan and M. Montagnani, "Intellectual property law: economic and social justice perspectives", *op. cit.*, p. x-xviii.
[271] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 65.
[272] *Ibid*., p. 66.
[273] E. Deci, R. Koestner and R. Ryan, "A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation", *Psychological Bulletin*, 1999, Volume 125, Issue 6, p. 627–668.
[274] A. Kohn, *Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, A's, Praise, and Other Bribes*, Boston, Houghton Mifflin, 1999, p. 136-138.
[275] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 66.
[276] *Ibid*., p. 101.
[277] *Ibid.* p. 66. On these motivational factors, see also S. Sandeen, "The value of irrationality in the IP equation", *op. cit.*, p. 44-65.
[278] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 66-67.
[279] CBS Television interview with Salk, *See It Now*, 12 April 1955, quoted in J. Cohen, *Shots in the Dark: The Wayward Search for an AIDS Vaccine*, New York, W.W. Norton, 2001.
[280] D. Bollier and S. Helfrich, *Free, Fair and Alive, op. cit.*, p. 227.

To conclude on this critique, it can also be added that some argue that creation and innovation are, in any case, profitable even without the granting of exclusive (intellectual) "property" rights, as first-mover advantages and "lead time" (although this lead time might be short-lived in the digital age) are alternative considerations that offset the lower production costs of free-riders.[281]

ii. Even if there is an underproduction problem, are IP rights the adequate solution?

43. Even if the dominant assumption that intangible goods face an underproduction problem was deemed to be correct[282], some have questioned whether exclusive (intellectual) "property" rights are the adequate solution to tackle it. Or rather, they question whether the balance struck in the past by IP rights is still optimal today, as our society increasingly relies on information and knowledge, which might entail the need to review the existing balance in favour of more access than what is currently allowed under the IP rights system.[283]

To support their argument, these authors allege that IP rights have enabled right holders to exclude the use of information and knowledge far beyond the economic incentive purposes that they were designed to serve, and that these rights have actually become a major tool to expand market power, reduce competition and concentrate the control over the production and distribution of information and knowledge.[284] Taking the example of copyright, Halbert argues that it is "a socially constructed discourse that has become a powerful social myth".[285]

Moreover, because knowledge heavily relies on sharing processes, overly extensive appropriation of it through strong IP rights will inexorably reduce the amount of access to it and will produce an adverse outcome for overall efficiency.[286] On the contrary, a weaker form of appropriation generates positive effects on knowledge production, as it will imply "lower productive costs for follow-on creators, wider access to knowledge, and the possibility of free-riding, understood as unpaid access to knowledge for a considerable amount of individuals. Stated differently, *efficiency in the knowledge domain requires the preservation of broad access*" (emphasis added).[287] In fact, some argue that the benefits from information and knowledge disclosure should be more strongly seen as important values in their own right, rather than merely as counter-weights to the granting of appropriation rights.[288] Taking the example of copyright, Morando argues that weaker forms of appropriation, such as the Creative Commons licences, are preferable default rules in terms of efficiency, fairness and

---

[281] *Ibid*., p. 62 and 69.
[282] For the purpose of this thesis, we do not believe that it is necessary to take a definitive stance on this issue.
[283] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 58.
[284] *Ibid*., p. 90. See also P. Régibeau and K. Rockett, "The relationship between intellectual property law and competition law", *op. cit*., 2007, p. 505-552.
[285] D. Halbert, *Intellectual Property in the Information Age, op. cit.*, p. 2. See also p. xi and xv.
[286] G. Ramello, "Intellectual property, social justice and economic efficiency", *op. cit*., p. 2-3.
[287] *Ibid*., p. 17.
[288] S. Sandeen, "The value of irrationality in the IP equation", *op. cit.*, p. 57.

social justice than the current copyright "default rule" (e.g. full protection – "All rights reserved").[289]

To summarise these authors' positions, they invite to reconsider the existing balance at the basis of exclusive (intellectual) "property" rights, because the costs, for society, of exclusion of information and knowledge through IP rights have grown, while society increasingly depends on the access to it. As outlined above, this notably derives from the fact that the access to large fractions of information and knowledge that are not covered by exclusive IP rights may now be technically or contractually excluded.[290]

c) The rationale for sharing intangible resources

44. In light of the above, it is apparent that the classic solution to the "exclusion v. access/sharing balance" is increasingly challenged, mainly for intangible resources.[291] Indeed, growing calls for a wider sharing of information and knowledge are being made, notably on the grounds of their non-rivalrous nature.[292] In fact, two types of rationale are called upon to support this reconsideration of the classic balance, namely economic considerations on the one hand, and more societal considerations, on the other hand. Because data are also non-rivalrous and non-depletable[293], the rest of this Section will focus on the rationale for sharing intangible resources, as these might suffer (like data) from an underproduction problem, rather than from the overconsumption problem of tangible goods.[294]

1. Economic rationale for sharing intangible resources

45. To a large extent, the economic rationale for sharing intangible resources has already been outlined above, in the discussion pertaining to the existence of the "underproduction problem" and of the appropriateness of the IP answer to it.[295] The key argument is that there is no social loss incurred by to the use of intangible resources, in light of their non-rivalrous character.[296] As outlined by Ramello, "efficiency in the knowledge domain requires the preservation of broad access", as it will lower the production costs for follow-on creation/innovation, while overly extensive exclusive rights will reduce the access to it and will produce an adverse outcome for overall efficiency.[297] This economic rationale has also been brilliantly explained in Benkler's work on the "networked information economy"[298], which will be briefly summarised here.

---

[289] F. Morando, "Copyright default rule: reconciling efficiency and fairness", *op. cit.*, p. 25-27.
[290] See point 41. N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 77.
[291] See Part I, Chapter 2, Section A, b), 3. "Questioning the underproduction problem and the IP answer to it".
[292] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 61.
[293] See point 52.
[294] See point 34. M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 9-10.
[295] See Part I, Chapter 2, Section A, b), 3. "Questioning the underproduction problem and the IP answer to it".
[296] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 61.
[297] G. Ramello, "Intellectual property, social justice and economic efficiency", *op. cit*., p. 2-3; 17.
[298] Y. Benkler, *The Wealth of Networks. How Social Production transforms Markets and Freedom*, New Haven, Yale University Press, 2003.

46. The more widely information and knowledge are diffused and shared, the more benefits it will generate for society. This has led to the establishment of a balance between static and dynamic efficiency.[299] Indeed, from a static perspective, the most efficient approach for society's overall welfare would be to ensure the broadest access to/sharing of information and knowledge possible, by limiting exclusive rights on it.[300] However, from a dynamic perspective, creators/innovators may refrain from generating this information/knowledge if they know that they will have to share it freely with anyone.[301] Therefore, under the classic approach, some static inefficiency is traded-off to achieve dynamic efficiency, i.e. exclusive rights are granted to creators/inventors so they can charge positive prices for resources that have a zero marginal cost[302], in order to incentivise them to create/invent.[303] Allegedly, the result of this balance will be to generate more information and knowledge over time, which will "outweigh the inefficiency at any given moment caused by selling the information at above its marginal cost".[304]

47. Yet, Benkler points out that there is in fact remarkably little support, both in theory and in empirical evidence, for such an approach of the information and knowledge production.[305] On the contrary, because information is non-rivalrous and because it is both an input and an output of its own production process, it is economically detrimental to excessively exclude the access to / sharing of it.[306] Indeed, because any new informational resource builds on pre-existing information and knowledge, granting strong exclusive rights on this prior information and knowledge will increase the price of new information production, which can lead to both static and dynamic inefficiency, as "we will not only have too little consumption of information today, but also too little production of new information for tomorrow".[307] Moreover, the high price for new information production deriving from strong exclusive rights will also drive concentration in the information production process.[308]

48. In light of the above, Benkler argues that it is more efficient for information and knowledge to be shared, and that the costs to do so have dramatically declined with the advent of the "networked information economy".[309] Indeed, the "networked information economy" has widely distributed the high-capital costs that were necessary for information production and sharing, which, in turn, has reduced the access barriers to information and allows for much more non-market decentralised models of information production and sharing that do not depend on proprietary strategies.[310]

---

[299] *Ibid*., p. 36.
[300] *Ibid*., p. 37.
[301] *Ibidem*.
[302] The cost of reproducing and sharing the resource is zero.
[303] Y. Benkler, *The Wealth of Networks, op. cit.*, p. 37.
[304] *Ibidem*.
[305] *Ibid*., p. 39.
[306] *Ibid*., p. 37-38.
[307] *Ibid*., p. 38.
[308] *Ibid*., p. 50.
[309] *Ibid*., p. 56.
[310] *Ibid*., p. 32-33. This might however not be true for all kinds of information, as there are still high costs associated with some types of information collection (e.g. satellite imagery).

While peer production of information, like Wikipedia, and peer-to-peer exchange platforms are good examples of this, the paramount example of this new paradigm is free software (or "freeware").[311] This freeware movement relies on licencing constraints, originally designed by Richard Stallman and Eben Moglen through the *Free Software Foundation*[312], which allow anyone to use the freeware on the condition that any modification of it must be distributed under the same licensing terms as the original freeware.[313] It can be seen as a formalised example of "inclusive property", as opposed to "exclusive property", as mentioned above.[314] The most well know licence in this regard is the *GNU General Public License*.[315] As the outputs of these processes are non-rivalrous resources (information and knowledge), sharing them freely is more efficient, all other things being equal, than if they were produced and shared under the classic proprietary model.[316] To summarise, the economic rationale for sharing intangible resources derives from two of their characteristics, namely that they are non-rivalrous and that they are both an input and an output of their own production process.

2. Societal rationale for sharing intangible resources

49. Next to the economic considerations outlined above, there are also more societal considerations that can justify sharing intangible resources. Once again, this mainly flows from these resources' non-rivalrous nature. Because everyone can use information and knowledge simultaneously, it is in the general interest to ensure that it is used by as many people as possible, as this will nurture the human capital that will subsequently contribute to the production of more information and knowledge.[317] This also flows from the fact that intangible resources are both an input and an output of their own production process.[318] Indeed, because the production of new information and knowledge depends on the broadest access possible to existing information and knowledge, sharing intangible resources is crucial for societal progress in all fields, whether it pertains to the preservation of human's health or living environment, to the understanding of the infinitely big or the infinitely small, or to the pursuit of other societal goals (better health, cleaner environment, etc.).

50. Yet, in practice, information and knowledge are increasingly concentrated in the hands of a few very large actors, who thus benefit from tremendous economic, political and technological power.[319] For Bollier and Helfrish, this is the natural result of a society built around capitalist markets and the narrative of individual freedom and property ownership developed by philosophers such as Descartes, Hobbes and Locke.[320] Indeed, if access to

---

[311] *Ibid*., p. 60.
[312] https://fr.wikipedia.org/wiki/Free_Software_Foundation
[313] Y. Benkler, *The Wealth of Networks, op. cit.*, p. 63.
[314] See point 32; S. Dusollier, "The commons as a reverse intellectual property - from exclusivity to inclusivity", *op. cit.*, p. 258-281; and G. Van Overwalle, "Inventing Inclusive Patents: From Old to New Open Innovation", *op. cit.*, p. 206-277.
[315] See https://www.gnu.org/licenses/gpl-3.0.en.html
[316] Y. Benkler, *The Wealth of Networks, op. cit.*, p. 107.
[317] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age, op. cit.*, p. 61.
[318] Y. Benkler, *The Wealth of Networks, op. cit.*, p. 37-38.
[319] U. Mattei and A. Quarta, *The Turning Point in Private Law, op. cit.*, p. ix and 3.
[320] D. Bollier and S. Helfrich, *Free, Fair and Alive, op. cit.*, p. 34; 88; 211.

intangible resources is regulated by the market via a "pay for access" model, this will automatically have as a consequence to provide greater access to, and control of, intangible resources to wealthier people, as their large financial means will not only allow them to pay for broader access to them, but also to invest more heavily in their creation/invention and management.[321]

Accordingly, Bollier and Helfrish call for an ontological shift (an "OntoShift" as they call it) from exclusion towards more access/sharing.[322] The rationale behind such increased sharing is that this would considerably diminish the access barriers to information and would improve everyone's equality of opportunity of access to information.[323] This fits into broader social justice and human rights considerations, as everyone has a right of access to information, which is important because it enables individuals to fully enjoy and exercise a variety of other rights (right to privacy, to education, to culture or to move freely) and to take fundamental decisions.[324] For instance, access to relevant health and environmental information has an impact on the individuals' right to privacy as it allows them to take informed decisions regarding the place where they want to live.[325] Moreover, access to mobility information such as information about public transportation schedules or traffic jams enables individuals to move freely in the most optimal way. Furthermore, broader access to/sharing of information and knowledge "creates the opportunities for greater autonomous action, a more critical culture, a more discursively engaged and better informed republic, and perhaps a more equitable global community".[326]

Once again, open source software production or peer production of knowledge can be cited as socially beneficial initiatives aiming at providing the largest access possible to information and knowledge.[327] Indeed, wide access to information through websites like Wikipedia can contribute to the individuals' right to education and culture, as they can easily obtain information about historical events, about fundamental rules and principles in all fields of social and natural sciences, about the functioning of mechanical objects and technologies, about works of arts (books, theatre plays, movies, paintings, music…), etc.

---

[321] *Ibid*., p. 72.
[322] *Ibid*., p. 29 and 72.
[323] Y. Benkler, *The Wealth of Networks, op. cit.*, p. 13-14.
[324] See C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *op. cit.*, p. 555-579.
[325] *Ibid.*, p. 573-576; ECtHR, *Guerra et al. v. Italy*, 19 February 1998, App. No. 14967/89, § 60; ECtHR, *McGinley and Egan v. United Kingdom*, 9 June 1998, App. No. 21825/93 and 23414/94, § 97 and 101; ECtHR, *Roche v. United Kingdom*, 19 October 2005, App. No. 32555/96, § 162 and 165.
[326] Y. Benkler, *The Wealth of Networks, op. cit.*, p. 92.
[327] *Ibid*., p. 32-33; D. Bollier and S. Helfrich, *Free, Fair and Alive, op. cit.*, p. 259; M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *op. cit.*, p. 4.

Section B. Economic rationale for data sharing

51. After having presented the classic balance between exclusive use of and access to/sharing of tangible and intangible resources, and the various critics pertaining to how it has been addressed, it is now time to turn towards the analysis of the same balance for data. In fact, most of the developments pertaining to intangible resources are equally applicable to data, which are also, by essence, intangible resources. Much like information and knowledge, data's value emerges when it is shared and aggregated.[328] This Section will focus on the economic rationale for data sharing, while Section C will be dedicated to the societal and "empowerment" rationale for data sharing.

a) Data's characteristics

52. Data is often presented in the policy debates as the "new oil" of our modern economy. Yet, this broadly used catchphrase is somewhat misleading as oil is both tangible and depletable, which is not the case of data, which is intangible and non-depletable, as its use does not affect its existence, although it may affect its value.[329] However, this metaphor does make some sense if one considers oil's ""infrastructural" qualities, in that it can be directed to numerous applications, with diverse values".[330] In this sense, data, much like oil, is an important component of a great number of technical and commercial applications and it "lubricates social and technical processes".[331] This is why data is, itself, sometimes characterised as an "infrastructural resource", because its use creates spill overs in multiple fields across society.[332]

According to Frischmann, infrastructural resources "are "shared means to many ends", which satisfy the non-rivalrous, the capital good and the general-purpose criteria".[333] First, data are a non-rivalrous resource that can be replicated and consumed by an unlimited number of actors – even simultaneously –, and "maximising access to the non-rivalrous [resource] will in theory maximise social welfare, as every additional private benefit comes at no additional cost".[334] Second, data is often a capital resource, which means that it is used as an input for goods or services rather than as an end it itself. This is because data often has no intrinsic value, as the value will derive from the use made of this data in order to extract information or knowledge. As data are a non-rival capital resource that "can in theory be used (simultaneously) by multiple users for multiple purposes as an input to produce an unlimited number of goods and services"[335], data access and sharing is highly valuable. Third, data may

---

[328] M. Madison, "Tools for Data Governance", *Technology and Regulation*, 2020, p. 29.
[329] M. Madison, "Tools for Data Governance", *op. cit.*, p. 31 and 34; M. Stucke and A. Grunes, *Big Data and Competition Policy*, Oxford, Oxford University Press, 2016, p. 44-45.
[330] M. Madison, "Tools for Data Governance", *op. cit.*, p. 31.
[331] *Ibidem*.
[332] *Ibid*., p. 40.
[333] B. Frischmann, *Infrastructure: The Social Value of Shared Resources*, Oxford, Oxford University Press, 2012, cited in OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications, 2015, available at https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm, p. 179.
[334] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 179-180. See also N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age: The limits of the analysis*, London, Routledge, 2013, p. 61.
[335] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 180-181.

be described as a general-purpose resource. Indeed, data could, in theory, be used for an unlimited number of purposes, including not only economic but also public and social purposes, and additionally, the use of data for one purpose can provide valuable insights for uses in other domains, thus having significant spill over effects.[336]

53. On the other hand, whether data should be considered as an excludable or non-excludable resource is less clear.[337] Indeed, even if data is arguably non-excludable by nature[338], in practice, data is both technically and contractually excludable.[339] Regarding technical excludability, it has already been outlined that technological changes in the digital environment enable much easier and cheaper technical exclusion of the access to intangible resources such as information and knowledge[340], and this equally applies to data. Data holders can set technical safeguards in order to ensure that third parties will not be able to access their data. They can also technically ensure that the data they hold remains secret in order, for instance, to benefit from the protection granted to trade secrets.[341] Moreover, data holders can contractually exclude the access to (some of) their data. In fact, as pointed out by Stucke and Grunes, "data's competitive significance (and value) arise in part from the ability of firms to exclude others from access and analysing it as quickly".[342]

54. Therefore, in light of data's potentially excludable character, it can be argued that data is not a public good, which is non-rivalrous and non-excludable, but is better depicted as a "club good", which is non-rivalrous but excludable.[343] This is an important finding because it means that the "public good market failure", that is at the basis of the justification of the creation of exclusive (intellectual) "property" rights to avoid the "underproduction problem" of intangible resources (such as information and knowledge), cannot simply be transposed to the realm of data. As will be outlined below, this has had an impact in the discussions pertaining to the creation of an "IP-like" data producer's right.[344]

55. That being said, if data holders are not able to exclude the access to their data (for instance because of data sharing obligations), the free-rider dilemma allegedly leading to the "public good market failure" and the "underproduction problem" for intangible resources (i.e. the prospect of free-riders may discourage the creators from producing intangible resources, in

---

[336] *Ibid*., p. 181-182.
[337] See also point 41 where some doubts are casted on the non-excludable nature of intangible resources such as information or knowledge.
[338] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 4.
[339] W. Kerber, "Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 118.
[340] N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age*, *op. cit.*, p. 77. See point 41.
[341] See Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157*, 15 June 2016. See point 185.
[342] M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 46.
[343] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34; M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 45.
[344] See point 63.

light of their potential inability to generate returns on investments)[345] may also surface for data. Indeed, data collection and processing, and consequently data sharing, entails costs for the data holder, and data sharing obligations might create disincentives for data collection and processing.[346] Accordingly, a balance must be found between the benefits and costs of data sharing.[347] As such balance had been solved, for intangible resources, through the means of IP rights, the question naturally emerged of whether the same balance, for data, could also be solved through (intellectual) "property" rights.

b) Are data subject to (intellectual) property rights?

56. Unsurprisingly, the strong establishment of (intellectual) property rights in our society has led to discussions on whether data should also be subject to some form of exclusive (intellectual) "property" right.[348]

1. Evolution of the debates on (intellectual) property over information towards discussions on (intellectual) property over data

57. In fact, these discussions build on older debates pertaining to "property" on information. Indeed, in the beginning of the 21st century, information, much like data today, was considered as an essential strategic resource because it was the "raw material" for important products such as databases or software, and this generated boiling discussions on the legal stakes of its potential "appropriation" by firms or people.[349] For instance, several French authors like Leclercq and Catala proposed, in the early 1980s, a theory according to which information, as such, should be considered as a good that can be subject to legal "appropriation".[350] The concept of "appropriation" is understood as another way of formulating the concept of "property", as it covers all exclusive rights on a good.[351] Indeed, according to Leclercq and Catala's theory, the "creator" of information must be considered as the owner of absolute exclusive rights on it, and should be able to exclude others from using it unduly.[352] On the contrary, others argued that there is no such principle of "appropriation/property" on information, and that this notably stems from the fact that

---

[345] M. Madison, K. Strandburg and B. Frischmann, "Knowledge Commons", *Legal Studies Research Paper Series: Working Paper No. 2018-39*, December 2018, available at http://ssrn.com/abstract=3300348, p. 9-10. See point 34.

[346] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era – Final report*"*, 2019, p. 76-77, available at http://ec.europa.eu/competition/publications/reports/ kd0419345enn.pdf.

[347] P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *Antitrust Law Journal*, 2008, n° 75, p. 616-620. For a more extensive analysis of this balance see points 89 and 90 below.

[348] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Building a European Data Economy*", Brussels, 10 January 2017, COM(2017) 9 final, p. 13.

[349] F. Dubuisson, *Existe-t-il un principe general d'appriopriation de l'information?*, Thèse de doctorat, Université Libre de Bruxelles, 2005, p. 1-2.

[350] P. Leclercq, "Essai sur le statut juridique des informations", *Les flux transfrontières de données : vers une économie internationale de l'information ?*, A. Madec (ed.), Paris, La Documentation française, 1982, p. 119-150; P. Catala, *Le droit à l'épreuve du numérique. Jus ex machina*, Paris, PUF, 1998, p. 224-263; F. Dubuisson, *Existe-t-il un principe general d'appriopriation de l'information?*, *op. cit*., p. 2.

[351] F. Dubuisson, *Existe-t-il un principe general d'appriopriation de l'information?*, *op. cit*., p. 14.

[352] *Ibidem*.

intellectual property rights such as copyright[353] and the *sui generis* database right[354] do not protect the information as such.[355]

58. Although this debate on the "property" of information will not be further analysed here in light of the scope of this thesis[356], it is worth underlining that IP rights such as copyright and the *sui generis* database right similarly do not erect a principle of "appropriation/property" on individual data either.[357] Indeed, data, as such, cannot be protected by copyright.[358] Only the particular expression of a semantic content extracted from data could be protected by copyright if the conditions for the benefit of this protection are met, such as originality.

That being said, data will rarely be apprehended as an isolated good and will often be included in databases[359], which benefit, in the European Union, from the protection of two distinct intellectual property rights, both contained in the Directive on the legal protection of databases.[360]

On the one hand, this Directive provides that databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright.[361] This copyright protection is however limited, as it is only granted to the structure of the database, not to its content.[362] On the other hand, a so-called *sui generis* right is granted to the maker[363] on the content of the database.[364] Its aim is to grant to the maker some form of control on the extraction, by third parties, of data from the database, as a reward for the investment it has made in building this database.[365] However, the scope of this *sui generis* right is also limited, as it is only granted to the maker of the database if there

---

[353] See Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ L 167/10*, 22 June 2001; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *OJ L 130/92*, 17 May 2019.

[354] See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 77/20*, 27 March 1996.

[355] See point 36. F. Dubuisson, *Existe-t-il un principe general d'appriopriation de l'information?*, *op. cit.*, p. 400-401.

[356] For an extensive analysis, see F. Dubuisson, *Existe-t-il un principe general d'appriopriation de l'information?*, *op. cit.*

[357] On this point, see M. Knockaert et T. Tombal, "Quels droits sur les données?", *Actualités en droit du numérique*, H. Jacquemin et B. Michaux (ed.), Limal, Anthémis, 2019, p. 58-68.

[358] N. Duch-Brown, B. Martens and F. Mueller-Langer, "The economics of ownership, access and trade in digital data", *Digital Economy Working Paper 2016-10*, JRC Technical Reports, 2016, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914144, p. 7.

[359] "A collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Article 1.2 of the Directive 96/9/EC).

[360] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 77/20*, 27 March 1996.

[361] Article 3.1 of the Directive 96/9/EC.

[362] Article 3.2 of the Directive 96/9/EC.

[363] "The person who takes the initiative and the risk of investing" (Recital 41 of the Directive 96/9/EC).

[364] Articles 7 to 11 of the Directive 96/9/EC.

[365] Recital 12 of the Directive 96/9/EC.

has been a qualitatively and/or quantitatively substantial investment in either the obtaining[366], verification[367] or presentation[368] of the contents.[369] Inversely, a substantial investment in the creation of the data will not induce protection under the Directive.[370] Moreover, this *sui generis* right allows the maker to prevent extraction[371] and/or re-utilisation[372] of the whole or of a qualitatively and/or quantitatively substantial part of the contents of that database.[373] Thus, this *sui generis* right only "protects the database as a whole and not specific data in the set".[374]

The maker of the database is thus only protected against the extraction and/or re-utilisation of substantial parts of the database, which implies that third parties can access the database in order to extract and re-use insubstantial parts of it. Nevertheless, the repeated and systematic extraction and/or re-use of insubstantial parts of the contents of the database will also be forbidden if it implies acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the database maker.[375] To evaluate this "substantial" nature of the extracted or re-used data, the economic value of the data also has to be taken into consideration.[376] Here, it is important to point out that what should be evaluated is not the intrinsic value of the data as such, but rather the amount of the human, technical or financial investments that were made by the maker to obtain, verify or present the data.[377]

59. While the text of the Database Directive can be relied upon to refute the idea of (intellectual) "property" on data, because the *sui generis* database right merely protects the contents of the database as a whole and not the individual data in the set, the evolution of the European Court of Justice's case law has arguably slipped towards the protection of some

---

[366] The investment in the obtaining refers to "the resources used to seek out existing independent materials and collect them in the database" (ECJ, *The British Horseracing Board e.a.*, 9 November 2004, C-203/02, EU:C:2004:695, § 31).
[367] The investment in the verification refers to "the resources used, with a view to ensuring the reliability of the information contained in that database, to monitor the accuracy of the materials collected when the database was created and during its operation" (ECJ, *The British Horseracing Board e.a.*, § 34).
[368] The investment in the presentation refers to "[the] systematic or methodical arrangement [of the data] in the database [and] the organisation of their individual accessibility" (ECJ, *The British Horseracing Board e.a,* § 36).
[369] Article 7.1 of the Directive 96/9/EC.
[370] ECJ, *The British Horseracing Board e.a.*, §§ 35-40. See also ECJ, *Football Dataco e.a.*, 1 March 2012, C-604/10, EU:C:2012:115, § 36. This distinction between unprotected creation and protected obtention can create some uncertainties in practice. For instance, it is not always clear whether the recording of weather data (temperature, humidity level, strength of the wind, etc.) or the taking of satellite pictures should be understood as data creation or obtention. Indeed, it is uncertain whether such data are "created" by their recording, or whether they "pre-exist" in the nature and are "obtained" through their recording. On this issue, see A. Masson, "Creation of database or creation of data: crucial choices in the matter of database protection", *E.I.P.R.*., 2006, Volume 28, Issue 5, p. 261-267.
[371] "Any unauthorised act of appropriation of the whole or a part of the contents of a database" (ECJ, *Directmedia Publishing*, 9 October 2008, C-304/07, EU:C:2008:552, § 34).
[372] "Any unauthorised act of distribution to the public of the contents of a protected database or a substantial part of such contents" (ECJ, *Innoweb*, 19 December 2013, C-202/12, EU:C:2013:850, § 37)
[373] Article 7.1 of the Directive 96/9/EC.
[374] N. Duch-Brown, B. Martens and F. Mueller-Langer, "The economics of ownership, access and trade in digital data", *op. cit.*, p. 14.
[375] Article 1.2 of the Directive 96/9/EC.
[376] M. Knockaert et T. Tombal, "Quels droits sur les données?", *op. cit.*, p. 62.
[377] ECJ, *The British Horseracing Board e.a.*, § 70-72.

"independent materials" (e.g. some of the data) in the set[378], and this may revive the debate on the "appropriation/property" of data.

This is notably apparent from the *Verlag Esterbauer* case, where the European Court of Justice was asked whether topographic maps can be defined as a database, and more specifically whether the data describing the nature of specific points on the maps constituted "independent materials" within the meaning of Article 1.2 of the Directive.[379] The Court first reminded that, will be classified as a database, under the Directive, the collection of "independent elements", defined as materials that retain their autonomous informative value after having been separated from one another.[380] It added that the Directive does not preclude the combination of two or more pieces of information from being held to be "independent materials", provided, however, that the extraction of that information from the database does not affect their autonomous informative value.[381] This implies that even if the value of these materials declines after their extraction from the database, they should still be considered as "independent materials" benefitting from the protection granted by Article 1.2 of the Directive, provided that they retain an autonomous informative value after the extraction.[382] Accordingly, following the Court's reasoning, the Directive protects (a combination of) some "independent materials" (e.g. some of the data) from this database, namely those that retain an autonomous informative value for the recipients after their extraction.[383] Nevertheless, in order to establish an infringement, the database maker will still have to demonstrate that the third party has extracted or re-used (a combination of) individual data that constitutes a qualitatively substantial part of the maker's database, in light of the human, technical or financial investments that were made by the maker to obtain, verify or present that data.[384]

However, this means that the database maker could prevent the extraction of (a combination of) a small number of these individual data, namely those which required a substantial investment to obtain.[385] In fact, in the case at hand, the extracted data (the geographical coordinates point of the map and the "signature", which is the numbered code used by the map producer to designate a unique feature, such as a church)[386] only represented an infinitesimally small part, and a very specific sub-category, of the total dataset.[387] As outlined by Michaux, "this phenomenon of fragmentation, or even atomisation, contributes to the

---

[378] See J. Drexl, "Data Access and Control in the Era of Connected Devices", *Study on Behalf of the European Consumer Organisation (BEUC)*, 2019, available at https://www.beuc.eu/publications/beuc-x-2018 121 data access and control in the area of connected devices.pdf, p. 74-75. See also M. Knockaert et T. Tombal, "Quels droits sur les données?", *op. cit.*, p. 62-64.

[379] ECJ, *Verlag Esterbauer*, 29 October 2015, C-490/14, EU:C:2015:735, § 9. On this case, see B. Michaux, "La Cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ?", note sous C.J.U.E., 29 octobre 2015, C-490/14, *Auteurs et Média*, 2017, Issue 1, p. 28-34.

[380] ECJ, *Verlag Esterbauer*, § 17; ECJ, *Fixtures Marketing*, 9 Novermber 2004, C-444/02, EU:C:2004:697, § 29.

[381] ECJ, *Verlag Esterbauer*, §§ 21-22.

[382] *Ibid*., §§ 23-24.

[383] *Ibid*., § 27.

[384] See J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 78.

[385] B. Michaux, "La Cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ?", *op. cit.*, p. 32.

[386] ECJ, *Verlag Esterbauer*, § 18.

[387] B. Michaux, "La Cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ?", *op. cit.*, p. 32.

impression that there is an *evolution towards the protection of data as such*, which seems to run counter to the legislator's initial objectives"[388], and "this movement towards an ever finer granularity could, if proven, be likely to *bring about a subtle gradual shift towards a protection of the data constituting the database*, rather than a protection of the database as a whole (taken in its entirety) or of its main subsets" (emphasis added).[389]

60. Another relevant decision of the European Court of Justice is the *Ryanair* case, where it held that the exceptions granted by the Directive to the lawful users of databases are not applicable to a database which is not protected by the Directive[390], and that, in those cases, the database maker is not prevented from adopting stricter contractual clauses concerning the conditions of use of such a database.[391] This leads to the peculiar consequence that the database maker can more strongly restrict the access to its database, via contractual clauses, if the latter is not covered by the Directive than if it is protected under the Directive. Indeed, these contractual clauses could go so far as to protect each individual data in the set from any kind of extraction or re-use, without granting any exceptions to third parties, through the self-proclamation of "ownership/property" rights on the data at hand.[392] This seriously endangers the balance between exclusive use of and access to/sharing of data that had been achieved by the European legislator in the Directive, notably through the limitations of the *sui generis* right and the provision of exceptions for lawful users, which define the circumstances in which the contents of the database can be accessed, extracted and/or re-used by third parties.

This is especially worrying when one considers that the Directive might allegedly not apply to data generated by connected devices and sensors, as these data could be considered as being created, rather than collected.[393] Indeed, and according to the *Ryanair* case, the maker of a database not covered by the Directive has the right to restrict more strongly the access to its database, via contractual clauses. This can be highly problematic if this database is the sole source of a specific type of data[394], although the refusal to provide access to a sole source of data might be considered as an abuse of dominant position according to the essential facilities doctrine, as will be outlined below.[395] It should however be noted that Drexl argues that the recognition of a *sui generis* database right to such sole sources of data might also potentially create additional barriers to data access, and that, as a consequence, some call for the introduction of a compulsory licencing system, as originally included in the Commission's proposal[396] for the Directive.[397]

---

[388] *Ibidem*. Author's own translation.
[389] *Ibid.*, p. 33. Author's own translation.
[390] In casu, the Court of Appeal of Amsterdam had ruled that Ryanair had failed to establish the existence of a "substantial" investment in either the obtaining, verification or presentation of the contents of its database, i.e. its website (ECJ, *Ryanair*, 15 January 2015, C-30/14, EU:C:2015:10, § 22).
[391] ECJ, *Ryanair*, § 39.
[392] On these "ownership/property" rights on data, see Part I, Chapter 2, Section B, b), 2.
[393] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 70.
[394] *Ibid*., p. 68.
[395] See Part III, Chapter 1, Section A.
[396] Proposal by the Commission of the European Communities for a Council Directive on the legal protection of databases, Brussels, 13 May 1992, COM(92) 24 final, Article 8.

In fact, the European Commission's inception impact assessment on its future "Data Act" seems to suggest that the Database Directive might need to be reviewed as it might constitute an obstacle to data sharing, which could lead to the introduction of a compulsory licencing scheme on fair, reasonable, proportionate, transparent and non-discriminatory terms.[398] Interestingly, this suggestion by the European Commission coincides with a recent decision by the European Court of Justice, which acknowledges that "it is necessary to strike a fair balance between, on the one hand, the legitimate interest of the makers of databases in being able to redeem their substantial investment and, on the other hand, that of users and competitors of those makers in having access to the information contained in those databases and the possibility of creating innovative products based on that information".[399]

2. Creation of a new "property-like" right over data?

61. The European Court of Justice is not the only institution that has revived the debate on the "appropriation/property" of data, as the European Commission also explored the potential creation of a new "data producer's right", establishing a form of ownership over non-personal data.[400] In doing so, the Commission was actually echoing a request originally stemming from the German automotive industry, as car manufacturers were seeking to appropriate exclusive rights on data generated by the cars they produce.[401] This is because such data is becoming more and more attractive for third parties such as car dealers, spare parts manufacturers, authorised and independent garages and repairers, developers of infotainment software used in vehicles, insurers, vehicle users, and possibly also public authorities. Taking a more general perspective, the Commission's underlying idea was that such a right would generate more data sharing by clarifying the situation for the data holders, while giving third parties the possibility to use the data in certain specific cases. The Commission's endeavour was thus in line with the default model of "exclusive property".[402]

---

[397] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 73 and 81-83. The pros and cons of such a compulsory licencing were extensively discussed in the final evaluation report of the Database Directive, but it has not led to any modification (see Jiip, Technopolis, L. Bently and E. Derclaye, "Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases – Final report", 2018, available at, https://ec.europa.eu/digital-single-market/en/news/study-support-evaluation-database-directive, p. 34-44; J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 81). Drexl is not in favour of such a compulsory licensing system, but rather supports the creation of a new exception in the Directive "that gives precedence to any existing and future data access regimes over the *sui generis* database right" (p. 85).

[398] European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 2-6.

[399] ECJ, *CV-Online Latvia*, 3 June 2021, C-762/19, EU:C:2021:434, § 41. For a brief comment of this decision, see Z. Aszendorf and G. Pratt, "CJEU narrows protection afforded to database right in the EU", 9 June 2021, available at https://www.lexology.com/library/detail.aspx?g=f399c5bb-58ac-4162-b2c8-b8a53297f800&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2021-06-11&utm_term=.

[400] Communication from Commission, "*Building a European Data Economy*", *op. cit*., p. 13.

[401] T. Hoeren and P. Bitter, "Data ownership is dead: long live data ownership", *E.I.P.R.*, 2018, 40(6), p. 347-348; T. Hoeren, "A New Approach to Data Property?", *A.M.I.*, 2018/2, p. 58.

[402] See point 29.

i. Data producer's right

62. Under this new "data producer's right", the producer, defined as the long-term owner or user of the machine creating the data, would have been granted a right to use and authorise the use of non-personal data.[403] However, the development of such a right was a source of uncertainty on four levels, namely the nature of the right, the scope of the data covered, the attribution of ownership of the right and the determination of exceptions to the right.

With regard to the nature of the right, the Commission considered two options. The first was the creation of a new right *in rem* enforceable *erga omnes*, conferring an exclusive right to use non-personal or anonymised machine-generated data.[404] In such perspective, this right would have allowed the holder to object to the use of these data by third parties, regardless of any contractual relationship, and to claim damages for any unauthorised access or use of the data. However, the Commission did not fail to point out that such a right could not have concerned personal data, since the right to personal data protection is a fundamental right aimed at ensuring that data subjects retain control on "their" personal data, which cannot be traded away. Indeed, according to the European Data Protection Supervisor, since such data are an integral part of the human being, they must therefore remain non-transferable, similarly to organs.[405] The second option was the creation of a *set of purely defensive rights*, similar to the protection afforded to trade secrets.[406] Unlike the more protective approach of the first option, this second option aimed to increase data sharing, while reassuring data owners by granting them a series of rights in the event of illegal use of data by third parties, equating to a protection of *de facto* possession of data rather than to a protection of ownership of data. Had such an approach been adopted, the question would also have arisen of the need to establish a (restrictive) list of hypotheses of legal and illegal use.

Regarding the scope of the data covered, it would probably have been limited to non-personal or anonymised data not yet structured in a protected database[407], as well as metadata[408]

---

[403] Communication from Commission, "*Building a European Data Economy*", *op. cit*., p. 13.

[404] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the Communication "*Building a European Data Economy*", Brussels, 10 January 2017, SWD(2017) 2 final, p. 33.

[405] European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017, available at https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf, p. 7; European Data Protection Supervisor, *Opinion 8/2018 on the legislative package "A New Deal for Consumers",* 5 October 2018, available at https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf, p. 16-17. See also, S. Gutwirth and G. Gonzalez Fuster, "L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre", *Law, norms and freedom in cyberspace – Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier and R. Queck (eds.), Bruxelles, Larcier, 2018, p. 117-140.

[406] *Ibid*., p. 33-34. See Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157/1*, 15 June 2016. See point 185.

[407] "A collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Article 1.2 of the Directive 96/9/EC). On database protection, see points 58 to 60.

[408] "Metadata is "data information that provides information about other data". Many distinct types of metadata exist, including descriptive metadata, structural metadata, administrative metadata, reference metadata and statistical metadata" (https://en.wikipedia.org/wiki/Metadata)

relating to such data.[409] However, only the syntactic level (data and code), and not the semantic level of the information or ideas expressed by that data, would have been protected, in order to avoid the creation of a "super IP right".[410] For example, this right would not have protected the visual rendering of a digital photograph, which is otherwise protected by copyright, but would have conferred certain rights on the data contained in this file.

Allocating the ownership of this right would also have been a thorny issue to be resolved. In the event that the option selected was the creation of a right *in rem*, the Commission suggested that the right should be allocated on the basis of the investments and resources devoted to the creation of the data.[411] In concrete terms, this would have led to the granting of the right to the manufacturer of the machine generating the data – the latter having invested in this tool –, or to the economic operator using this machine. This would have posed practical attribution difficulties, especially since in many situations, several persons or companies jointly invest in such machines, making it virtually impossible to accurately identify one or more holders. On the contrary, if the option selected had been the creation of a series of purely defensive rights, the Commission proposed to grant these rights to the legitimate *de facto* possessor of these data, subjecting this protection to the condition that the *de facto* possessor has put in place technical protection measures in order to limit access to its data by third parties.[412]

Finally, as with intellectual property rights, it would also have been required to specify a range of exceptions to the data producer's right. In practice, these exceptions would have taken the form of an obligation to share data in certain situations, for instance in order to foster scientific research or to achieve public interest purposes (environmental protection, mobility, etc.).[413]

ii. Criticism in the literature

63. While some have supported the idea of developing such a right[414], the large majority of legal scholars have expressed their concern about the creation of a "property-like" right over data, arguing that there was no economic justification to support such a proposal.[415] Indeed,

---

[409] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, *op. cit*., p. 34.

[410] *Ibidem*. On this distinction between syntactic and semantic information, which is not always easy to make in practice, see H. Zech, "Data as tradeable commodity", *European Contract Law and the Digital Single Market*, A. De Franceschi (ed.), Cambridge, Intersentia, 2016, p. 51-79.

[411] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, *op. cit*., p. 34-35.

[412] *Ibid*., p. 35.

[413] *Ibid*., p. 35-36. Communication from Commission, "*Building a European Data Economy*", *op. cit*., p. 13.

[414] B. Van Asbroeck, J. Debussche and J. César, "White Paper – Data ownership in the context of the European data economy: proposal for a new right*"*, 2017, available at https://www.twobirds.com/en/news/articles/2017/global/data-ownership-in-the-context-of-the-european-data-economy. In this White Paper, the authors suggest the creation of a non-exclusive, flexible and extensible ownership right in data(sets).

[415] See, *inter alia*, J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*"*, *Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975, p. 30-38; A. Weibe, "Protection of industrial data - a new property right for the digital economy?", *Journal of Intellectual Property Law & Practice*, 2017, Vol. 12, n° 1, p.

according to the latter, there is no evidence that the absence of such a right creates a lack of incentives for the production, analysis or marketing of data.[416] There is thus no "underproduction problem". Moreover, the creation of such a right could lead to disruptive juxtapositions and delimitation problems with existing IP rights[417], and it could also strengthen entry barriers that, consequently, would increase market power of large data holders.[418] Additionally, the difficulty in determining the scope of application of such a right and the allocation of its ownership could have led to significant legal uncertainty, entailing high costs and obstacles for future innovation.[419] Furthermore, the reference to the concept of "property" seems inappropriate in view of the intangible and non-rivalrous nature of data, and, in any case, "the dependency of data's value on contextualisation contradicts the justification for establishing a hypothetical property right as a one-size-fits-all measure".[420]

Finally, it is important to remind that data may be technically and contractually excludable.[421] Therefore, data is arguably not a public good, which is non-rivalrous and non-excludable, but rather a "club good", which is non-rivalrous but excludable.[422] Accordingly, the "public good market failure", on which the justification of IP rights is based, cannot simply be applied by analogy to data. This is an additional reason for excluding the creation of "property" rights on data.

iii. Contractual freedom and market self-regulation rather than "property" rights

64. In light of this criticism, the European Commission has therefore abandoned the idea of creating a "property-like" right on data. Rather, the discussions pertaining to "property" on data have shifted towards legal reflections revolving around notions of data "control" and

---

66-71; B. Hugenholtz, "Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 78-82; W. Kerber, "Governance of Data: Exclusive Property vs. Access", *IIC*, 2016, Volume 47, Issue 7, p. 761; W. Kerber, "Rights on Data", *op. cit.*, p. 115-120 ; H. Zech, "Data as tradeable commodity", *op. cit.*, p. 51-79; A. Strowel, "Big Data and Data Appropriation in the EU", *Research Handbook on Intellectual Property and Digital Technologies*, T. Aplin (ed.), Camberley, Edward Elgar, 2020, p. 107-135; T. Hoeren and P. Bitter, "Data ownership is dead: long live data ownership", *op. cit.*, p. 347-348; T. Hoeren, "A New Approach to Data Property?", *op. cit.*, p. 58-60; D. Kim, "No one's ownership as the status quo and a possible way forward: A note on the public consultation on Building a European Data Economy", *Journal of Intellectual Property Law & Practice*, 2018, Volume 13(2), p. 154-165.

[416] J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access", *op. cit.*, p. 30-34; A. Weibe, "Protection of industrial data", *op. cit.*, p. 67; B. Hugenholtz, "Data Property in the System of Intellectual Property Law", *op. cit.*, p. 80-81; W. Kerber, "Governance of Data: Exclusive Property vs. Access", *op. cit.*, p. 761; W. Kerber, "Rights on Data", *op. cit.*, p. 115-120.

[417] A. Weibe, "Protection of industrial data", *op. cit.*, p. 67-68; B. Hugenholtz, "Data Property in the System of Intellectual Property Law", *op. cit.*, p. 89-94.

[418] L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability", *EDPL*, 2020/1, p. 86.

[419] W. Kerber, "Governance of Data: Exclusive Property vs. Access", *op. cit.*, p. 761.

[420] L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU", *op. cit.*, p. 86.

[421] See points 53 and 54.

[422] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34; M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 45.

"access".[423] Nevertheless, as a fall-back solution, the Commission has established, in its Communication "Towards a common European data space", key principles for *voluntary* data sharing between companies.[424] However, these principles are not binding, in order to respect the contractual freedom of the parties. In addition to these principles, the Commission has also been working on more concrete recommendations as to which contractual provisions should ideally appear in data sharing contracts, in addition to the traditional clauses relating to the duration of the contract, the conditions for the termination of the contract, etc.[425]

65. Moreover, it should be mentioned that the Commission has created a "Support Centre for Data Sharing"[426], with the aim of putting in place a series of measures facilitating (voluntary) data sharing, in particular by providing examples of good practice, standard contractual clauses or existing contract models.[427] This Support Centre has notably analysed the legal characteristics of a set of existing data sharing contracts, and has developed a standardised set of "tags", in order to determine which types of clauses are contained in each of the specific contracts, thereby creating a searchable repository of contracts based on a clear and consistent standardised classification system.[428]

3. (Anti-)"reservation" of data rather than "property" on data

66. There has thus been a shift from discussions pertaining to "property" on data, towards legal reflections revolving around notions of data "control" and "access".[429] Indeed, independently of any establishment, in law, of a "property" right on data, the reality of the situation on the field, from a technical and contractual point of view, is that data holders have a *de facto* exclusive control on their data and can decide on whether, and to whom, they provide access to it.[430] These data holders thus have the ability to "reserve" their data.

i. Data reservation

67. This concept of "reservation" has been suggested by Mousseron and Vivant, in order to avoid the complex debates on the "property" of information.[431] Rather, "reservation" designates a form of control on this information, which can be legal (exclusive rights) but also

---

[423] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Towards a common European data space*", Brussels, 25 April 2018, COM(2018) 232 final, p. 8-9.
[424] *Ibid*., p. 10. See also Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication "*Towards a common European data space*", Brussels, 25 April 2018, SWD(2018) 125 final, p. 7.
[425] Commission Staff Working Document establishing a guidance on sharing private sector data, *op. cit*., p. 6-8.
[426] See https://eudatasharing.eu/homepage
[427] Commission Staff Working Document establishing a guidance on sharing private sector data, *op. cit*., p. 6.
[428] Support Centre for Data Sharing, "B.1 – Report on collected model contract terms", SMART 2018/2019, 26 July 2019, available at https://eudatasharing.eu/fr/legal-aspects, p. 4. For more information on these tags, see p. 8-17.
[429] See Communication from the Commission, "*Towards a common European data space*", *op.cit.*, p. 8-9.
[430] W. Kerber, "Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars", 26 August 2019, available at https://ssrn.com/abstract=3445422, p. 32.
[431] J.-M. Mousseron et M. Vivant, "Les mécanismes de réservation et leur dalectique: Le «terrain» occupé par le droit", *Semaine Juridique, Cahiers de Droit de l'Entreprise,* 1989/1, p. 2-4; S. Dusollier, "Du commun de l'intelligence artificielle", *Penser le droit de la pensée. Mélanges en l'honneur de Michel Vivant*, Paris, Dalloz, 2020, p. 109.

factual (exclusion through contractual or technical means) or intellectual (trade secrets).[432] As summarised by Mousseron and Vivant, "it is the fact of being alone on the market that is always sought after in the end: the various paths taken or likely to be taken, which are intertwined, all have the aim, clearly stated or not, of ensuring the economic reservation of information to the one who has control over it".[433]

This concept can perfectly be translated from the realm of information to the realm of data, as data holders' *de facto* control on data allows them to economically reserve this data, through technical and contractual exclusion.[434] It also circumvents the issues of "property" on data. Accordingly, the remainder of this thesis will refer to the reservation/control on data, rather than to "property" on data.

Nevertheless, it is relevant to point out that, even if the Commission has moved away from "property" on data towards data "reservation", it has not moved away from the dominant model of "exclusivity" (economic reservation of data through contractual and technical means).[435] In this sense, data are thus commodified, and some authors question whether another avenue, based on an anti-reservation paradigm ("data commons"), could be pursued instead, in order to guarantee a larger collective access to data.[436]

ii. Data commons – Anti-reservation of data

68. According to Dusollier, this anti-reservation paradigm of the "data commons" implies an impossibility to exert exclusive control on data and a correlative obligation to share it.[437] Instead of thinking in terms of exclusive control on and individual access to data, this paradigm calls for a collective use of this resource, because data is a common good and it should therefore be managed in order to produce collective benefits.[438] Such an approach is justified by data's characteristics, as they are non-rivalrous, capital and general-purpose resources[439], whose use creates multiple spill overs across society.[440]

To give a concrete example, Shkabatur suggests that user-generated data (personal "primary data" and "inferred/derived data" in this thesis' typology"[441]) should be recognised as a "global commons", and that a wide range of independent stakeholders (researchers, journalists, NGOs, public authorities…) should be granted access to the user-generated data

---

[432] S. Dusollier, "Du commun de l'intelligence artificielle", *op. cit.*, p. 109.
[433] J.-M. Mousseron et M. Vivant, "Les mécanismes de réservation et leur dalectique", *op. cit*., p. 3 (author's own translation).
[434] S. Dusollier, "Du commun de l'intelligence artificielle", *op. cit.*, p. 111.
[435] *Ibid*., p. 113. See also point 29.
[436] *Ibid*., p. 109 and 114. See also J. Shkabatur, "The Global Commons of Data", *Stanford Technology Law Review*, 2019, Vol. 22, p. 354-411; M. Madison, "Tools for Data Governance", *op. cit.*, p. 29-43; S. Gutwirth et I. Stengers, "Le droit à l'épreuve de la résurgence des *commons*", *Revue Juridique de l'environnement*, 2016/2, Vol. 41, p. 306-343; P. Drahos, *Intellectual Property, Indigenous People and their Knowledge,* Cambridge University Press, 2014, p. 1-11.
[437] S. Dusollier, "Du commun de l'intelligence artificielle", *op. cit.*, p. 115.
[438] *Ibidem*.
[439] B. Frischmann, *Infrastructure: The Social Value of Shared Resources*, Oxford, Oxford University Press, 2012, cited in OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being, op. cit.*, p. 179. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 3.
[440] M. Madison, "Tools for Data Governance", *op. cit.*, p. 40. See point 52.
[441] See points 21 to 24.

collected, aggregated and processed by any company operating an online platform (and thus not just the GAFAMs), in order to address a variety of public challenges related to transportation, health, agriculture or natural disasters.[442] Importantly, Shkabatur outlined that such a "global data commons" regime would not imply that these data platforms would have to lose their commercial benefits and decision-making prerogatives, nor that the access to the user-generated data should be free and open to all, independently of any personal data protection and security considerations.[443] Rather, such a regime would need to offer a whole spectrum of data access modalities, some more restrictive and some more permissive, which would have to strike a balance between the collective benefits derived from a broader access to data, on the one hand, and the need to protect the user's personal data[444] and the platform's legitimate commercial interests, on the other hand.[445] For instance, the principle of purpose limitation of the GDPR[446] should be kept in mind to restrict the cases in which this user-generated data can be re-used, because if a lid is not put on these re-use purposes, data subjects would lose control on "their" data as they would not know by whom and for which purposes it is processed.[447]

69. Transitioning towards, and establishing, such data commons is a matter of political choice and could be a fertile ground to move away from the classic Western social construct of "exclusivity as the rule", towards more "generative" forms of "rights", based on data sharing and on collective access and usage rights, whose goal is not to lead towards accumulation by the few, but rather towards collective benefits for the many.[448] While this "data commons" approach is certainly a worthy avenue of exploration for future research, this will not be an exercise conducted in the context of this thesis. This is because such an approach requires voluntary efforts, within a diffused community of actors, to govern data and to share it. It thus relies on *voluntary* data sharing in the context of the exercise of collective rights on data as commons. Yet, this thesis is instead focussed on hypotheses of *compulsory* B2B data sharing[449], which do not fit in this "data commons" approach.

c) The economic rationale for data sharing

70. In light of data's characteristics, and notably of the fact that data could be considered as an "infrastructural resource"[450], a growing call for data sharing is being made.[451] As for

---

[442] J. Shkabatur, "The Global Commons of Data", *op. cit.*, p. 383 and 389.
[443] *Ibid*., p. 362.
[444] For an analysis, in the United States, of privacy as a commons, see M. Sanfilippo, B. Frischmann and K. Standburg, "Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework", *Journal of Information Policy*, 2018, Vol. 8, p. 116-166.
[445] J. Shkabatur, "The Global Commons of Data", *op. cit.*, p. 362 and 385. For a complete analysis of this spectrum of modalities, see p. 385-398.
[446] Personal data can only be processed for specified, explicit and legitimate purposes, and cannot be further processed in a manner that is incompatible with those purposes (Article 5.1.b) of the GDPR).
[447] On this control by individuals, see Part I, Chapter 2, Section C, b).
[448] S. Dusollier, "Du commun de l'intelligence artificielle", *op. cit.*, p. 116-117. See also U. Mattei and A. Quarta, *The Turning Point in Private Law. Ecology, Technology and the Commons*, Cheltenham, Edward Elgar, 2019.
[449] See points 4 and 5.
[450] See points 52 to 55.
[451] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 179; V. Mayer-Schonberger and T. Ramge, *Re-inventing capitalism in the age of big data*, New York, Basic Books, 2018.

intangible resources, two types of rationale can be called upon to support data sharing, namely economic considerations on the one hand, which will be addressed here, and more societal and "empowerment" considerations, on the other hand, which will be addressed in Section C.

Importantly, compulsory B2B data sharing is not a goal in itself, and it should only be used, in specific circumstances, as a mean to achieve determined objectives.[452] Indeed, a balance must be found between exclusive use of and access to/sharing of data, as an equilibrium must be found between the benefits and costs of data sharing.[453] The aim has never been, and should arguably never be, an unconditional availability of data. Rather, a case-by-case assessment of the necessity of imposing such compulsory sharing legislation will always be required.[454]

71. To get a better grasp at the economic rationale for data sharing, it is first necessary to understand the economics of data in general. Accordingly, the incentives to collect and produce data will first be outlined. Then, it will be outlined that these data collection and production incentives could also create barriers to entry to the data market, and might accordingly entail market failures. These market failures will serve as a rationale for more data sharing, although such sharing should not be absolute, as it should factor the costs and incentives for each of the parties.[455] Naturally, in light of the scope of the thesis, the aim is not to strive for exhaustivity regarding these questions, but rather to provide a sufficient basic understanding of these economic considerations.

1. Data collection and production incentives

72. As outlined above, data's true value does not generally stem from data as such, but rather from the value of the information and knowledge that can be extracted from its combination and aggregation.[456] Indeed, "the more available and more varied the data, the better the knowledge that can be mined from it".[457] In economic terms, this means that data is characterised by economies of scope and scale, which provide an advantage to data holders and incentivise them to collect and produce as much data as possible.

To understand the difference between economies of scope and economies of scale, the easiest is to picture a dataset "as a two-dimensional spreadsheet with the number of columns representing the number of variables and the number of rows the number of observations on these variables. (…) Economies of scale refer to increased prediction accuracy due to an increase in the number of rows. Economies of scope refer to increased prediction accuracy

---

[452] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.
[453] See points 90, 91 and 95.
[454] Support Centre for Data Sharing, "B.2 – Analytical report on EU law applicable to sharing of non-personal data", SMART 2018/2019, 24 January 2020, available at https://eudatasharing.eu/fr/legal-aspects, p. 4.
[455] P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *op. cit.*, p. 616-620.
[456] See point 15. D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 342.
[457] M. Gal and D. Rubinfeld, "Data Standardization", *New York University Law Review*, 2019, Vol. 94, Number 4, p. 774.

due to an increase in the number of columns or explanatory variables".[458] Economies of scale thus pertain to the breadth of the data (e.g. a broad dataset has data about more people), while economies of scope pertain to the depth of the data (e.g. a deep dataset contains more data about each person).[459] Digital platforms, such as Facebook or Google, are good examples of data aggregators who can realise economies of scope and scale, as their intermediation services allow them to expand both the breadth and depth of their data.[460]

73. Economies of scope in data aggregation generate economic efficiency gains, as more insights and economic value can be extracted from merging two complementary datasets than from keeping them separated in data silos.[461] As a consequence, there are economic efficiencies in concentrating data in large data pools, and there are clear incentives for data-driven firms to expand their activities in as many data-related service markets as possible.[462] Moreover, economies of scale also generate efficiency gains, as having data about more people allows to improve the service offered, which in turn attracts more users, etc.[463]

This is described by Prüfer and Schottmüller as data-driven *indirect* network effects.[464] These *indirect* network effects should not be confused with *direct* network effects, which are completely demand-driven, and which relate to the fact that the utility of a service for a user will be function of, and will increase with, the number of other users that use the service.[465] For instance, users will only be interested in joining a social network if there are a sufficient number of people already using it with whom they can interact or if their friends are already using it. *Indirect* network effects, on the other hand, are also driven by the number of users, but they generate benefits on the supply-side, as the more users use the service, the more user information will be generated as a costless by-product, which will allow the service provider to better adapt its service or its algorithm to user preferences, which in turn will attract more users, etc.[466] Search engines are a good example of this phenomenon.[467] This is also referred

---

[458] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 13.
[459] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability: case studies and data access remedies", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/, p. 7.
[460] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 15.
[461] *Ibid*., p. 4.
[462] *Ibid*., p. 5.
[463] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 7.
[464] J. Prüfer and C. Schottmüller, "Competing with Big Data", *TILEC Discussion Paper No. 2017-006 and CentER Discussion Paper No. 2017-007*, February 2017, available at https://pure.uvt.nl/ws/portalfiles/portal/15514029/2017_007.pdf, p. 1; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 15. For a detailed analysis of the various classic and data driven network effects, see M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 162-216.
[465] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2.
[466] *Ibid*., p. 1-2.
[467] C. Argenton and J. Prüfer, "Search engine competition with network externalities", *Journal of Competition Law and Economics*, 2012, Vol. 8(1), p. 73-105.

to, from a dynamic perspective, as a "user feedback loop".[468] It entails decreasing marginal costs of innovation, due to the high consumer demand.[469] Naturally, these two types of network effects are not mutually exclusive, as illustrated by online social networks that are characterised by both.[470]

From a dynamic perspective, these data-driven network effects can also give rise to another self-reinforcing feedback loop, namely a "monetisation feedback loop", as explained by Krämer *et al*.[471] Indeed, as these data-driven companies derive a large chunk of their revenues from advertising, collecting more user data enables them to provide more targeted advertising. Because it is more effective, this generates more advertising revenues, which in turn allows them to further invest in the quality of their service, which will attract more users, etc.

74. In light of these economies of scope and scale and of these network effects[472], data holders are thus incentivised to aggregate data as this provides them with a competitive advantage and generates economic benefits. This is especially true in circumstances where *first mover advantages* "can become sustained competitive advantages, because competitors are unable to initiate the same feedback loop".[473] This will be further developed below when presenting the potential data market failures.[474] That being said, as outlined by Stucke and Grunes, "while network effects can help insulate the dominant firm from competitive pressure, they do not immunize [it] from competition altogether".[475]

2. Entry barriers to data markets

75. While economies of scale and scope and data-driven network effects in data aggregation incentivise data collection and data production, the flip side of the coin is that these same economic characteristics of data may also raise entry barriers to data markets. These possible entry barriers have been extensively analysed by Rubinfeld and Gal, whose work will be briefly summarised here.[476] Next to the classic legal barriers to data collection (e.g. in circumstances where the data collection is prevented by personal data protection legislation or IP rights such as the *sui generis* database right)[477], these authors mostly focus on what they describe as technical barriers to data collection. As these technical barriers mainly derive from

---

[468] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 64. See also A. Lerner, "The Role of 'Big Data' in Online Platform Competition", 26 August 2014, available at SSRN http://dx.doi.org/10.2139/ssrn.2482780; M. Bourreau, A. de Streel and I. Graef, "Big Data and Competition Policy: Market power, personalised pricing and advertising", *CERRE Report*, 2017, available at http://www.cerre.eu/publications/big-data-and-competition-policy.

[469] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 1-2.

[470] *Ibid*., p. 2.

[471] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 64.

[472] For a detailed analysis of the various classic and data driven network effects, see M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 162-216.

[473] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 64.

[474] See points 78 to 85.

[475] M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 214

[476] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 339-381. On these entry barriers, see p. 350-365.

[477] *Ibid*., p. 359-362.

the economic characteristics of data mentioned above, it will be referred to them, in this thesis, as techno-economic entry barriers.

76. Firstly, techno-economic entry barriers can arise if incumbent data holders have achieved substantial economies of scope and scale, which allowed them to partially or totally sink their investments.[478] Moreover, they might also take advantage of "economies of speed", if the velocity of their data collection allows them to discern trends well before others.[479] Google could be such an example in the search market, as its large dominant position allows it to collect much more search data than its competitors and, consequently, to discern new trends faster than others. If the incumbent data holders' economies of scope, scale and speed are sufficiently large, the high fixed costs of data collection for a new entrant might make entry prohibitive.[480]

Secondly, the data-driven network effects mentioned above could also create techno-economic entry barriers, as new entrants would have to make substantial investments in order to counter, or even merely overcome, the existing network effects benefiting the incumbent data holders.[481] Indeed, the entrant would not only have to invest to overcome the direct network effects (i.e. invest in order to attract a sufficient number of users in order for the service to attain a critical mass and "take-off"), but also the indirect network effects (i.e. because the incumbent has access to more (timely) data about user preferences than the entrant, it can more easily and quickly adapt to the changing demand and it can better target its advertising, which generates more revenue).[482]

Thirdly, techno-economic entry barriers could also emerge due to *lock-in* considerations.[483] Indeed, users could be "locked into" the service of the incumbent data holder for two reasons. On the one hand, they could be locked-in because the incumbent's data-driven network effect deters new entrants from developing alternatives. Because no alternative having a minimum scale (i.e. a minimum number of users) exists, the users have nowhere else to go. On the other hand, they could be locked-in because the incumbent makes it technically difficult (or even impossible) to extract the data from its service in order to provide it to a new entrant, which then entails high switching costs.[484] This second problem has been tackled, to a certain extent, by data portability rights.[485] Importantly, these two reasons are not mutually exclusive and in fact reinforce each other.

Fourthly, techno-economic entry barriers could emerge due to the uniqueness of the data collected by the incumbent data holder, or due to the fact that it is the unique gateway to such

---

[478] *Ibid*., p. 352.
[479] *Ibid*., p. 353.
[480] *Ibid*., p. 352-353.
[481] *Ibid*., p. 355.
[482] *Ibid*., p. 355-356. See also M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 170 and 189-199.
[483] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 364. See also M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 159.
[484] M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 291-292.
[485] See Part II, Chapter 1, Sections A and B.

data.[486] Indeed, while the non-rivalrous nature of data implies that it can usually be collected from various alternative sources and that, as a consequence, the costs of data collection are usually not prohibitive for new entrants, "unique access points to unique data may lead to situations in which the data cannot be easily replicated".[487] This could notably be the case for data created as the result of interactions on a social network, for data pertaining to a very specific event (e.g. data gathered at a specific point in time about a natural disaster) or for data generated as a by-product of a very specific activity conducted by the incumbent data holder (e.g. data about oil-drilling sites).[488] This could also be the case in hypotheses where the incumbent data holder has technically or contractually excluded the access to a unique source of data, or where the access to this unique source is subject to a very high access price and/or to very strict conditions.[489] Pre-installed applications could also act as more subtle gateway barriers to data collection, as it will be difficult for new entrants to replace them, due to the combination of the default option and of users' *status quo* bias (i.e. users tend to simply use the default options/settings/applications and rarely modify them).[490]

Fifthly, techno-economic entry barriers could emerge from the failure to compete for the user's attention, which is mainly captured by several incumbents (Google, Facebook, Netflix…), as new entrants may struggle to collect data if they do not manage to attract users (who only have a finite amount of attention to spend) to their services.[491]

Sixthly, if the new entrant opts to acquire the data that it needs from third parties, rather than to collect it itself, techno-economic entry barriers could "arise from limited information on who owns the relevant data, or on the costs of locating and contracting with such data holders".[492]

77. Naturally, it would be erroneous to say that all of these techno-economic barriers exist in all of the data driven markets. Rather, these must be understood as a list of potential entry barriers that might occur in these markets. Their existence and magnitude will be function of the characteristics of each data market, and they should not simply be assumed to exist.[493] A case-by-case analysis is required in order to assess whether these entry barriers exist, and, if they do, the extent to which they prevent market entry.[494] Indeed, even if, in theory, incumbent data holders benefiting from a data advantage (economies of scale, scope and speed and network effects) could be incentivised to engage in exclusionary conduct and to erect techno-economic entry barriers to maintain or strengthen their advantage, "the mere

---

[486] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 350-351.
[487] *Ibid*., p. 351.
[488] *Ibid*., p. 351 and 357.
[489] *Ibid*., p. 362. See also B. Lundqvist, "Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law", *Stockholm Faculty of Law Research Paper Series n° 54*, 2018, available at https://ssrn.com/abstract=3103870, p. 4.
[490] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 351.
[491] *Ibid*., p. 357.
[492] *Ibid*., p. 359.
[493] *Ibid*., p. 369.
[494] M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 158.

existence of high entry barriers into these markets, by itself, does not automatically lead to the conclusion that social welfare will be harmed".[495]

Finally, it is important to point out that, in assessing these entry barriers, the "capital resource" characteristic of data (i.e. it is used as an input for goods or services rather than as an end it itself[496]) should be factored, having as consequence that "the analysis of entry barriers should often extend beyond the specific market under scrutiny to related parts of the data-value chain".[497] Indeed, as will be developed below, incumbent data holders are rarely present in a single market, but rather build up conglomerates operating across several data-driven markets.[498]

3. Data market failures

78. As outlined above, extreme returns to scale, network effects and the prominent role of data (i.e. being able to use data to develop or improve innovative products or services) are incentives for data collection and production and are key competitive parameters. These characteristics lead to strong economies of scope, scale and speed that benefit large incumbent data holders who have access to more (recent) data than their competitors.[499] As summarised by Fast *et al*., six factors may provide incumbent data holders with a competitive advantage, namely "(i) exclusive access to data, (ii) exploitative access to data, (iii) economies of scale in data analytics, (iv) platform business models and network effects, (v) data-induced switching costs, and (vi) economies of scope and ecosystem expansion".[500] Looking at it from the other side of the coin, these characteristics and factors might lead to techno-economic entry barriers (uniqueness of the data collected by the incumbent data holder or unique gateway to it; economies of scale, scope and speed; network effects; lock-in and switching costs)[501], which will makes it very difficult to dislodge these incumbent data holders.[502] This is where data market failures might occur. This thesis will focus on the types of market failures that are the most relevant for the topic of compulsory B2B data sharing, namely those that can derive from data concentration on the one hand, and data conglomerates and *domino effects* on the other hand.

Naturally, other market failures, such as the lack of incentives to collect data, uncertainties in terms of risks, high transaction costs for sharing and missing markets, and asymmetries of

---

[495] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 370.
[496] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 180-181.
[497] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 375.
[498] See, *inter alia*, J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *CERRE Report*, March 2019, available at http://www.crid.be/pdf/public/8377.pdf.
[499] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era – Final report", 2019, available at http://ec.europa.eu/competition/publications/reports/ kd0419345enn.pdf, p. 3 and 19-24.
[500] V. Fast, D. Schnurr and M. Wohlfarth, "Data-Driven Market Power: An Overview of Economic Benefits and Competitive Advantages from Big Data Use", July 2019, available at https://ssrn.com/abstract=3427087, p. 2 and 19-35.
[501] See point 76.
[502] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 24.

information distorting decision-making can also impact the data markets.[503] However, these are, in fact, rather obstacles to *voluntary* data sharing that require other remedies than *compulsory* B2B data sharing. Indeed, the first three of these market failures rather require regulatory interventions in the technical (standardisation, interoperability, etc.) and governance sphere, in order to create more favourable conditions for the emergence of third party intermediaries that can remedy, or at least reduce, these market failures.[504] This is, for instance, materialised in the European Commission's proposal for a Data Governance Act that notably aims at promoting *voluntary* data sharing services by intermediaries.[505] Asymmetries of information, on the other hand, require transparency interventions, such as provided in Article 9 of the Platform to Business Regulation[506].[507] For the reasons mentioned in the introduction[508], these other market failure will however not be extensively analysed in this thesis. On the other hand, for the types of market failures on which this thesis will focus, namely data concentration on the one hand, and data conglomerates and *domino effects* on the other hand, market-based solutions, even if supported by regulatory interventions, may not be sufficient, hence leading to the need for *compulsory* B2B data sharing remedies.[509]

i. Data concentration

79. As data aggregation generates network effects and economies of scope, scale and speed, the economics of data favour concentration.[510] Indeed, due to these factors, data driven

---

[503] For a broader analysis of all of the potential types of data market failures, see M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*.; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit*.; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*; B. Martens, "An economic perspective on data and platform market power", *JRC Digital Economy Working Paper 2020-09*, February 2021, available at https://www.researchgate.net/publication/349179464.

[504] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 28. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability: Towards a Governance Framework*", CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/.

[505] See Articles 9 to 14 of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final, p. 11-12; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 25-27.

[506] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019; Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports.

[507] See below, Part II, Chapter 1, Section D.

[508] See points 4 and 5.

[509] See, *inter alia*, M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit*.; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*

[510] M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 336.

markets have a natural tendency to tip towards monopolisation.[511] Moreover, because such dominance is persistent once the market has tipped, even in dynamic high-tech markets, there is thus "a strong *first-mover advantage* in data-driven markets, which leads towards monopolization and is built upon data-driven indirect network effects" (emphasis in the text).[512]

Such concentration risks had already been outlined by Benkler at the beginning of the century, who pointed to the fact that the infrastructure of, and the patterns of attention on, the internet may turn out to be much less distributed than what was promised by the decentralised ideology of the internet.[513] Indeed, he outlined that "a high degree of attention is concentrated on a few top sites – a tiny number of sites are read by the vast majority of readers, while many sites are never visited by anyone"[514], before adding, as a matter of example, in a quasi-prophetic statement that "Google could become so powerful on the desktop, in the e-mail utility, and on the Web, that it will effectively become a supernode".[515]

80. Due to these first-mover advantage and market tipping dynamics, data concentration might increase entry barriers for new firms and strengthen data aggregators' market power, leading to diminishing incentives for innovation.[516] Moreover, if the market has tipped and if the entry barriers are high, this will drastically reduce the threat of "creative destruction"[517], and the monopolistic incumbent will thus have fewer incentives to innovate in order to protect its monopoly position from a potential competitor who will be less likely to develop the "next big thing".[518] Indeed, as outlined by Prüfer:

> "The smaller firms, even if they are equipped with a superior idea/production technology, face higher marginal costs of innovation because they lack access to the large pile of user information that the dominant firm has access to due to its significantly larger user base. Consequently, if a smaller firm were to heavily invest in innovation and roll out its high-quality product, the dominant firm could imitate it quickly – at lower cost of innovation – and regain its quality lead. The smaller firm would find itself once again in the runners-up spot, which entails few users and low revenues, but it would still have to pay the large costs involved in attempting a leap in innovation. Foreseeing this situation, no rational entrepreneur would invest in innovation in a smaller firm. In turn, because the dominant firm knows about the

---

[511] See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf, p. 6-9; J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*., p. 2.
[512] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*., p. 2.
[513] Y. Benkler, *The Wealth of Networks. How Social Production transforms Markets and Freedom*, New Haven, Yale University Press, 2003, p. 214.
[514] *Ibid*., p. 235.
[515] *Ibid*., p. 261.
[516] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 24. See also J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*
[517] See J. Schumpeter, *The Theory of Economic Development: an Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*, Harvard University Press, 1932.
[518] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 71. See also M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*., p. 281-285.

disincentive to innovate among its would-be competitors, it is protected by its large (and constantly renewed) stream of user information and can remain content with a lower level of innovation, too".[519]

81. Such concentration may also establish long-term competitive advantages and this could endanger the contestability of these data driven markets.[520] This notably derives from the positive feedback loops mentioned above[521], as "initially superior access to data may give rise to feedback effects, such that data-driven competitive advantages are magnified over time as improved service quality from data leads to more users and this then turns into access to even larger data sets".[522] Because competitors cannot have the same continuous inflow of data as the incumbent data holder – which benefits from self-reinforcing data driven network effects and economies of scope, scale and speed –, it will lack the ability to adapt its good or services to the users changing desires and it will thus struggle to be competitive.[523]

Moreover, the lack of contestability could stem from the fact that incumbent data holders could leverage such data concentration phenomenon to exclude competitors from entering the market.[524] This might especially be the case if the incumbent's first mover advantage has allowed it to reach a monopolistic market position and that it retains an exclusive access on its data.[525]

Additionally, a lack of contestability could also stem from the fact that data concentration leads to an asymmetry of information between the incumbent data holder and smaller potential competitors, which might distort the latter's efficient decision-making and thus reduce their competitive counterweight.[526] To some extent, this asymmetry of information problem is however tackled by transparency and fairness initiatives such as the Regulation on the Free-flow of non-personal data[527] and the Platform to Business Regulation[528].[529]

82. Finally, it should be added that, more recently, the incumbent data holders have developed an alternative way of aggregating data and reinforcing this concentration phenomenon. They have started to offer ancillary services to third parties, such as identity management services

---

[519] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 6. See also J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2.
[520] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 55.
[521] See point 73.
[522] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 56.
[523] *Ibid*., p. 71.
[524] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 19.
[525] *Ibid*., p. 5.
[526] *Ibid*., p. 27.
[527] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018. See in particular Article 6 pertaining to the porting of non-personal data.
[528] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019; Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", *op. cit*.
[529] See below, Part II, Chapter 1, Section D.

("Login with Facebook", "Login with Google", "Sign in with Microsoft"), payment services ("Pay with Amazon", "Pay with Apple"), or tracking technologies ("Google Analytics", "Facebook Pixel"), which act as a new source of data for these incumbents.[530] Indeed, even if offering such ancillary services implies a loss of exclusivity on the incumbents' data as they have to reveal some of it in order for the third parties to be able to use the services, the user data that they obtain in return is far more valuable to them, as it allows them to also track these users, and thus gather more data about them, on websites that are operated by third parties.[531]

This subtler alternative mechanism of data collection thus also reinforces the incumbents' data driven network effects and also raises entry barriers. More specifically, and as outlined by Krämer *et al.*, in the short run, these third parties are incentivised to adopt these ancillary services in order to gain a competitive advantage on the ones who do not.[532] However, in the medium to long run, as the other third parties also start adopting these ancillary services, none of these third parties manages to gain a truly competitive advantage, and they are actually worse off than if they had refrained from adopting the ancillary service, as they have agreed to broad transfers of data towards the incumbent data holder. As a consequence, and from a dynamic perspective, the incumbents have in fact further strengthened their position through data concentration and competition is weakened.

ii. Data conglomerates and domino effects

83. These network effects and economies of scope, scale and speed may not only protect incumbent data holders in their core data driven markets by providing them with a competitive data advantage leading to data concentration, but they may also be leveraged by the incumbent to expand and strengthen its position in adjacent markets.[533] Accordingly, there are clear incentives for data driven firms to expand their activities in as many markets as possible and to build conglomerates.[534]

Indeed, the dominant position gained in a data driven market could be leveraged to gain a dominant position in a *connected market*, i.e. another distinct market in which the data gathered in the first market turns out to be a valuable input to improve the goods or services offered.[535] In fact, such expansion to a connected market could even reinforce the incumbent's position in the first market, if the data gathered on the second market is a valuable input to

---

[530] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 72-73.
[531] *Ibid*., p. 73.
[532] *Ibidem*. See also J. Krämer, D. Schnurr and M. Wohlfarth, "Winners, losers, and facebook: The role of social logins in the online advertising ecosystem", *Management Science*, 2019, Vol. 65(4), p. 1678-1699.
[533] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 56; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 19.
[534] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*
[535] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2-3.

improve the goods or services offered on the first market.[536] This is linked to the general-purpose nature of data, which can be re-used for a wide variety of goods and services.[537]

If these connected markets' dynamics are combined with the first mover advantage outlined above, this could lead to a *domino effect*, i.e. "a first mover in market A can leverage its dominant position, which comes with an advantage on user information, to let connected market B tip, too, even if market B is already served by traditional incumbent firms".[538] Indeed, once a firm has established a strong data position in one market, "the marginal costs of expanding into an adjacent complementary data domain are lower than for *de novo* entrants in that domain or incumbents who only cover that specific domain".[539] The domino effect deriving from this first mover advantage in an initial market could thus lead to successive market tipping in several connected markets. Indeed, venturing into related markets opens the access to more users, and thus consequently to more data, which will strengthen even more the incumbent data holder's data driven network effects, and this will, in turn, allow them to venture into further markets.[540] In time, this can lead to the constitution of digital conglomerates. Google, and its ability to leverage its dominant position in the search market to other connected markets (shopping, maps, etc.) is a prime example of such data conglomerate.[541]

84. To constitute these data conglomerates, incumbent data holders either rely on mergers and acquisitions[542], or on *envelopment strategies*, which are summarised in Eisenmann *et al*.'s seminal paper "Platform Envelopment":

> "Through envelopment, a provider in one platform market can enter another platform market, and combine its own functionality with that of the target in a multi-platform bundle that leverages shared user relationships. Envelopers capture market share by foreclosing an incumbent's access to users; in doing so, they harness the network effects that previously had protected the incumbent".[543]

The target platform can either be a complement, a substitute or functionally unrelated to the enveloping platform.[544] In the first case (complementary platform), the enveloper will be the most likely to succeed in situations where both platforms' users overlap significantly.[545] In the second case (substitute platform), the enveloper will be the most likely to succeed in

---

[536] *Ibidem*.
[537] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 10. On the general-purpose nature of data, see point 52.
[538] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2-3.
[539] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 24.
[540] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 71.
[541] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 11.
[542] *Ibid*., p. 4. For a discussion of the "killer acquisitions" issue, see p. 21-23.
[543] T. Eisenmann, G. Parker and M. Van Alstyne, "Platform Envelopment", *Strategic Management Journal*, 2011, Vol. 32(12), p. 1270.
[544] *Ibid*., p. 1279.
[545] *Ibid*., p. 1280.

situations where bundling leads to significant economies of scope.[546] In the third case (functionally unrelated platform), the enveloper will be the most likely to succeed in situations characterised by both significant users' overlap and high economies of scope deriving from bundling.[547] Additionally, it should be outlined that the envelopment strategy will be especially efficient if the users are unable to multi-home, i.e. to use multiple platforms at the same time.[548] That being said, even if the users multi-home, the enveloper can still gain a competitive advantage over the target platform.[549]

These envelopment strategies are widespread in the data driven markets, and have notably been used by Microsoft, Google, eBay or LinkedIn.[550] According to Condorelli and Padilla, some of these firms even engage in envelopment strategies through privacy policy tying[551], which is a strategy through which "the enveloper requests consumers to grant their consent to combining their data in both [the] origin and target market[s]".[552] This combination of data allows the enveloper to fund all of its services by monetising data from each of the services in all of the other services, and thus allows the enveloper to entrench its dominant position in the origin market and to expand it in the other markets.[553] This facilitates the domino effect mentioned above.[554]

85. While the constitution of such conglomerates could have pro-competitive effects, they might also entail various market failures, such as raising entry barriers for innovative entrants, which could in turn endanger the contestability of these markets on which the conglomerate is active.[555] This is well explained by Tirole:

> "A start up that may become an efficient competitor to such firms generally enters within a market niche; it's very hard to enter all segments at the same time. Therefore, bundling may prevent efficient entrants from entering market segments and collectively challenging the incumbent on the overall technology".[556]

Moreover, the conglomerate could also foreclose competition on some of the markets where it is active if these markets depend on the access to an essential resource, such as specific types of data, produced on a primary market where the conglomerate is also active and dominant,

---

[546] *Ibid*., p. 1281.
[547] *Ibid*., p. 1281-1282.
[548] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 16.
[549] *Ibid*., p. 17.
[550] T. Eisenmann, G. Parker and M. Van Alstyne, "Platform Envelopment", *op. cit.*, p. 1271.
[551] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", December 2019, available at https://ssrn.com/abstract=3504025. On this specific issue see Part III, Chapter 2, Section A.
[552] *Ibid*., p. 1.
[553] *Ibid*., p. 5.
[554] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 72.
[555] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 14.
[556] J. Tirole, "Federal Reserve Bank of Richmond: Econ Focus", Fourth Quarter 2017, available at www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2017/q4/interview.pdf, cited in M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 15.

and if the conglomerate refuses to provide access to this resource to its competitors and reserves its use for itself.[557]

In the same vein, the combination of conglomeration (through vertical integration) with the occupation of a gatekeeping position could entail market failures. As outlined by Krämer *et al*., this is especially the case in situations where an incumbent data holder is the gatekeeper of an upstream service and also offers downstream services via this upstream service (for example, Amazon operates an e-commerce website and also sells goods on it; Google operates a search engine and also offers other services (maps, shopping…) that are findable through that search engine).[558] As this incumbent is the gatekeeper to an important upstream service, third parties operating on downstream markets have to use the upstream service to reach consumers/users, but, in order to do so, they have to reveal key data about their business and their users to the incumbent. Yet, because the incumbent is also active on the downstream markets, these data flows provide it with a great deal of information about these third parties and their users, which seriously hampers their ability to compete with the incumbent on these downstream markets. Moreover, the incumbent's gatekeeper position does not only allow it to gain data advantages from its competitors, but also to favour its own downstream services, by steering the users towards them rather than towards the ones offered by third parties (self-preferencing).[559]

In this regard, the European Commission imposed, in June 2017, a fine of 2,4 billion euros on Google for having positioned and displayed more favourably on "Google Search" its shopping services over those of its competitors.[560] Similarly, the European Commission has opened an investigation in July 2019 against Amazon, which is suspected of using the data it gets from the sellers on its platform to launch competing products and of steering the consumers towards its own products.[561] In November 2020, the Commission sent a Statement of Objections to Amazon in this regard.[562] Unsurprisingly, and from a broader policy perspective, the European Commission wishes to ensure that platforms that have acquired significant scale and a systemic role, effectively allowing them to act as "private

---

[557] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 18-19. On these refusals to provide access to data, see Part III, Chapter 1.

[558] See J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 73-74.

[559] On this "frenemy" relationship between the incumbent and these third parties, see M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 293-297.

[560] European Commission, *Google Search (Shopping)*, 27 June 2017, AT.39740.

[561] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291. See also J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 74; D. Mattioli, "Amazon scooped up data from its own sellers to launch competing products", *The Wall Street Journal*, 23 April 2020.

[562] See https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077: "The Commission's preliminary findings show that very large quantities of non-public seller data are available to employees of Amazon's retail business and flow directly into the automated systems of that business, which aggregate these data and use them to calibrate Amazon's retail offers and strategic business decisions to the detriment of the other marketplace sellers. For example, it allows Amazon to focus its offers in the best-selling products across product categories and to adjust its offers in view of non-public data of competing sellers".

gatekeepers", will not endanger the fairness and openness of the markets.[563] In fact, it recently adopted a proposal for a Digital Markets Act[564], which notably contains a series of obligations and prohibited practices[565] for "gatekeepers"[566] offering "core platform services"[567], including the prohibition of some forms of self-preferencing.[568]

4. Benefits from sharing

86. In order to remedy the market failures deriving from the phenomena of data concentration and data conglomeration presented above, compulsory B2B data sharing is increasingly considered in numerous policy reports across the globe.[569] Indeed, it is presented by some

---

[563] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Shaping Europe's digital future*", Brussels, 19 February 2020, COM(2020) 67, p. 8.

[564] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.

[565] See Articles 5 and 6 of the Proposal for a Digital Markets Act.

[566] See Articles 2.1 and 3 of the Proposal for a Digital Markets Act. A data holder will be considered as gatekeepers if: "(a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future" (Article 3.1 of the Proposal). For more details on the designation of these gatekeepers, see points 397 and 398.

[567] See Article 1.2 of the Proposal for a Digital Markets Act. "Core platform services" are: "(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; (h) advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g)" (Article 2.2 of the Proposal). For a definition of these services, see Articles 2.5 to 2.11 of the Proposal.

[568] Gatekeepers shall refrain from using any data that is not publicly available and that has been provided or generated by the business users or their end users through their activity on the gatekeeper's core service, in order to compete with these business users (Article 6.1.a) of the Proposal for a Digital Markets Act). They shall also apply fair and non-discriminatory conditions to their ranking services and shall refrain from treating their own products/services more favourably than those of third parties (Article 6.1.d) of the Proposal).

[569] See (EU) J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*; (Germany) H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *Report by the Commission "Competition Law 4.0" for the German Federal Ministry for Economic Affairs and Energy*, 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competitionframework.pdf?__blob=publicationFile&v=2; (Germany) H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, Baden-Baden, Nomos, 2018 (also available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtigeunternehmen.html (an executive summary in English is available at https://ssrn.com/abstract=3250742)); (France) Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf; (BeNeLux) J. Steenbergen, M. Snoep and P. Barthelmé, "Joint memorandum of the Belgian, Dutch and Luxembourg competition authorities on challenges faced by competition authorities in a digital world", 2 October 2019, available at https://www.belgiancompetition.be/en/about-us/publications/joint-memorandum-belgian-dutch-and-luxembourg-competition-authorities; (UK) J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel; (UK) UK Competition & Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-

authors as the best solution to tackle the data concentration problem, as it reduces the incumbent data holder's data advantage derived from network effects and economies of scope, scale and speed since. Through data sharing, competitors get access to (some of) its data and can thus benefit from those same advantages and compete on the same basis.[570] As a consequence, fair competition would be stimulated.[571]

Similarly, sharing specific types of (essential) data could attenuate the anti-competitive effects of conglomerates by allowing competition to emerge and ensuring market contestability, as "compulsory access will allow entrants, on the one hand, to enjoy the same economies of scope in product development than the incumbent firm and, on the other hand, to generate demand-side synergies of similar magnitude when integrating the key [data] in their product ecosystems".[572]

In this regard, the European Commission has notably announced in its *Strategy for data* that it would explore legislative options in order to promote a wider sharing and availability of data, and to ensure that markets stay open and fair.[573] Indeed, the Commission realises that a number of large firms currently hold a significant part of the world's data, that this might diminish the incentives of smaller data-driven firms to emerge, grow and innovate, due to high entry barriers, and that the high degree of market power deriving from this "data advantage" could also affect the contestability of some markets.[574] In fact, the Commission's proposal for a Digital Markets Act contains several specific data sharing obligations.[575]

Naturally, compulsory B2B data sharing remedies are not the only option to tackle these concentration and conglomeration issues and other avenues are suggested in the legal doctrine, such as the imposition of non-discrimination obligations; structural breakups; preventing incumbent data holders from concentrating more data or forcing them to silo their data, in order to limit the self-reinforcing feedback loops and network effects mentioned above; or preventing "killer acquisitions" in order to hamper the conglomeration of these

---

advertising-market-study; (USA) Stigler Committee on Digital Platforms, "Final Report", September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report; (Australia) Australian Competition and Consumer Commission, "Digital Platforms Inquiry – Final Report", 26 July 2019, available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report. For a comparative analysis of some of these reports, see W. Kerber, "Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia", September 2019, available at https://ssrn.com/abstract=3469624; and S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", 31 March 2020, available at https://ssrn.com/abstract=3565491.

[570] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 5. See also C. Argenton and J. Prüfer, "Search engine competition with network externalities", *op. cit.*, p. 73-105; J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*; G. Parker, G. Petropoulos and M. Van Alstyne, "Digital Platforms and Antitrust", May 2020, available at https://ssrn.com/abstract=3608397.

[571] Support Centre for Data Sharing, "B.2 – Analytical report on EU law applicable to sharing of non-personal data", *op. cit.*, p. 4.

[572] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 30.

[573] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", Brussels, 19 February 2020, COM(2020) 66, p. 5 and 14.

[574] *Ibid*., p. 3 and 8.

[575] See Recitals 54 to 56 and Articles 6.1.h) to 6.1.j) of the Proposal for a Digital Markets Act. On these obligations see points 169, 182 and 382. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.

incumbent data holders and the domino effect.[576] However, as this thesis focusses on compulsory B2B data sharing, these alternatives will not be further detailed here.

87. The economic benefits of data sharing are, however, not limited to potentially solving the market failures deriving from the phenomena of data concentration and data conglomeration outlined above. Because data is non-rivalrous and can be used for many different purposes, sharing data entails economic welfare gains.[577] Moreover, data sharing also creates economies of scope in data re-use, as it allows recipients to aggregate various datasets and thus provides them with a wider range of data.[578] Moreover, as outlined by the United Kingdom's Open Data Institute, there are several key business benefits in sharing data, such as "improving market reach; supporting benchmarking and insights; driving open innovation; driving supply chain optimisation; addressing sector challenges; and building trust".[579] This perspective of substantial welfare gains deriving from these key business benefits and from the exploitation of the non-rivalrous nature of data is at the core of the data sharing debates.[580]

Indeed, data sharing has a fundamental role to play in the "European Data Economy".[581] This is notably apparent from the "European Data Market Study Monitoring Tool", which identifies three potential scenarios for the evolution of the European Data Market (Baseline, High Growth and Challenge scenarios), and which identifies the amount of data sharing as one of the factors that will influence this concrete evolution (low data sharing will lead towards the Challenge scenario, while high data sharing will lead towards the High Growth scenario).[582] In turn, this will have an impact on the value of the Data Economy, which is

---

[576] On these alternative remedies, see *inter alia*, J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*; United States House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets – Majority Staff Report and Recommendations", 2020, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf; J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data: On Data-specific Theories of Harm and Remedies", *Max Planck Institute for Innovation and Competition Research Paper No. 19-05*, 31 May 2019, available at https://ssrn.com/abstract=3364792; OECD, "Lines of Business Restrictions – Background note", 8 June 2020, DAF/COMP/WP2(2020)1, available at https://one.oecd.org/document/DAF/COMP/WP2(2020)1/en/pdf. See also Articles 3.8, 5 and 6 of the Proposal for a Digital Markets Act.

[577] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 4. Massive sharing of personal data can however entail long-term losses of control for the individuals (see Part I, Chapter 2, Section C, b)).

[578] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.

[579] Open Data Institute, "Sharing data to create value in the private sector", 2020, available at https://theodi.org/article/report-sharing-data-to-create-value-in-the-private-sector/, p. 4.

[580] B. Martens, "An economic perspective on data and platform market power", *op. cit.*, p. 6.

[581] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Towards a thriving data-driven economy*", Brussels, 2 July 2014, COM(2014) 442 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A Digital Single Market Strategy for Europe*", Brussels, 6 May 2015, COM(2015) 192 final; Communication from Commission, "*Building a European Data Economy*", *op. cit.*; Communication from the Commission, "*Towards a common European data space*", *op.cit.*; Communication from the Commission, "*A European strategy for data*", *op. cit.*; Communication from the Commission, "*Shaping Europe's digital future*", *op. cit.*

[582] International Data Corporation and the Lisbon Council, "The European Data Market Study Monitoring Tool – Final Study Report", June 2020, SMART 2016/0063, available at http://datalandscape.eu/, p. 8-9.

expected to reach, by 2025, 432 billion euros in the Challenge scenario, 550 billion euros in the Baseline scenario and 827 billion euros in the High Growth scenario.[583]

88. Finally, data sharing is key for the development of a competitive artificial intelligence landscape and is therefore a cornerstone of the European Commission's "Coordinated Plan on Artificial Intelligence".[584] Indeed, data is a vital input for the development of machine learning technologies (a form of artificial intelligence), as their learning capabilities are directly function of the amount of data they can be trained on. Following-up on this objective, the Commission has outlined, in its *Strategy for data*, that it will strive for the creation of "Common European data spaces", in fields such as manufacturing, energy and health, whose aim will be to aggregate public and business data in order to make them accessible to recipients wishing to use these data to train their machine learning technologies.[585] The aim is to facilitate innovation through data re-use and through the fostering of appropriate technical standards and interoperability requirements.[586] These European data spaces should lead to the availability of large pools of data in strategic economic sectors such as the industrial manufacturing and the financial sectors.[587] To support the establishment of these European data spaces, the European Commission has adopted a proposal for a Data Governance Act, which aims at creating an overarching framework encompassing horizontal measures relevant for all Common European data spaces.[588]

5. Need for a balance between the benefits and costs of data sharing

89. While data sharing presents numerous benefits, it does not come without a cost.[589] Indeed, data collection and processing, and consequently data sharing, entails costs for the data holder, and data sharing obligations might create disincentives for data collection and processing.[590] This is because imposing data sharing might deter innovation by the data holder that is compelled to share its data, as it might no longer want to invest in data collection that used to provide him with a competitive advantage, due to the fear of free-riding that derives from the non-rivalrous nature of data.[591] Moreover, imposing data sharing might also deter innovation by third parties who will no longer see the point in innovating in order to collect the data themselves, as they will receive it from the data holder (expectation to free-ride).

---

[583] *Ibid*., p. 9.
[584] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Coordinated Plan on Artificial Intelligence*", Brussels, 7 December 2018, COM(2018) 795 final, p. 6-7.
[585] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 5; Communication from the Commission, "*Coordinated Plan on Artificial Intelligence*", *op. cit*., p. 7.
[586] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 12.
[587] *Ibid*., p. 22-23. These strategic economic sectors are further detailed in the Appendix of the "European strategy for data" (see p. 26-34).
[588] Proposal for a Data Governance Act, p. 6. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*
[589] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.
[590] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 76-77.
[591] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 374. Importantly however, these incentive costs might be quite low if the data has been collected as a by-product of the data holder's core economic activity, rather than as the object its core economic activity. See points 12 and 304.

Indeed, while allowing data re-use will not functionally affect the data holder's ability to keep using the data herself, it may have an economic impact on the data holder's business, depending on whether the re-use is complementary or substitutable to it.[592] If the recipient uses the data to develop a substitutable good/service to that of the data holder, this might negatively affect the data holder's business. It will thus not be willing to share the data. On the contrary, if the data recipient uses the data to develop a complementary good/service to that of the data holder, this new good/service might increase the demand for the data holder's good or service and thus positively affect her business. The recipient's good/service could also be purely neutral towards the data holder's good/service, in which case the data holder will have an interest in sharing the data against a price.

While this distinction seems quite straightforward in theory, it will rarely be clear in practice whether the recipient will use the data to develop a substitutable, complementary or neutral good/service.[593] Indeed, a complementary good/service could, in fact, end up becoming a substitute good/service, due to the evolution of the users' needs and expectations.[594] This uncertainty explains why data sharing has not taken off at sufficient scale, as data holders fear to lose the competitive edge they derive from their "data advantage", because they do not trust the recipients and fear that they might misappropriate "their" data.[595]

90. Accordingly, any regulatory initiative must consider this balance between the benefits and costs of data sharing.[596] The efficiency gains stemming from sharing (increased competition and innovation from third parties) shall be carefully weighed against the efficiency gains stemming from the data holder's data-driven network effects and economies of scope, scale and speed.[597] Maximising data sharing should thus not be an objective in its own right, and data sharing obligations should only be imposed if the benefits it creates trump the related costs.[598] This fits in the broader balancing between private and public/social interests and requires a case-by-case analysis.

In evaluating this balance, inspiration can be drawn from the classic balancing exercise, underlying the allocation of intellectual property rights, between the need to incentivise creation/innovation, on the one hand, and the benefits from a large dissemination of these creations/innovations, on the other hand.[599] Indeed, as pointed out by Martens, data economics issues are very similar to the intellectual property rights' law and economics

---

[592] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 20-21.
[593] *Ibid*., p. 5.
[594] See L. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. Valletti and M. Van Alstyne, "The EU Digital Markets Act: A Report from a Panel of Economic Experts", *EU Science Hub*, 2021, available at https://ec.europa.eu/jrc/en/publication/eu-digital-markets-act, p. 26.
[595] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 7.
[596] P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *op. cit.*, p. 616-620; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.
[597] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 75.
[598] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 12.
[599] See *supra* points 33 to 43.

issues, as they struggle with the same balancing act "between the social welfare costs of monopolistic exclusive rights and the social welfare gains from the innovation incentive effects".[600]

However, it should be pointed out that, as data are non-rivalrous, capital and general-purpose resources whose use creates spill overs in multiple fields across society[601], and as data are potentially (technically and contractually) excludable – making them closer to "club goods" than to "public goods" –[602], the benefits of data sharing may arguably be greater than the benefits of sharing other resources, and the costs of data sharing may arguably be smaller than the costs of sharing other resources.[603] This serves as an economic rationale for more data sharing.

91. Finally, reaping the potential benefits deriving from data sharing will only be acceptable if this is done in compliance with the right to privacy[604] and to personal data protection[605] of the individuals whose personal data would be shared.[606] Indeed, as outlined by the European Data Protection Supervisor, a cautious approach should be taken towards initiatives aimed at compulsory access to / sharing of personal data, as such sharing/access must comply with other policy concerns, especially personal data protection.[607]

---

[600] B. Martens, "An economic perspective on data and platform market power", *op. cit.*, p. 23.
[601] See point 52. B. Frischmann, *Infrastructure: The Social Value of Shared Resources*, Oxford, Oxford University Press, 2012, cited in OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 179; J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 3; M. Madison, "Tools for Data Governance", *op. cit.*, p. 40.
[602] M. Madison, "Tools for Data Governance", *op. cit.*, p. 34; M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 45.
[603] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 31; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", Report for the German Federal Ministry for Economic Affairs and Energy*, 29 August 2018, available at https://ssrn.com/abstract=3250742, p. 10. See also J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*
[604] Article 7 of the Charter of Fundamental Rights of the European Union, *OJ C 326/391*, 26 October 2012.
[605] Article 8 of the Charter of Fundamental Rights of the European Union, *OJ C 326/391*, 26 October 2012.
[606] See European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf, p. 8. See Part III, Chapter 2 and Chapter 3, Section B, b).
[607] *Ibid*., p. 12.

Section C. The societal and the "empowerment" rationale for data sharing

92. While the focus, at the European level, is usually set on the economic rationale for data sharing, which was analysed in Section B, data sharing could also be justified by other objectives. On the one hand, it could support broader societal objectives.[608] On the other hand, it could support individual "empowerment" objectives.[609]

a) Societal rationale for data sharing

93. As outlined in the European Commission's *Strategy for data*, "making more data available and improving the way in which data is used is essential for tackling societal, climate and environment-related challenges, contributing to healthier, more prosperous and more sustainable societies".[610] Indeed, more access to data through data sharing can foster more transparency, more security and it can support research.[611] The underlying idea is that not only public sector data, but also private sector data, can make a significant contribution to the common good.[612] In this regard, the Commission has set to support the development of a series of "Common European data spaces", which should lead to the availability of large pools of data in domains of public interest such as environmental protection, health, mobility, energy and agriculture.[613] To support the establishment of these European data spaces, the European Commission has adopted a proposal for a Data Governance Act, which aims at creating an overarching framework encompassing horizontal measures relevant for all Common European data spaces.[614] Articles 15 to 22 of this Data Governance Act notably contain measures aiming at facilitating voluntary data sharing in the common good ("data altruism").

In terms of environmental protection, increased data sharing between businesses would notably allow them to better understand the environmental impact of each step of the supply chain, in order to identify the friction points where they could act in order to reduce the pollution deriving from their activity, thus contributing to Europe's goal to become climate-neutral by 2050.[615] Moreover, increased data sharing, notably with NGOs, could allow the identification of priority actions to be undertaken in order to address fundamental issues such as deforestation, the loss of biodiversity and the management of hazardous waste.[616] In the energy sector, B2B data sharing about the result of innovative experiments aiming at decarbonising the existing energy systems could generate significant environmental benefits, by accelerating the transition towards greener energy production.[617] It could also allow

---

[608] See Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 3.
[609] *Ibid.*, p. 10. See also p. 20-21.
[610] *Ibid.*, p. 3.
[611] Support Centre for Data Sharing, "B.2 – Analytical report on EU law applicable to sharing of non-personal data", *op. cit.*, p. 4.
[612] See Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 6.
[613] *Ibid.*, p. 22-23. These domains of public interest are further detailed in the Appendix of the "European strategy for data" (see p. 26-34).
[614] Proposal for a Data Governance Act, p. 6. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*
[615] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 26-27.
[616] *Ibid*em.
[617] See Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 31.

undertakings to share information about the energy consumption of certain processes or machines that they use, in order to optimise the efficiency of their energy consumption. Additionally, increased sharing of data about the quality of the air and about the rejection of polluting materials could also enable third parties to develop services recommending, or on the contrary advising against, certain leisure activities for more fragile people in certain specific places.

In terms of mobility, data sharing between navigation technology service providers and freight and logistics businesses can assist the latter in their transition towards more sustainable transport services, as economies of scale can be reached if some travels are rationalised, while also making this transport more efficient and secure.[618] Furthermore, data sharing between transport service providers (trains, buses, trams, shared cars, bikes, scooters, etc.) and mobility information service providers could allow the latter to provide suggestions to individuals on how to get the fastest from point A to point B, by relying on multimodal transportation (e.g. taking a train, then a bus, then a shared bike). This could notably take the form of a "multimodal mobility open data platform", in order to "facilitate cooperation between different actors involved in mobility issues, establishing the basis for future development of Mobility as a Service (MaaS) concepts for citizens".[619] Such a platform, built on B2B data sharing, would indeed allow the gathering and provision of data from various transport modes, and would notably enable the individuals to opt for the most sustainable ones.

Another interesting example could be the combination of navigation and location data, collected by navigation technology service providers, with data from other sources. This would notably allow the development of ride-sharing services for elderly people who have difficulties moving on their own, such as a shuttle bus service powered by data analytics that calculate and determine the optimal allocation of users between buses and the most efficient routes to bring them to their destination.[620] In fact, such an initiative could even further be combined with the sharing of data with parcel delivery companies, as these shuttle buses could also be used to deliver parcels, for example if a parcel has to be delivered in the same street as the one where a person is being picked up in the context of the ride-sharing service. This would contribute to two important societal objectives, namely reducing the environmental footprint of transport services, as well as improving mobility by reducing traffic congestion.

Similar objectives could also justify the exchange of data between car manufacturers, navigation system providers, fleet managers and parking operators, in order to develop "smart parking" services, as "drivers looking for a parking spot cause about one-third of traffic in city centres".[621] Through such data exchange, a driver looking for a parking spot could be

---

[618] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 28. See also https://www.aisin.com/en/product/mobility/cs-s/

[619] See https://www.bable-smartcities.eu/explore/use-cases/use-case/useCase/open-platform-for-multimodal-mobility-information-and-services.html

[620] See https://www.aisin.com/en/product/mobility/cs-s/

[621] See https://erticonetwork.com/saving-time-and-reducing-costs-thanks-to-smart-parking/

quickly and efficiently informed about the nearest parking availability and be instantly redirected to it by her navigation system. If deployed at a large scale, this would limit the pollution deriving from CO_2 car emissions and would also pursue mobility objectives, by reducing the number of cars on the network.

Regarding healthcare, data sharing can contribute to the prevention, diagnosis and treatment of certain diseases (such as cancer, rare diseases and complex diseases), notably through the sharing of information about the safety and efficacy of medical products and medicines, and can further support research and innovation.[622] In this regard, it is worth mentioning here the Finnish Act on the Secondary Use of Health and Social Data[623], which compels certain private and public health service providers and social service providers to pool together some of their health and social data, under the supervision of a government agency, in order to make it accessible for research, steering, statistics, supervision and development in the health and social sectors.[624] Moreover, if food and drink companies were to share data about the contents of their products (for instance whether they contain gluten, lactose or certain allergens), this could allow third parties to offer dietary services to individuals, by recommending to them products that are healthier, that are gluten-free, that do not contain traces of peanuts, etc.

B2B data sharing can also prove to be vital in order to tackle global pandemics, such as the COVID-19 pandemic. For instance, the sharing, between healthcare institutions and emergency services, of data pertaining to the bed occupation rate of the healthcare institutions' intensive care units would allow to better distribute the arrival of new patients in order to ensure that each and every one receives the best care possible in a timely fashion. Similarly, the sharing, between pharmaceutical companies, healthcare institutions and research institutions, of data pertaining to vaccine/medicine trial results could allow to rapidly abandon trials that lead to unsatisfactory results, or on the contrary to highlight promising results, in order to address such global healthcare challenges caused by pandemics as fast as possible.

In the agricultural sector, sharing production data, supply chain data and other types of data, such as earth observation or meteorological data, would allow the actors of the sector to apply more tailored and precise production approaches.[625] Indeed, farmers increasingly make use of various sensors in order to improve the efficiency of their operations. These can be weather stations, humidity sensors, soil scanners, crop sensors, etc.[626] The latter notably enable the monitoring of the health of crops, as well as to detect plant diseases at an early stage. Accordingly, the sharing of such data pertaining to the apparition of a disease with nearby farmers, which might not be aware of the problem, would contribute to the prevention of food waste, by enabling the farmers to address the issue rapidly and to limit the loss of crops.

---

[622] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 29-30.
[623] For more information on this Act, see https://stm.fi/en/secondary-use-of-health-and-social-data
[624] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 33.
[625] *Ibidem*.
[626] Everis, "Study on data sharing between companies in Europe – Case studies", *Study for the European Commission*, 2018, available at https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en, p. 43.

Similarly, B2B data sharing about the efficiency of a certain type of pesticide and the appropriate dose to be sprayed could reduce the environmental footprint of such practices, by avoiding "over-spraying". Furthermore, if "smart farming" data was shared with NGOs, this could allow the latter to pass on this knowledge to farmers in developing countries and to suggest to them tailored cultivation strategies that are the most efficient for specific climates or soils.

94. As illustrated by the numerous examples mentioned above, which are by no means exhaustive (including in terms of the sectors covered), it is clear that B2B data sharing can significantly contribute to the realisation of several societal objectives. Interestingly, this societal rationale for data sharing seems to receive a large adherence from all categories of actors, as 91.5% of the respondents to the Commission's public consultation on its *Strategy for data* agreed that more data that are useful for the common good (e.g. for improving mobility, delivering personalised medicine, reducing energy consumption and/or contributing to a greener society) should be made accessible.[627] Naturally, such sharing for the common good would have to be respectful of people's privacy and right to personal data protection[628], and it would have to be ensured that it would not reinforce existing (or create new) situations of data oligopoly by a limited number of large data holders.[629]

95. It is thus clear that data sharing can generate societal benefits. In contrast, this implies that a lack of data sharing, deriving from data concentration and conglomeration, will not only create economic challenges, but also societal challenges. Indeed, as outlined by Shkabatur:

> "Companies such as Google, Facebook, Apple, and eBay have amassed more data about people and their behavior, health, markets and networks than many governments and organizations around the globe. This data could enlighten us about ourselves, and instruct us on various matters, such as how to improve our health [or] make better informed political decisions".[630]

As the societal value of the data held (exclusively) by some incumbent data holders is enormous, allowing (some) third parties to use this data could generate immense scientific, environmental, health and mobility benefits for our society.[631] Accordingly, for Shkabatur, a just, fair and equal access to (some) of the data that these incumbents hold would be necessary to avoid socio-economic disparities and inequalities of opportunity.[632]

96. Yet, and as for the economic benefits of sharing[633], these societal benefits would have to be balanced with the corresponding costs for the data holder (notably in terms of incentives for data collection and production), when considering whether to impose B2B data sharing

---

[627] European Commission, "Summary Report on the open public consultation on the European strategy for data", 24 July 2020, available at https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-european-strategy-data, p. 2.
[628] See point 91.
[629] European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, *op. cit.*, p. 8.
[630] J. Shkabatur, "The Global Commons of Data", *Stanford Technology Law Review*, 2019, Vol. 22, p. 357.
[631] *Ibid*., p. 383. See point 93 for some examples.
[632] *Ibid*., p. 401-402.
[633] See points 89 and 90.

obligations for societal purposes. In this perspective, the requirements of necessity and proportionality entail that such compulsory data sharing should only be imposed if less stringent alternatives, such as *voluntary* data sharing for societal purposes/the common good[634], turn out to be insufficient to achieve the desired societal objectives, or if it is highly important and/or urgent to achieve these objectives.[635] This will be further analysed below.[636] Nevertheless, it can already be outlined here that if the rationale for data sharing is societal rather than economic, the incumbent data holder's costs may weigh less heavily in the balance, as they are opposed to fundamental societal objectives that could be viewed as superseding "mere" economic considerations. However, reaping the potential societal benefits deriving from data sharing will only be acceptable if this is done in compliance with the right to privacy and to personal data protection of the individuals whose data would be shared.[637]

b) The "empowerment" rationale for data sharing and its impact on individuals' autonomy and self-determination

97. Data sharing is also increasingly presented as a way to "empower" individuals, by giving them more control on "their" data through tools and means allowing them to decide, at a much more granular level, what can be done with it.[638] The underlying idea is that data sharing can optimise the individuals' control over their data by allowing them to securely share it with third parties, in order to be offered better services, more choice and lower prices.[639] As a result, individuals would thus be empowered to compare services, to multi-home and to switch more easily between them, as this would reduce their searching and switching costs.[640] Indeed, it is argued that, at the moment, there is a strong consumer inertia which creates a barrier to entry and expansion for new actors wishing to offer alternative services, as simply providing information about these services (notably about the fact that they are cheaper than the incumbent's service) is not sufficient to convince the consumers to switch.[641] This is because consumers do not always have the necessary background to understand all of this information. Moreover, "consumer decision-making can be affected by a range of factors which reinforce inertia, such as high searching and transaction costs (either real or perceived), behavioural biases and contextual factors, but also by firms' strategic conduct aimed at exploiting these biases and poor consumer information by increasing

---

[634] See, in this regard, Articles 15 to 22 of the Proposal for a Data Governance Act.
[635] H. Richter, "The Law and Policy of Government Access to Private Sector Data ('B2G Data Sharing')", *Max Planck Institute for Innovation and Competition Research Paper No. 20-06*, 2020, available at: https://ssrn.com/abstract=3594109, p. 22.
[636] See Part III, Chapter 4.
[637] See point 91 and Part III, Chapter 4. See European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, *op. cit*., p. 8.
[638] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 10. See also p. 20-21.
[639] See point 183. Open Data Institute and Fingleton, "Open Banking, Preparing for lift off: Purpose Progress and Potential", 16 July 2019, available at https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf, p. 6.
[640] Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit*., p. 4; O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking", 3 January 2020, available at SSRN: https://ssrn.com/abstract=3513514, p. 4 and 12.
[641] See point 172. O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance", *op. cit*., p. 1 and 6.

searching and switching costs, thus taking advantage of these demand-side problems in order to weaken competition".[642]

This individual "empowerment" is an important policy goal for the European Commission, and it constitutes one of the four pillars of its *Strategy for data*, as "this promises significant benefits to individuals, including to their health and wellness, better personal finances, reduced environmental footprint, hassle-free access to public and private services and greater oversight and transparency over their personal data".[643] Indeed, this control that data subjects can (re)claim on their data is fundamental as it will also allow them to exercise a series of other rights, such as their freedom of information[644], and its deriving right of access to information (covering both personal and non-personal data).[645] Such access to information is important because it can improve the recipients' decision-making and, consequently, their ability to exercise other rights (right to health[646], right to environmental protection[647], right to move freely[648], etc.) and to take fundamental decisions about all aspects of their life.[649] Indeed, access to information about the processing of "their" personal data by a data controller[650] allows individuals to exercise their data subject rights;[651] and access to suitable health and environmental information allows them to take informed decisions regarding their place of living.[652] More control on their personal data also allows individuals to better understand how they are "profiled" and why they are offered a specific type of advertisement,

---

[642] *Ibid*., p. 2.
[643] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 10.
[644] Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950; Article 11 of the Charter of Fundamental Rights of the European Union, *OJ C 326/391*, 26 October 2012.
[645] ECtHR, *Youth Initiative for Human Rights v. Serbia*, 25 June 2013, App. No. 48135/06, §§ 20 and 24; D. Voorhoof, "Freedom of expression and the right to information: Implications for copyright", *Research Handbook on Human Rights and Intellectual Property*, C. Geiger (ed.), Cheltenham, Edward Elgar, 2015, p. 337. See also C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 555-579.
[646] See Article 25 of the Universal Declaration of Human Rights, signed in Paris on 10 December 1948; Article 12 of the International Covenant on Economic, Social and Cultural Rights, 16 December 1966; Article 35 of the Charter of Fundamental Rights of the European Union, OJ C 326/391, 26 October 2012.
[647] Article 37 of the Charter of Fundamental Rights of the European Union, OJ C 326/391, 26 October 2012.
[648] See Article 5 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950; Article 2 of Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, securing certain rights and freedoms other than those already included in the Convention and in the first Protocol thereto, as amended by Protocol No. 11, signed in Strasbourg on 16 September 1963; Article 45 of the Charter of Fundamental Rights of the European Union, OJ C 326/391, 26 October 2012.
[649] See C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *op. cit.*, p. 555-579; ECtHR, *Guerra et al. v. Italy*, 19 February 1998, App. No. 14967/89, § 60; ECtHR, *McGinley and Egan v. United Kingdom*, 9 June 1998, App. No. 21825/93 and 23414/94, § 97 and 101; ECtHR, *Roche v. United Kingdom*, 19 October 2005, App. No. 32555/96, § 162 and 165.
[650] "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4.7 of the GDPR).
[651] Articles 13 to 22 of the GDPR; C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *op. cit.*, p. 569.
[652] C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *op. cit.*, p. 573-576; ECtHR, *Guerra et al. v. Italy*, 19 February 1998, App. No. 14967/89, § 60; ECtHR, *McGinley and Egan v. United Kingdom*, 9 June 1998, App. No. 21825/93 and 23414/94, § 97 and 101; ECtHR, *Roche v. United Kingdom*, 19 October 2005, App. No. 32555/96, § 162 and 165.

search result or content.[653] It should also allow them to understand why they are presented with certain news feed, which may influence their political and democratic choices, as illustrated by the Facebook/Cambridge Analytica scandal. In the same vein, increased access to museum collections via virtual visits through their websites can contribute to the individual's right to culture, and the increased availability of open access lectures by university professors, of recordings of conference presentations, and of open access scientific contributions can all contribute to the individuals' right to education.[654]

Moreover, access to information about a product's environmental footprint (origin, composition, durability, re-use and repair possibilities, recycling at the end-of-life, etc.) allows individuals to make conscious decisions in order to contribute to the protection of the environment by adopting more sustainable habits.[655] For instance, individuals could be inclined to buy food that has been produced in their region, to buy clothes that are made from recycled or second hand materials, or to buy products that are more easily repairable, all of which would contribute to a cleaner environment.

In the field of mobility, access to more information about both the public and private transport operators would enable the offer of more efficient, green and customer friendly multi-modal travel options to individuals.[656] Furthermore, information about traffic jams could also enable the individual to better organise her day, by articulating home-office and normal office hours in order to avoid losing too much time during the commute from home to work and vice-versa.

Additionally, increasing the individuals' access to health data should "improve access to and quality of care, cost effectiveness of care delivery and contribute to the modernisation of health systems".[657] In the same vein, access to information about the most common symptoms of a pathology or about the spread of a new disease can allow the individuals to detect potential issues earlier, in order to improve their chances of being treated in due time and of healing, or to reduce the risks of catching a disease.

The main instrument aiming at achieving this "empowerment" objective is the personal data portability right granted by Article 20 of the General Data Protection Regulation (hereafter "GDPR")[658], to which this thesis will revert further.[659] However, this objective is being increasingly pursued through several tools – such as consent management tools, personal data spaces / personal information management systems (PIMS)[660] or personal data trusts –[661], and

---

[653] See Articles 13.2.f) and 14.2.g) of the GDPR, which grant to the data subject the right to receive meaningful information about the logic involved in automated decisions, including profiling, pertaining to her.
[654] See also the examples mentioned at point 50.
[655] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 27.
[656] *Ibid*., p. 28.
[657] *Ibid*., p. 29.
[658] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), *OJ L 119*, 4 May 2016.
[659] See Part II, Chapter 1, Section A. See also the Digital Content Directive (Part II, Chapter 1, Section B, a)), PSD2 (Part II, Chapter 1, Section B, b)) and the Electricity Directive (Part II, Chapter 1, Section B, c)).
[660] See points 109 and 174. See, for instance, https://www.midata.coop/; https://mydata.org/; http://mesinfos.fing.org/selfdata/; https://solidproject.org/; https://www.decodeproject.eu/.

through several initiatives such as the Open Banking[662], Open Finance[663] and Smart Data[664] initiatives in the UK, which are, however, often still in their infancy.[665]

98. While legislators and policy makers usually heavily focus on the positive aspects of these "empowerment" tools and initiatives for the individuals[666], they must be careful not to be blinded by these benefits and should also pay great attention to the risks that they could entail in terms of personal autonomy and informational self-determination.[667]

The first reference to the individuals' right to informational self-determination can be found in a decision of the German Federal Court of December 1983 pertaining to the German Census Act (Volkszählungsurteil)[668], where the Court derived it from Articles 1 and 2 of the German Constitution, protecting human dignity, self-determination and the right to freely develop one's personality, which are foundational to the concept privacy.[669] The Court defined this right as "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about private life should be communicated to others".[670] Self-determination is thus "an elementary functional condition of a free democratic community based on citizens' capacity to act and collaborate".[671] It is linked with the autonomic capabilities of individuals, which relate to their capacity to make decisions on all aspects of their life and "to resist social pressures to conform with dominant views".[672]

In this regard, the right to personal data protection could, in fact, be seen as an intermediate tool for the preservation and promotion of this more fundamental value of autonomic self-determination.[673] Indeed, the GDPR grants to the data subjects[674] a certain number of rights[675], which strengthen their informational self-determination.[676] In fact, the aim of these

---

[661] On the concept of data trust, see point 112.
[662] See points 163 and 171.
[663] See points 165 and 171.
[664] See points 172 and 173.
[665] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 10.
[666] See Part II, Chapter 1, Sections A and B.
[667] See Preamble of the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, CM/Inf(2018)15-final.
[668] See German Federal Constitutional Court, *Volkszählungsurteil*, 15 December 1983, 1 BvR 209/83 et al., 65 BVerfGE 1.
[669] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", *Reinventing Data Protection: Proceedings of the International Conference (Brussels, 12-13 October 2007)*, Dordrecht, Springer, 2009, p. 45, 49 and 74; C. de Terwangne, "La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel", *Quelle protection des données personnelles en Europe?*, C. Castets-Renard (dir.), Bruxelles, Larcier, 2015, p. 91-92.
[670] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 45.
[671] *Ibid*., p. 47.
[672] *Ibid*., p. 46. See also C. Sunstein, *Why Societies Need Dissent*, Cambridge, Harvard University Press, 2003, p. 157-158.
[673] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 50.
[674] "*Any identified or identifiable natural person*" (Article 4.1 of the GDPR).
[675] Articles 13 to 22 of the GDPR.

rights is, among other things, to give data subjects a certain form of control[677] over "their" personal data and to ensure respect for human dignity in an increasingly technological environment. To do so, the data subjects' rights strive to address the information and power asymmetries between the data subjects and the data controllers.[678] Firstly, this right to informational self-determination is at the root of the adaptation of the right of access in the GDPR, which now explicitly provides that the data subject has the right to receive a copy of her personal data undergoing processing.[679] Secondly, the right to informational self-determination is also the basis of the right of the data subject to receive meaningful information about the logic involved in automated decisions pertaining to her.[680] Thirdly, the right not to be subject to a decision based solely on automated processing is also intended to promote informational self-determination and human dignity.[681] This right indeed echoes the strong desire of human beings not to be completely subjected to the machine, since they do not accept the idea that a decision may be imposed on them solely on the basis of conclusions reached by the machine, independently of any human intervention. Fourthly, the right of the data subject to object, at any time and on grounds relating to her particular situation, to profiling also promotes her right to informational self-determination.[682] Fifthly, the desire to establish a "right to be forgotten" is also rooted in the broader aim of strengthening the data subject's informational self-determination.[683] This is particularly relevant in light of the specificities of the Internet as, unlike in the physical world, erasure in the digital world will never be automatic and implies voluntary and well-considered action. Finally, the prime example of the promotion of informational self-determination in the GDPR is the right to personal data portability, enshrined in Article 20, which aims at strengthening the power of control that the data subjects have on "their" personal data.[684] This right to data portability will be further analysed below.[685]

99. This right to informational self-determination has traditionally been interpreted in an individual-centric way, in the sense that "controlling and manipulating information and data about oneself is an exercise of "self-determination".[686] As a result of this traditional interpretation, "in a context of pervasive possessive individualism and at a time where private property and the laws of the market are perceived as the most efficient ways to allocate

---

[676] On this right to informational self-determination in the GDPR, see T. Tombal, "Les droits de la personne concernée dans le RGPD", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 555-556; L. Somaini, "The right to data portability and user control: ambitions and limitations", *MediaLaws – Rivista dir. media*, 2018/3, p. 172.
[677] Recital 7 of the GDPR indeed provides that "natural persons should have control of their own personal data".
[678] L. Somaini, "The right to data portability and user control", *op. cit.*, p. 176.
[679] Article 15.3 of the GDPR.
[680] Articles 13.2.f) and 14.2.g) of the GDPR.
[681] Article 22 of the GDPR.
[682] Article 21.1 of the GDPR.
[683] Article 19 of the GDPR.
[684] Recital 68 of the GDPR.
[685] See Part II, Chapter 1, Section A.
[686] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 51.

rights[687], the right to "informational self-determination" has increasingly been understood as implying a sort of alienable property right of the individual over his personal data and information".[688] Yet, for Rouvroy and Poullet, this is a misunderstanding of this concept, as:

> "Information and data are not the pre-existing "elements" or "building blocks" of an individual's personality or "self". Such a conception would be misleading and unduly reductionistic: the "self" is not merely irreductible but also essentially different from "data" and "information" *produced about it*. What the expression "informational self-determination" means is rather that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said "self-determined". This is an important thing to recall today, as personal data have become *proxies* for persons" (emphasis in the text).[689]

Said otherwise, the individuals' right to informational self-determination should not only be understood as their ability to decide which information/data they share with whom, but also, and more fundamentally, as their right to understand and exercise control on who has their data, what is being done with it and how this impacts their life and their possibility to exercise their autonomy by making their own choices, as opposed to being subject to decisions made about them on the basis of personal data used as proxies and on which they might not have control.[690] Indeed, it is fundamental to take into account the "individuals' capacity for not doing or wanting everything which they are "statistically" predisposed to do or want, and to always assert their right to themselves account for their own motivations".[691] Some forms of opacity are indeed necessary to sustain the individuals' self-determination.[692]

100. Yet, as both public and private actors increasingly rely on ever-more invasive observation and monitoring technologies (Big Data, profiling, data mining, machine learning, etc.) as we shift towards a "(capitalism) surveillance society"[693], individuals, who are asked to share more and more data, become increasingly transparent and lose this opacity.[694] As a

---

[687] See point 29.

[688] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 51.

[689] *Ibidem*.

[690] *Ibid*., p. 56. See also C. de Terwangne, J.-P. Moiny, Y. Poullet et J.-M. Van Gyzeghem, "Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)", *Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD)*, T-PD-BUR(2010)09 (II) FINAL, Conseil de l'Europe, Strasbourg, 3 novembre 2010, p. 6; Y. Poullet, J.-M. Dinant, C. de Terwangne et M.-V. Perez-Asinari, "L'autodétermination informationnelle à l'ère de l'internet", *Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD)*, Conseil de l'Europe, Strasbourg, 18 novembre 2004.

[691] A. Rouvroy, ""Of Data and Men": Fundamental Rights and Liberties in a World of Big Data", *Report for the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)*, T-PD-BUR(2015)09REV, Council of Europe, Strasbourg, 11 January 2016, p. 37.

[692] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 58.

[693] See S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, New York, PublicAffairs, 2019.

[694] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 45-46.

result, they are increasingly subjected to (semi-)automatic decisions taken on the basis of the constant observation of their choices, behaviours and emotions, and therefore become "decreasingly capable of living by their fully autonomous choices and behaviours".[695] This feeling of loss of autonomy and control can be particularly strong when considering the large informational power of a few giant digital actors such as the GAFAM. In this regard, "empowerment" initiatives such as those mentioned above are sometimes presented as potential avenues to address this loss of autonomy and control, by offering more choices to individuals in the hope that they will get free from the clutches of these giant digital actors.[696]

However, great caution should be applied when considering the adoption of such "empowerment" initiatives. Indeed, "empowering" individuals by offering them more choice will not necessarily increase their control, autonomy and (informational) self-determination. In fact, if these "empowerment" initiatives are not strictly delineated, they might actually entail a high price and a loss of control for the individuals. Indeed, if, in the name of "empowerment", individuals are asked to divulge large quantities of data about themselves in order to be provided with more personalised choices, there is a risk that those data could be further disseminated with other actors, such as data brokers. This is notably due to the fact that there are strong informational asymmetries, as individuals "have no direct interaction with these data brokers, [and] they have no way of knowing the extent or nature of the information collected and sold for a multitude of reasons including fraud prevention, marketing and credit scoring".[697] This is fundamental to keep in mind because, due to these asymmetries of information "consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information".[698] Often, they will not know exactly which data will be used, for which purposes and whether these processing are truly necessary.[699] Moreover, "personal data may be used to influence individual decision-making in subtle, targeted, and hidden manners[700], raising questions over the limits of a person's autonomy and self-determination in a world where so much personal data can be gathered and used to influence the individual".[701]

As a result, an over-emphasis on the beneficial aspects of these "empowerment" initiatives could overshadow these risks, for individuals, of losing control and of becoming decreasingly capable of living by their fully autonomous and self-determined choices and behaviours. Therefore, it will be of paramount importance, when considering the adoption of such "empowerment initiatives", to exercise caution and to balance the potential short-term gains that are promised to individuals (e.g. getting a more tailored offer from an energy provider

---

[695] *Ibid*., p. 47.
[696] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 10. See also p. 20-21.
[697] A. Rouvroy, "'Of Data and Men'", *op. cit.*, p. 8.
[698] A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *Sloan Foundation Economics Research Paper No. 2580411*, 8 March 2016, available at https://ssrn.com/abstract=2580411, p. 3.
[699] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 68.
[700] See R. Calo, "Digital market manipulation", *George Washington Law Review*, 2014, Volume 82, Issue 4, p. 995-1051.
[701] A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *op. cit.*, p. 44.

based on my exact consumption)[702] with the potential long-term costs for these individuals in terms of control, autonomy and self-determination.[703] Indeed, it must be factored that data that has been shared by these individuals in exchange of these short-term gains, might, in the long-term, be broadly disseminated and/or be used against them, potentially leading to (price) discrimination, a loss of autonomy and the strengthening of a surveillance society[704].[705] This will be further developed below.[706] Moreover, such a large data dissemination would increase risks of potential data breaches, abuses and frauds.[707]

101. In addition to this short-term / long-term balancing exercise, it must also be underlined that protecting an individual's autonomy and self-determination is not only necessary for the individual itself, but also, more critically, for the "collective or societal interest in preserving a free and democratic society: individual autonomy and deliberative democracy presuppose a series of rights and liberties allowing individuals to live a life characterized as (partly at least) self-determined, self-authored or self-created, following plans and ideals that they have chosen for themselves".[708] Accordingly, the individuals' autonomy and their right to (informational) self-determination should not be conceived "as a liberty held in isolation by an individual living secluded from the rest of society but, on the contrary, as a right enjoyed as member of a free society".[709]

Therefore, when considering "empowerment" initiatives such as those mentioned above, it would be ill-advised to solely take an individual approach of the situation (e.g. offering more choice to a specific individual/consumer), without considering this necessary collective approach of autonomy and (informational) self-determination. Indeed, if this collective approach is overlooked:

> "The empowerment of individuals with regard to their personal data risks being interpreted as making the satisfaction of individuals' immediate preferences with regard to their personal data, their choice to keep it undisclosed or to commodify personal information a *final value*. It is well-known that those preferences would lead to a large part of the population to waive any protection of their personal data provided they receive immediate gratifications or commercial advantages. What would be lost in such an interpretation is the *intermediate value* of data protection as an instrument aimed at

---

[702] See point 166.
[703] For the analogous need to balance short-term gains and long-terms costs in competition law, see L. Khan, "Amazon's Antitrust Paradox", *Yale Law Journal*, 2017, Volume 126, Number 3, p. 710-805.
[704] See S. Zuboff, *The age of surveillance capitalism, op. cit*.
[705] A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *op. cit.*, p. 6 and 28 to 31.
[706] See Part II, Chapter 2, Section A, c).
[707] O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance", *op. cit.*, p. 10.
[708] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 55. See also G. Dworkin, *The Theory and Practice of Autonomy*, Cambridge, Cambridge University Press, 1988.
[709] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 57.

> fostering the autonomic capabilities of individuals and therefore not something they may dispose of or trade on the market of personal information" (emphasis in the text).[710]

Said otherwise, an individual's decision to share (or not to share) data will not only have an impact on her own autonomy and self-determination, but also on those of others. To understand why this is the case, one must first understand how the increasingly sophisticated technologies that are used to process growing amounts of data operate (e.g. Big Data analytics or artificial intelligence techniques such as machine learning). Indeed, these technologies exploit the relational and collective nature of data[711], as the focus is no longer on the individuals as such, but rather on their relations with one another and the profile they correspond to (i.e. their "statistical doppelganger").[712]

More concretely, the aim of these technologies is to draw models/categories, called "profiles" when referring to human behaviour, which are "dynamic patterns formed from correlations observed not in the physical world but among the digital data collected in diverse contexts, independently of any causal explanation".[713] The goal is thus not to describe the "truth" from the physical world, but rather to create operational models at the level of the digital world.[714] Importantly, these models/categories/profiles:

> "are built from data derived from large numbers of people, and since one person's data are no less (in)significant than another's when it comes to modelling, only a small amount of not-very-personal data are needed to produce "new" knowledge about any given individual, i.e. to infer certain pieces of information that bear no immediate relation to "their" personal data but which nevertheless enable them to be "categorised". In other words, when it comes to building a "profile", in order to be able to "capitalise" on the risks and opportunities that we present, our neighbours' data are as good as our own".[715]

Indeed, when an individual shares data about her own behaviour, habits and preferences, this also reveals significant information about her friends, family, neighbours as well as about any other people having similar characteristics.[716] This can be illustrated by the infamous Cambridge Analytica scandal, where the data disclosed by 270.000 users of the application called "This is your digital life" allowed Cambridge Analytica to infer detailed information about more than 50 million Facebook users and to use these insights to send targeted political messages to these Facebook users in order to influence the Brexit referendum and the 2016

---

[710] *Ibid*., p. 50.
[711] A. Rouvroy, "*Homo juridicus* est-il soluble dans les données ?", *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 429.
[712] A. Rouvroy et T. Berns, "Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?", *Réseaux*, 2013, Volume 177, Issue 1, p. 168, 180 and 184.
[713] A. Rouvroy, ""Of Data and Men"", *op. cit.*, p. 10-11.
[714] *Ibid*., p. 12.
[715] *Ibid*., p. 22. See also A. Rouvroy and B. Stiegler, "The Digital Regime of Truth: From Algorithmic Governmentality to a New Rule of Law", *Online Journal of Philosophy*, 2016, Number 3, p. 9.
[716] D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Too much data: prices and inefficiencies in data markets", *NBER Working Paper No. 26296*, 2019, available at https://www.nber.org/system/files/working_papers/w26296/w26296.pdf, p. 1.

US presidential election.[717] This illustrative example, which is only the tip of the iceberg, reveals that "the very nature of predictive big data approaches is to forecast the behaviour or characteristics of groups of individuals from data shared by samples".[718]

Data sharing by an individual thus creates negative externalities[719], as it also reveals information about other individuals whose information is correlated with hers, even if they themselves did not share any data.[720] This is depicted by Ben-Shahar as a phenomenon of "data pollution".[721] Therefore, an individual's ability to protect her privacy is influenced by disclosure choices made by others, as "protecting one's data becomes increasingly costly the more others reveal about themselves".[722] This can be highly problematic in terms of individual autonomy and (informational) self-determination, as these negative externalities might lead towards excessive data sharing situations, where individuals decide to overlook their own privacy preferences by sharing more data than they would have wanted to, because they know that the fact that others have broadly shared their own data will already have revealed much information about them.[723]

102. Another important thing to understand about these "profiles" built from data derived from large numbers of people, through Big Data analytics or artificial intelligence techniques, is that "a profile is not, in reality, about any one person. No-one fits it exactly and no profile pertains to a single identified or identifiable individual".[724] Rather, through the application of clustering processes, "individuals are placed into socially and existentially a-significant "categories", which are imperceptible (because they emerge only as the process unfolds), and most often without any possibility of being aware of what is happening or recognising

---

[717] D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Can we have too much data?", 18 November 2019, available at https://voxeu.org/article/can-we-have-too-much-data; D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Too much data: prices and inefficiencies in data markets", *op. cit.*, p. 1. See also A. Chang, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram", 2 May 2018, available at https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram; K. Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens", *New York Times*, 19 March 2018, available at https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[718] D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Can we have too much data?", *op. cit*.

[719] On these negative externalities, see also J.A. Fairfield and C. Engel, "Privacy as a public good", *Duke Law Journal*, 2015, Volume 65, Issue 3, p. 385-457; M. MacCarthy, "New directions in privacy: Disclosure, unfairness and externalities", *Journal of Law and Policy for the Information Society*, 2011, Volume 6, p. 425–512.

[720] D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Can we have too much data?", *op. cit*.; D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Too much data: prices and inefficiencies in data markets", *op. cit.*, p. 3 and 36-37.

[721] O. Ben-Shahar, "Data pollution", *Journal of Legal Analysis*, 2019, Volume 11, p. 104-159.

[722] A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *op. cit.*, p. 5.

[723] D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Too much data: prices and inefficiencies in data markets", *op. cit.*, p. 1. Accordingly, "in the presence of data-sharing externalities, the value of users' privacy cannot be inferred from their revealed data-sharing decisions" (D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Can we have too much data?", *op. cit*.). To deal with this issue, Acemoğlu *et al*., propose the adoption of a new regulation scheme "where data transactions are mediated in a way that reduces their correlation with the data of other users. The main idea is to achieve "de-correlation", by removing the correlation between an individual's data and information of those who are not actively sharing their own data" (D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Too much data: prices and inefficiencies in data markets", *op. cit.*, p. 34-36).

[724] A. Rouvroy, ""Of Data and Men"", *op. cit.*, p. 22.

themselves".[725] Moreover, due to this imperceptibility and lack of awareness, individuals will often be unable to challenge this profiling.[726]

Yet, using such "profiles", without precautions and specific safeguards, could seriously hamper the individuals' human dignity, autonomy and self-determination[727], as being assigned a specific profile "affects the opportunities that are available to us and consequently the realm of possibilities that defines us: not only what we have already done or are doing, but also what we could have done or could do in the future".[728] For instance, the call centres of certain companies do not assess candidates on the basis of their CV or of their inherent qualities or characteristics, but rather evaluate "whether they match certain data points, which on the face of it are unrelated to the qualities the post or job will require (…) but which are statistically predictive of, amongst others, good performance or the ability to cope with the demands of the vacant position".[729] Similarly, the benefit of an insurance or of a financial credit could be refused to an individual that has been profiled as a potential fraudster due to her network of relationships and/or because she shares some characteristics with people that have frauded in the past.[730] Both of these cases create serious issues in terms of individual autonomy and (informational) self-determination.[731] Indeed, as outlined by Rouvroy:

> "How can we still presuppose, if only as a functional fiction, the autonomy of a subject when the subject is exposed to profiling of all kinds which seizes him or her 'in real time' not as a person, but as an aggregate of propensities, a good part of which is unknown to the person himself or herself, or an aggregate of impulses before any transformation of these impulses into conscious desire".[732]

103. It can therefore be concluded, from this relational and collective nature of data[733], that it will also be fundamental, when considering the adoption of "empowerment" initiatives, to balance the individual's potential gains from data sharing with the potential collective costs for other individuals in terms of control, autonomy and self-determination. This will be further developed below.[734]

104. To conclude, it must also be added that, as for the economic and broader societal rationale for sharing, the benefits from these "empowerment" initiatives will have to be balanced with the corresponding costs for the data holder when considering whether to

---

[725] *Ibid*., p. 28.
[726] *Ibid*., p. 37.
[727] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010, available at https://rm.coe.int/16807096c3, p. 3.
[728] A. Rouvroy, ""Of Data and Men"", *op. cit.*, p. 22.
[729] *Ibid*., p. 9; H. Guillaud, "L'emploi à l'épreuve des algorithmes", *InternetActu*, 3 May 2013, available at http://www.internetactu.net/2013/05/03/lemploi-a-lepreuve-des-algorithmes/.
[730] A. Rouvroy, ""Of Data and Men"", *op. cit.*, p. 15.
[731] *Ibid*., p. 10; A. Rouvroy et T. Berns, "Gouvernementalité algorithmique et perspectives d'émancipation", *op. cit*., p. 175.
[732] A. Rouvroy, "*Homo juridicus* est-il soluble dans les données ?", *op. cit.*, p. 433.
[733] *Ibid*., p. 429.
[734] See Part II, Chapter 2, Section A, c).

impose B2B data sharing obligations.[735] Additionally, any form of data sharing will have to comply with the personal data protection rights of the (other) individuals whose data would be shared.[736]

[735] See points 89, 90, and 96.
[736] See points 91 and 96 and Part II, Chapter 2, Section A, b). See European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, *op. cit*., p. 8.

Chapter 3. Sharing how? A typology of data sharing models and initiatives

105. Now that the concept of data has been specified (**What?**) and that the rationale for (data) sharing has been outlined (**Why?**), this thesis can turn to the way in which data is shared (**How?**). Accordingly, this Chapter will present a **typology of data sharing models and initiatives.** To do so, this chapter will be subdivided in two sections. Section A will take a more practical approach, and will present the most common *conceptual models of data sharing*. Section B, on the other hand, will take a more abstract approach, by focussing on the underlying objectives pursued by *compulsory B2B data sharing initiatives*. In doing so, two main categories will be established, namely *empowerment" initiatives imposing B2B data sharing*, and *economic or societal initiatives imposing B2B data sharing*.

Section A. Conceptual models of data sharing

106. As outlined in Chapter 2[737], the European Commission has abandoned the idea of creating a "property-like" right on data. Rather, it opted for a form of market self-regulation relying on *voluntary data sharing* and contractual freedom. This approach opens the door for creativity in setting up *conceptual models of data sharing* allowing the data holder and the data recipient, as well as intermediaries in some cases, to extract the most value out of the data. Yet, opting for the "right" model requires careful consideration and depends on the specific situation of each undertaking. This lack of a "one-size-fits-all" solution has given rise to a plethora of models. For the sake of concision, all of these models will not be presented[738], and the focus will be set on the most notorious ones.

a) Diversity of conceptual data sharing models

1. Bilateral contracts

107. The most basic conceptual model of data sharing is bilateral contracts. At first sight, this model is very simple: a data holder enters into a contract with a data recipient in order to provide data in exchange of a monetary price, another means of exchange (other data, a service…) or even without any compensation (purely free sharing).

Figure 2: Bilateral contracts

The reality is much more complex, as these contracts can take various forms. Indeed, not all data holders engaging in bilateral contracts operate in the same way, as they can be either considered as data suppliers or data managers, as explained by Thomas and Leiponen.[739] Data

[737] See point 64.
[738] For an original overview of a wider spectrum of models, in the form of an interactive map, see the UK Open Data Institute's "Data Access Map", available at https://theodi.org/project/the-data-access-map/#1565707571855-6d70b0a0-3243.
[739] L. Thomas and A. Leiponen, "Big Data Commercialization", *IEEE Engineering Management Review*, 2016, Volume 44(2), p. 74-90.

suppliers put less effort in providing their data as they typically share unprocessed raw data, for instance a telecommunication operator sharing customer location data with a recipient providing traffic information, such as Waze. Data managers engage in more preparatory work before sharing the data, as they add value to the raw data by cleaning and structuring it, which converts this raw data into a format that is more interpretable and more efficient to use for the recipient's analysis. Moreover, the object of the contract can differ greatly.[740] However, bilateral contracts are not only used to "sell" data. They can also be used to outsource data analytics of previously gathered data to another undertaking, or to enter into partnerships or joint ventures where two undertakings combine forces to improve their data analytics capabilities. Moreover, they can also be used to sell value added services that are based on insights generated through data collection, aggregation, repurposing, cross-referencing and contextualisation. Additionally, the concrete output that is shared also varies. In that regard, de Montjoye *et al.* identify four types of concrete outputs:[741]

- Firstly, the output can simply be a "copy of (part of) the data holder's dataset*"* that is shared with the recipient. This is the most intuitive conception of bilateral data sharing. For instance, TomTom sells copies of its navigation and map data to recipients from the automotive and technology sectors, as well as to geographical information system (GIS) providers.[742]

- Secondly, rather than sharing a copy of the data, the data holder can opt to share "indicators or synthetic data representations*"* derived from the original data. For example, Telefónica shares aggregated and anonymised insights with recipients, rather than its raw data.[743]

- Thirdly, instead of sharing data as such, the data holder can choose to offer "remote access to its system*"*, which means that the holder's data is not released but rather stays under its control and that, accordingly, the data analysis conducted by the data recipient takes place within the holder's premises and the data recipient can only extract aggregated data that is the result of this remote analysis. This provides advantages for both the data holder – who can easily supervise by whom the data is accessed, for what purpose, how it is used and can make sure that no data other than aggregated data resulting from the remote analysis leaves the secure area –, and the recipient, who gets access to near-real time data which is highly valuable. This is the model used by Orange, who provides recipients with a remote access to its cloud, where they can analyse some of Orange's anonymised raw datasets (such as call detail

---

[740] See L. Priego, D. Osimo and J. Wareham, "Data sharing practices in Big Data ecosystems", *ESADE Working Paper 273*, 2019, available at https://ssrn.com/abstract=3355696.

[741] Y.-A. de Montjoye, S. Gambs, V. Blondel, G. Canright, N. de Cordes, S. Deletaille, K. Engø-Monsen, M. Garcia-Herranz, J. Kendall, C. Kerry, G. Krings, E. Letouzé, M. Luengo-Oroz, N. Oliver, L. Rocher, A. Rutherford, Z. Smoreda, J. Steele, E. Wetter, A. Pentland and L. Bengtsson, "Comment: On the privacy-conscientious use of mobile phone data", *Scientific Data*, 2018, Issue 5, available at https://www.nature.com/articles/sdata2018286.

[742] Everis, "Study on data sharing between companies in Europe – Case studies", *Study for the European Commission*, 2018, available at https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en, p. 38.

[743] *Ibid*., p. 31.

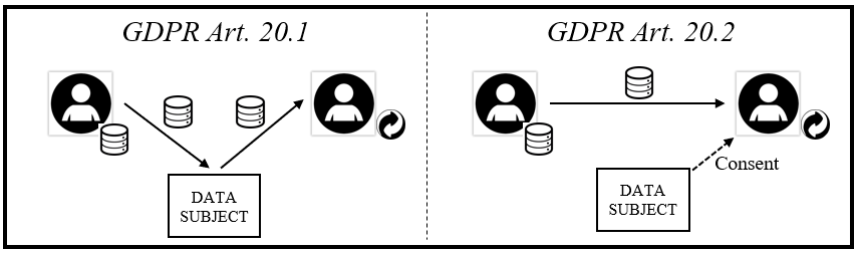
records (CDR)) directly on the cloud, but they can only extract the insights derived from their analysis and not any of the underlying raw data.[744]

- Fourthly, the data holder can opt for a "question-and-answer model", which resembles the remote access model because the data stays within the data holder's system, but differs from it as recipients only access the data through an API and a question-and-answer system (e.g., SafeAnswers or SQL queries). For instance, the data recipient could access the data holder's system and ask "How many people have participated to the demonstration going from point A to point B on the 20th of September 2020?" and would be provided with the answer "24.672" via the API. This is notably done by Telefonica, who answers, in exchange for a fee, recipients' specific questions in the form of insights.[745]

2. Data portability

108. In the last decade, another conceptual model of data sharing has gained a lot of attention, notably due to the adoption of the GDPR[746], namely data portability.[747]

Figure 3: Data portability



Indeed, Article 20.1 GDPR provides that the data subject has the right to receive the personal data concerning her, which she has provided[748] to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the original controller. For instance, the data subject should have the possibility to extract her list of contacts from her webmail application in order to build a wedding invitation list that she can then share with her wedding planner.[749] If limited to the hypothesis targeted by Article 20.1 of the GDPR, data portability would be a quite cumbersome mechanism of data sharing, as it implies that the data would necessarily have to

---

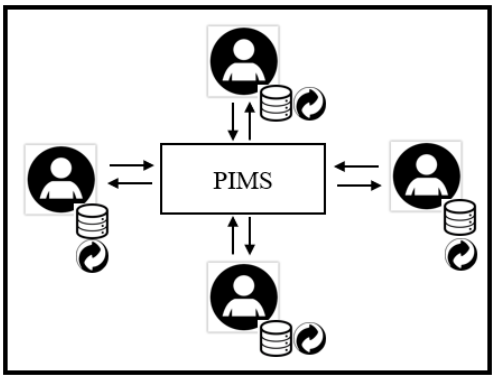
[744] *Ibid*., p. 25.
[745] *Ibid*., p. 31.
[746] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), *OJ L 119*, 4 May 2016.
[747] On the right to data portability, see *infra* Part II, Chapter 1, Section A.
[748] Are considered as "provided" the "data actively and knowingly provided by the data subject" (name, age, email address…) and the "observed data provided by the data subject by virtue of the use of the service or the device [of the data controller]" (search history, traffic and localisation data, number of steps walked during the day…). However, will not be considered as "provided" the "inferred data and derived data (…) created by the data controller on the basis of the data provided by the data subject" (user profiles, results of an evaluation of the data subject's health based on the data collected by her smart watch…): Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 10, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[749] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 5.

transit through the data subject's IT system (cloud storage, personal computer, laptop…) before being shared with a recipient. Fortunately, Article 20.2 of the GDPR provides that the data subject also has the right to have the personal data transmitted directly from one controller to another. In essence, this means that a data recipient can port data directly from the data holder's system provided that the data subject has consented to this operation. This hypothesis is a more effective mechanism of data sharing. However, it only applies "*where technically feasible*". Finally, it should be pointed out that the concept of data portability is not limited to personal data and also has been used for non-personal data.[750]

3. Personal Information Management Systems (PIMS)

109. Data portability can also be used as an instrument to create personal data platforms managed by the data subject or by a trusted third party, from which controllers could access and process such data under the control of the data subject.[751]

Figure 4: Personal Information Management System



Pilot projects for such personal information management systems (PIMS) already exist in Europe, such as "MiData"[752] in the United Kingdom and "MesInfos / SelfData"[753] in France, and at a more global level, with the MyData movement.[754] In practice, the data subjects use trusted third party's services (which may take the form of websites, platforms, applications or personal clouds) on which data controllers who have agreed to participate in the project provide, with the consent of the data subject and in accordance with the right to portability, access to the latter's personal data which they process. This type of initiative shows that portability can be an opportunity and not solely a constraint for data controllers.

In the mainstream PIMS models, the person managing and controlling the access rights of data controllers to the personal data is the data subject herself. Another approach is however

---

[750] See Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019, article 16.4; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018, article 6. For more information, see Part II, Chapter 1, Section B, a) and Section D, a).

[751] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 15.

[752] See https://www.midata.coop/.

[753] See http://mesinfos.fing.org/selfdata/

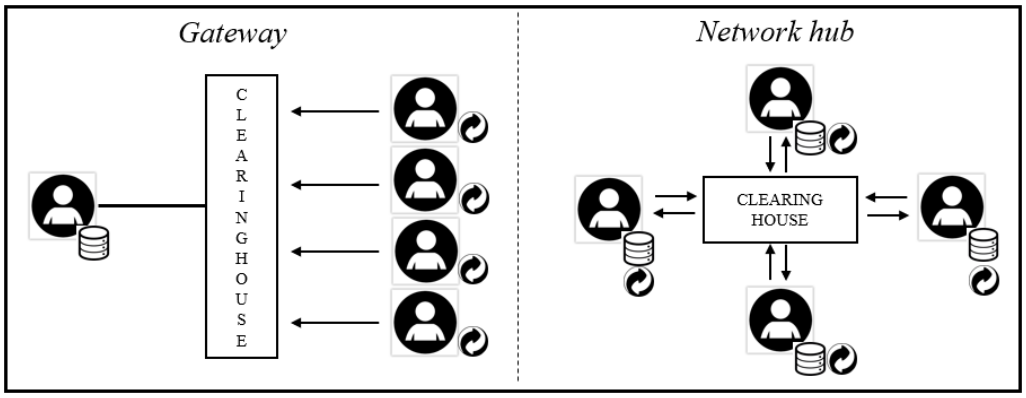
[754] See L. Langford, A. Poikola, W. Janssen, V. Lähteenoja and M. Rikken (eds.), "Understanding MyData Operators", *MyData Global Report*, 29 April 2020, available at https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf.

possible, namely that the PIMS could be managed by an independent intermediary, as explained by Delacroix and Lawrence.[755] This intermediary would exercise the data subject's rights contained in the GDPR on behalf of the data subject and would negotiate data access and use with the data controllers in conformity with the terms of the agreement entered into with the data subject. The long-term objective would be to have a whole ecosystem of such agreements, whether publicly or privately funded, among which the data subjects could choose between different approaches to data governance, and allowing them to switch from one intermediary to another if need be. For this ecosystem to work, the entry barrier for new intermediaries must be low, the security of the data subjects' data must be ensured, and this data must be portable and erasable.

4. Data clearinghouses

110. The PIMS model described above resembles another conceptual data sharing model, namely data clearinghouses. In this model, a clearinghouse acts as a checkpoint between the data holder and the data recipient, verifying that the recipient has the clearance to access the data holder's data. In essence, this data clearinghouse model can be divided in two sub-models. In the first, the clearinghouse acts as the gateway through which all recipients have to go in order to access a single database. In the second, the data clearinghouse is the hub of a peer-to-peer network involving various data holders and recipients.

Figure 5: Data clearinghouses



An example of the gateway model can be found in the field of connected cars and the sharing of vehicle data. Indeed, these connected cars generate a huge amount of data that are not only valuable for the car manufacturers (so-called original equipment manufacturers, OEMs) but also for a wide array of stakeholders who have an interest in accessing these data to provide additional services (independent repairers, component suppliers, on-board entertainment service providers, insurers, public authorities…). In the current situation, which raises controversial data sharing questions[756], the OEMs favour the "extended vehicle" approach to

[755] S. Delacroix and N. Lawrence, "Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance", *International Data Privacy Law*, November 2019, Volume 9, Issue 4, p. 236-252. See also C. Wendehorst, "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 349-353.

[756] See *infra* Part III, Chapter 3, Section A., a) "The current strong reliance on sectoral legislations".

share car data. Under this approach, all vehicle data are transferred on a single central server outside of the car controlled by the OEM. The recipients access the data on those remote servers (one for each OEM), rather than directly in the car. In this model, the OEMs themselves act as clearinghouse for their own data, as they decide whether these recipients can get access to their data.[757]

An example of the network hub model is the Belgian Crossroad Bank for Social Security (CBSS).[758] The CBSS acts as the hub of the network of all Belgian social security institutions (SSIs). The CBSS is the core of the network and SSIs are the nodes.[759] While each (or some) of these institutions remain in control of their authoritative sources of social data, the CBSS acts as the central actor for the data sharing between them.[760] Indeed, given the sensitive nature of the personal data at hand, the SSIs can only access the other institutions' data via the CBSS if they have received an authorisation to do so.[761] The CBSS thus does not itself store any data, but rather acts as a "clearinghouse" that checks that an SSI has the right to access data stored on one of the nodes of the network (another SSI). This distributed model allows for GDPR compliance and for each of the SSIs to remain in control of their authoritative sources of social data, while also avoiding multiple collection of the same data by all the SSIs, in accordance with the "once-only principle".[762]

5. Data marketplace

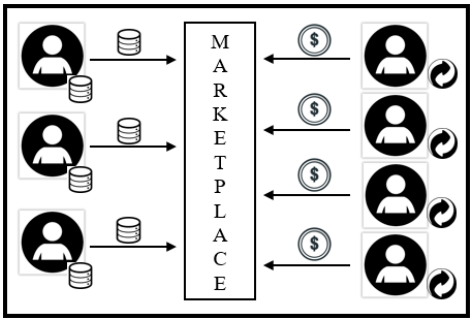
111. A fifth conceptual data sharing model is the data marketplace model, or the "eBay of data". This marketplace, which can be an online store or a platform, is set up to act as an intermediary between data holders and data recipients, where the latter can buy the former's data. A third party builds up an infrastructure enabling the resale and re-use of data by generating trust for both the data holders and data recipients, thanks to identity management and auditing services that ensure the integrity and the quality of the data on a secure platform.[763] These data marketplaces can also offer a range of additional services such as data

---

[757] See W. Kerber and J. Frank, "Data Governance Regimes in the Digital Economy: The Example of Connected Cars", 3 November 2017, available at https://ssrn.com/abstract=3064794.
[758] Loi du 15 janvier 1990 organique de la Banque Carrefour de la sécurité sociale, *M.B.*, 22 février 1990.
[759] See https://www.ksz-bcss.fgov.be
[760] Loi du 15 janvier 1990 organique de la Banque Carrefour de la sécurité sociale, *M.B.*, 22 février 1990, article 3.
[761] *Ibid*., articles 5 and 11.
[762] See Loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier, *M.B.*, 4 juin 2014; Tallinn Declaration on eGovernment, 6 October 2017, available at https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*EU eGovernment Action Plan 2016-2020 - Accelerating the digital transformation of government*", Brussels, 19 April 2016, COM(2016) 179 final.
[763] See L. Thomas and A. Leiponen, "Big Data Commercialization", *op. cit.*, p. 74-90.

storage, enrichment, aggregation, analysis or exchange, and they are usually financed through the collection of a fee for each transaction that occurs on the platform.[764]

Figure 6: Data marketplace



An example of such a data marketplace is Dawex[765], founded in 2015, that operates an independent online platform allowing data sharing.[766] In order to generate trust and before being allowed to sell/buy data, data holders and data recipients need to subscribe to the platform and outline what their business is. Dawex does not only enable data sharing within a sector but also between sectors, and a search tool is embedded in the platform in order to facilitate the identification of potentially interesting datasets. The price of the dataset is set by the data holders, who nevertheless have the possibility to ask the platform to help them to value their dataset if they are clueless about its worth. Dawex also allows the data holders to specify the conditions and restrictions under which their data can be shared, such as (no) sector-specific limitation; (no) possibility to re-sell the data; limited geographical scope; (no) purpose limitation. Moreover, Dawex also offers visualisation and sampling tools to data recipients, which allow them to visualise representative samples of the dataset generated by algorithms before completing the transaction. This incentivises data recipients to engage in data sharing as it solves the Arrow information paradox, according to which the data recipient does not know the value of the dataset until it gets access to it, but if the dataset is disclosed then it has in fact acquired it at no cost.[767] Thus, providing the data recipient with a representative sample allows it to estimate the value of the whole dataset, but also benefits the data holder as it preserves the value of the original dataset.

6. Data pools

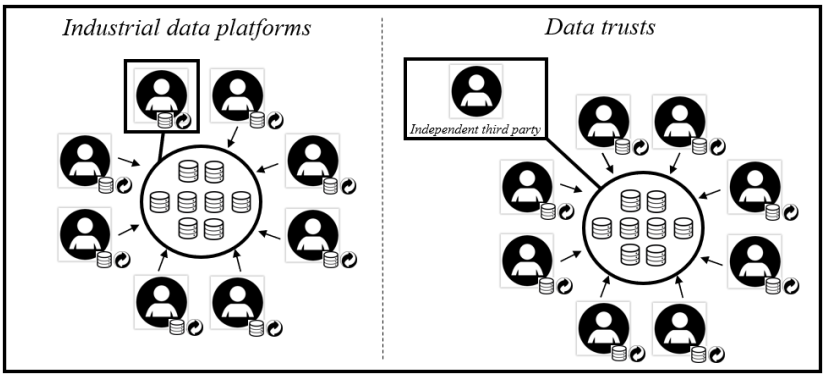
112. While data marketplaces create a trusted intermediation framework and the necessary technical conditions to enable data sharing and re-use, data pools go a step further as they actively seek to match data holders and data recipients according to their interests and needs.[768] In essence, data pools are a conceptual model of data sharing in which several

---

[764] Everis, "Study on data sharing between companies in Europe – Final report", *Study for the European Commission*, 2018, available at https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en, p. 10.
[765] https://www.dawex.com
[766] See Everis, "Study on data sharing between companies in Europe – Case studies", *op. cit.*, p. 49-55.
[767] K. Arrow, "Economic Welfare and the Allocation of Resources for Invention", *The Rate and Direction of Inventive Activity: Economic and Social Factors*, National Bureau of Economic Research (ed.), 1962, p. 609-626.
[768] Everis, "Study on data sharing between companies in Europe – Final report", *op. cit.*, p. 93.

stakeholders pool their data together, in order to extract more insights and value from the pooled data. This leads to a win-win situation for each of the members of the pool, as they use this data to improve their products or services or to develop new ones. The generic term "data pool" is used to encompass two data pooling models, namely industrial data platforms and data trusts.

Figure 7: Data pools



An industrial data platform can be defined as a "virtual environment enabling the exchange of data among different companies through a shared reference architecture, common governance rules and within a secure business ecosystem".[769] While these industrial data platforms could, in principle, be open to all, they are often composed of a restricted group of stakeholders who voluntarily join the platform to share some of their data in exchange for the access to some of the other partners' data, in a secure and exclusive environment. They will also usually be sector-specific, though they could also cover different business sectors. Contrary to data marketplaces, the goal is generally not to share data for money, but to share data in exchange for the access to a data pool that is used by each member to enhance its products/services. Such platforms are often managed by a stakeholder that also participates in the pool. One example is the Skywise platform created by Airbus.[770] Launched in 2017, Skywise is a web-based platform on which Airbus and the airlines that purchased Airbus aircrafts share aviation data for free among themselves.[771] This allows Airbus to improve its aircrafts and the participating airlines to become more performant and efficient thanks to the access to the pooled aggregated data. Another example is the cloud-based RIO platform, created by MAN, that pools data from a plurality of stakeholders involved in the transport, freight and logistics sector.[772]

Mostly known in the UK, data trusts, on the other hand, are defined by the Open Data Institute as "a legal structure that provides independent stewardship of data".[773] Stewardship is about having control on the access to the data, on the purposes and conditions under which

[769] *Ibid*., p. iv.
[770] https://www.airbus.com/aircraft/support-services/skywise.html
[771] Everis, "Study on data sharing between companies in Europe – Final report", *op. cit.*, p. 66. See also Everis, "Study on data sharing between companies in Europe – Case studies", *op. cit.*, p. 56-64.
[772] https://rio.cloud/fr/. See Everis, "Study on data sharing between companies in Europe – Case studies", *op. cit.*, p. 64-71.
[773] Open Data Institute, "Data trusts: lessons from three pilots", 2019, available at https://theodi.org/article/odi-data-trusts-report/, p. 6.

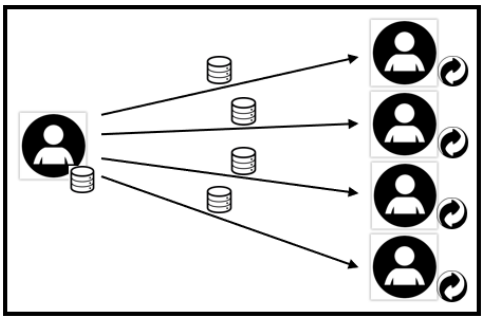
data sharing can occur, and on the determination of the beneficiaries of such sharing. In the data trust model, several stakeholders entrust an independent organisation (the trustee) to decide on how the pooled data should be used and shared. This is the main difference with industrial data platforms, as in the later model, the pool is generally managed by a stakeholder that also participates in the pool. Trustees, on the other hand, do not themselves contribute any data to the pool, but only manage the participants' data, to the benefit of the latter. Naturally, the trustees' margin of manoeuvre is limited as they are bound by the pre-defined rules of the trust and the previously-agreed purpose of the data trust.[774]

Examples of such data trusts are the three pilot projects by the UK Open Data Institute: the first pilot with the Greater London Authority and the Royal Borough of Greenwich aims at creating an urban space data trust dealing with data about parking spaces for electric vehicles and sensor data collected in residential housing; the second pilot with the WILDLABS Tech Hub is designed to fight illegal international wildlife trade by relying on data acquired by officials at borders and on acoustic and image data; and the third pilot with manufacturers and retailers from the food and drink sector aims at tackling global food waste, by focusing not only on food waste data but also on sales data.[775]

7. Open Data platforms

113. The last conceptual model is the Open Data platform, where the data holder chooses to share its data with anybody who wishes to access it. This is generally done for free, but it can also entail a small fee covering the reproduction, provision and dissemination costs.

Figure 8: Open Data



Open Data is mostly used in the G2B context[776], where public sector data are compiled on Open Data platforms, gathering data from various public sector bodies, such as the national data platforms "data.gov.be", "data.gouv.fr", "data.overheid.nl" or "data.gov.uk". Yet, some

[774] Conceptually, such a model evokes the Common Law "Trust" mechanisms, but it should be pointed out that data trusts cannot take the form of "Trusts" in the Common Law sense, and instead will have to be built using legal structures inspired from these Common Law "Trusts" (Open Data Institute, "Data trusts", *op. cit.*, p. 6). See also C. Reed, BPE Solicitors and Pinsent Masons, "Data trusts: legal and governance considerations", 2019, available at https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf.

[775] Open Data Institute, "Data trusts", *op. cit.*, p. 11 *et seq*.

[776] Directive 2003/98 of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ L 345/90*, 31 December 2003; Directive 2013/37 of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, *OJ L 175/1*, 26 June 2013; Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019.

private undertakings have also started experimenting with this model in a B2B context. For instance, Elering, an electricity and gas system operator from Estonia, has launched the "Estfeed" data platform, which allows providers of energy applications and consumers to access energy data from various data holders.[777] Another example is the French company Enedis, which has set up a platform providing the access to energy distribution and consumption data to recipients active in the (renewable) energy market, or in the smart building/homes sector.[778] Interestingly, both these undertakings started sharing data because of legal obligations and voluntarily went one step further as they realised that Open Data could be a valuable business model.

b) A typology of conceptual data sharing models

114. After having reviewed the most notorious conceptual data sharing models, two main parameters underlying these models emerge, namely whether the sharing is bilateral or multilateral and whether the sharing is intermediated by a platform or not.

1. Bilateral/multilateral sharing

115. As data sharing comes into multiple forms and shapes, the number of recipients depends on the conceptual model that is chosen. This parameter is especially important in terms of control, by the data holder, of the shared data. Indeed, if the sharing benefits a single recipient, the control exercised by the data holder on the shared data is much greater than in cases where the data is shared with a large (sometimes even unknown) number of recipients. The greater the number of recipients, the lesser the amount of control on what the data is used for. In this regard, four situations can be identified: single bilateral sharing, multiple bilateral sharing, multilateral sharing with finite users and multilateral sharing with indefinite users.

116. In the case of single bilateral sharing, the sharing takes place in a one-to-one situation. There is a single recipient per act of sharing. This is the situation where the control on the data remains the greatest for the data holder. Bilateral contracts belong to this category, but so does data portability. On the one hand, Article 20.2 of the GDPR, which provides that the data subject has the right to have the personal data transmitted directly from one controller to another, benefits a single recipient, who must nevertheless have obtained the prior consent from the data subject. On the other hand, Article 20.1 of the GDPR, which provides that the data subject has the right to receive the data in a structured, commonly used and machine-readable format and have the right to transmit it to another controller without hindrance from the controller, implies two successive and independent acts of bilateral sharing. The first occurs between the data controller and the data subject, and the second between the data subject and the data recipient.

117. In the case of multiple bilateral sharing, sharing occurs within a network involving multiple actors, but it remains bilateral in nature because each act of sharing within the network requires a form of consent by one of the parties in order to get access to the data. The

[777] Everis, "Study on data sharing between companies in Europe – Case studies", *op. cit.*, p. 98-103.
[778] *Ibid*., p. 104-109.

data holder keeps a strong control on the data as there is still, in this category, a single recipient per act of sharing.

The first model falling within this category is the PIMS. Indeed, though these PIMS create a network involving multiple recipients who get access to (some) of the data subject's data, each individual act of sharing only benefits one recipient. This is because the access, by recipients, to the data subject's data, held by a data holder belonging to the network, is subject to this data subject's consent. Therefore, each act of consent (for instance to port the data from firm A to firm B) represents an isolated act of sharing, within a wider network, and only benefits a single recipient.

The second model falling within this category is the data clearinghouse. This is true for both the gateway and the network hub sub-models identified above. In the gateway model, the clearinghouse acts as the checkpoint through which all recipients have to go in order to access a single database. Thus, even though the clearinghouse model involves multiple actors (for instance, all the stakeholders having an interest in accessing vehicle data), each individual act of sharing is bilateral and only benefits a single recipient, as the clearinghouse has to authorise each and every one of them. Similarly, in the network hub model, the data clearinghouse is the hub of a network involving various data holders and recipients and is at the core of each interaction between two peers of the network. Once again, though multiple actors participate in the network, each individual act of sharing is bilateral and only benefits a single recipient, as the clearinghouse has to authorise each of them. For instance, though all the Belgian social security institutions participate in the CBSS ecosystem, each access request made by one institution to another institution's data requires a prior approval and only benefits a single recipient.

The third model falling within this category is the data marketplace. Here, the third party managing the marketplace provides data holders/data recipients with a platform offering multiple potential buyers/sellers. Yet, each act of data sharing is bilateral, as it is subject to the data holder's approval and only benefits a single recipient.

118. In the case of multilateral sharing with finite users, the data is shared with multiple well-identified recipients. The data holder retains less control on the data as it is shared with a larger number of recipients, but still retains some control as these recipients are, in principle, known in advance. This is typically the case for data pools. Indeed, in both the industrial data platform and the data trust models, the data holders contribute data to the pool, which will benefit multiple recipients, namely all the other participants to the data pool. For instance, when Airbus feeds a dataset to its "Skywise" platform, all the airlines that participate to this data pool get access to this dataset. The sharing thus benefits a pre-determined and finite number of recipients, i.e. all the members of the pool.

119. In the case of multilateral sharing with indefinite users, the data is shared with an indefinite number of recipients. The "unknown" factor is what distinguishes this category from the "multilateral sharing with finite users" category, as in the latter case, the number of recipients is pre-determined and finite. The only model falling within this category is the Open Data platform model. Indeed, making the data available in Open Data implies that it can

be accessed by anyone. By uploading its data on the platform, the data holder signals that any recipient can access it. The sharing thus benefits an indefinite number of recipients.

2. Intermediated/non-intermediated sharing

120. The second main parameter is whether these conceptual data sharing models are intermediated or not. A model is intermediated when the sharing occurs thanks to a platform that has been set to enable the large scale and systematic exchange of the data between multiple actors, by providing them with the necessary technical infrastructure for this exchange and by lowering transaction costs.[779]

In fact, only the bilateral contracts and data portability models are non-intermediated. All the other models imply some form of intermediation. Indeed, the Open Data model is usually intermediated by a passive third party (the government having set up the Open Data platform accessible to all) on which the data holder uploads its data, allowing an unlimited number of data recipients to access it. The PIMS model is intermediated by an active third party, as it implies the creation of a personal data platform, from which the access to the data subject's data is managed by the data subject herself or by a trusted third party. Similarly, in the data clearinghouse model, the clearinghouse can be considered as a platform through which every access request has to pass. Data marketplaces obviously also qualify as such platforms, whose goal is to match data holders and data suppliers and to technically enable the data sharing. Finally, data pools are also intermediated by an active third party that controls the access to the pooled data, whether this platform is managed by one of the participants of the pool (industrial data platforms) or by an independent third party (data trusts).

121. This intermediation parameter is also important because, when dealing with intermediation platforms, it is crucial to distinguish whether the undertaking that set up this intermediation platform also uses the data in order to improve its own business, or whether it solely acts as an intermediate third party that does not make use of the data shared on its platform, but rather acts as a mere sharing facilitator. Indeed, if the sharing platform has been set up by an undertaking who also uses the data, there is a risk that the platform owner might integrate third party data and, if this leads to a lock-in situation, this might entail a risk for competition.[780] This probably explains why, in its proposal for a Data Governance Act, the European Commission included a provision precluding trusted data intermediaries from using the data, obtained through the operation of an intermediation service, for other purposes than to put them at the disposal of data recipients.[781]

When looking at the outlined data sharing models, it appears that platform owners generally solely act as intermediate third parties not making use of the data in the PIMS, data clearinghouse, data marketplace, data trust and Open Data platform models. On the contrary,

---

[779] H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *IIC*, 2019, Volume 50, Issue 1, p. 9-10. See also B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 25-27.

[780] H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *op. cit.*, p. 15.

[781] See Article 11.1 of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final.

in the industrial data platform model, platform owners do not solely set up the intermediation platform but also use the data themselves.

122. It is also useful to discuss whether the data sharing model is open or closed. For intermediated data sharing models relying on platforms, the question is whether the platform is open to new participants.[782] A platform is closed if access to it is restricted to a limited number of participants and no other participant can join it in any case whatsoever. A platform is open if the access is open to any party wishing to join it. Having an open platform can imply that some conditions have to be met in order to get access to it. Rather, the open nature comes from the fact that any party is free to meet those conditions. For clarity purposes, it is distinguished below between platforms that are open provided that some conditions are met, and platforms that are completely open.

Data clearinghouse-network hub models are generally closed as they are limited to a strict category of participants. For instance, only the Belgian social security institutions can participate in the Belgian's CBSS. The data pools (industrial data platforms and data trusts) in which only a strict category of participants is allowed will also generally be considered as closed. This is the case of the "Skywise" platform, which can only be accessed by Airbus and the airlines having purchased Airbus aircrafts.

The PIMS model is open provided that some conditions are met, as any recipient may get access to the platform, provided that it has obtained the data subject's consent and that it respects the other provisions of the GDPR. Moreover, while the data pools (industrial data platforms and data trusts) will generally be closed, some of them might be open if any third party can join the pool. This openness will however often be subject to the fulfilment of some conditions.

By nature, data marketplaces are completely open as their success relies on having as many data holders and data recipients on the platform as possible, in order to generate network effects. Similarly, data clearinghouse-gateway models are open as any third party is free to file a request to the clearinghouse in order to get access to the data holder's data. Finally, by essence, Open Data platforms are necessarily completely open, as the aim is to make the data uploaded on the platform available to as many recipients as possible.

As far as the non-intermediated models are concerned, bilateral contracts are completely open because, in principle, any two parties are free to conclude such a contract. Similarly to PIMS, data portability is open provided that some conditions are met, as any data subject and/or data recipient is entitled to rely on Article 20 of the GDPR, provided that this provisions' conditions are met and that the other provisions of the GDPR are respected.

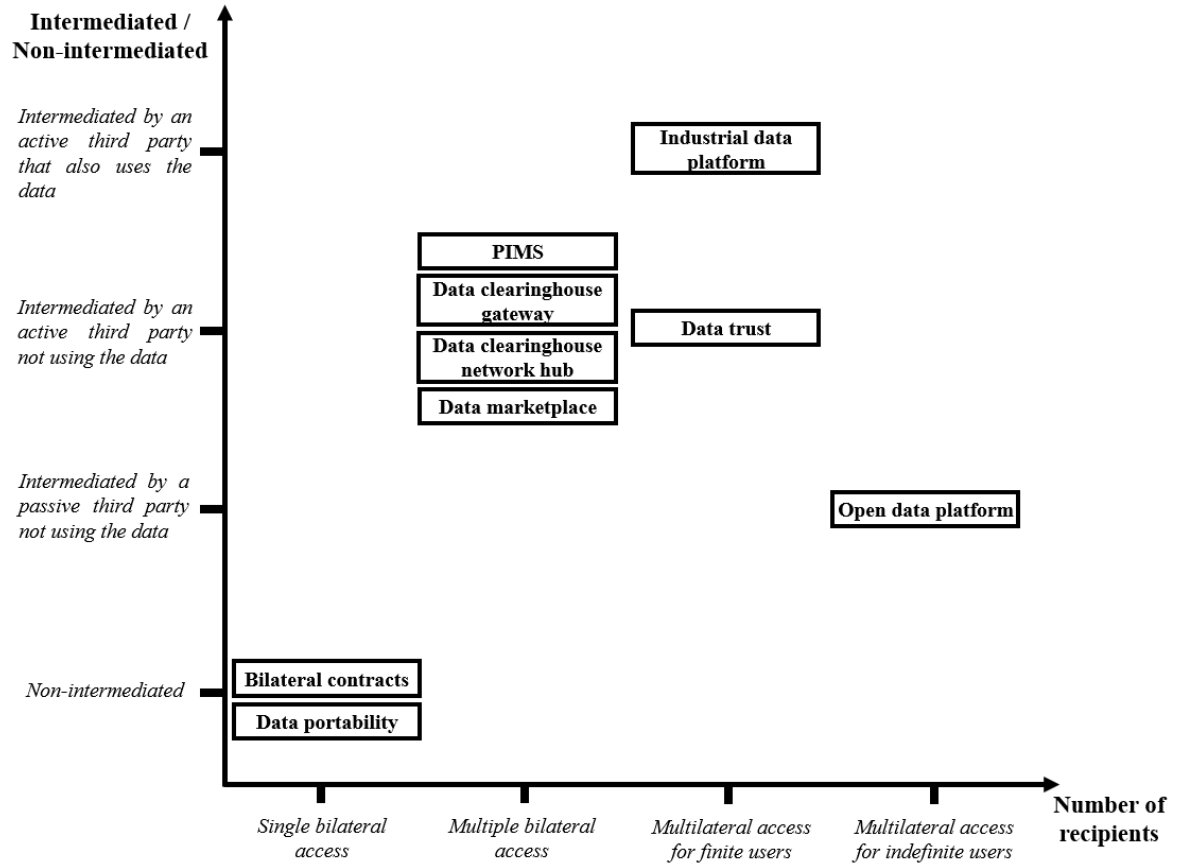
3. Summary

123. In sum, the conceptual data sharing models reviewed above can be classified in four groups, on the basis of these two main parameters. The first group is made of the bilateral

[782] H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *op. cit.*, p. 11-12.

contracts and the data portability models, which are single bilateral and non-intermediated. The second group is made of the PIMS, data clearinghouses and data marketplace models, which are multiple bilateral and actively intermediated. The third group is made of data pools, which are multilateral for finite users and actively intermediated. The fourth group is made of Open Data platforms, which are multilateral for indefinite users and passively intermediated.

Figure 9: Typology of main data sharing models



c) The typology in the European legal framework

124. After having suggested a typology of conceptual data sharing models, it is interesting to briefly depict how the European legal framework approaches these models. In fact, it is striking to observe that the European legislator favours certain models when it comes to adopting binding legislations. On the one hand, for B2B data sharing, the European legislator favours (forms of) data portability models. Indeed, four recent legal instruments rely on (forms of) this conceptual data sharing model.[783] On the other hand, for G2B data sharing, the European legislator favours Open Data models.[784]

125. Referring to the first typology parameter ("Number of recipients"), the European legal framework seems to favour the two "extreme" categories ("Single bilateral sharing" and "Multilateral sharing with indefinite users"), while neglecting to consider the middle categories ("Multiple bilateral sharing" and "Multilateral sharing with finite users"). Yet,

[783] See Part II, Chapter 1, Sections A and B.
[784] See Part III, Chapter 3, Section B, a), 1.

numerous valuable conceptual data sharing models are located in these middle categories (PIMS, data clearinghouses, data marketplaces, data pools) and these could be relevant options as well. Nevertheless, these other types of conceptual data sharing models are mentioned in soft law instruments, such as the European Commission's "Guidance on sharing private sector data in the European data economy", which underlines that data sharing models may be bilateral or be concluded between multiple parties and which mentions the data marketplace and the data pools models.[785] Moreover, it is apparent from the Commission's *Strategy for data* that it is starting to focus on PIMS and data pools. Indeed, it indicated that it would support the development and roll-out of "Personal data spaces" in order to empower data subjects by strengthening the control they exercise on their data[786], and that one of its priorities would be to create an enabling legislative framework for the governance of common European data spaces (data pools), in order to facilitate cross-border data use and to foster standardisation activities and data interoperability.[787] These European data spaces should lead to the availability of large pools of data in strategic economic sectors and domains of public interest[788], which could be organised in a centralised or distributed way. In fact, the Commission's reflections expressed in its *Strategy for data*, have been integrated in a proposal for a Data Governance Act that notably aims at promoting *voluntary* data sharing services by intermediaries through PIMS, data marketplaces and data pools.[789]

Referring to the second typology parameter (Intermediated/non-intermediated), the European legal framework focusses on non-intermediated data sharing models (data portability) and on models intermediated by a passive third party (open data), and somewhat overlooks models intermediated by an active third party. However, as outlined above, the European Commission included in its proposal for a Data Governance Act a provision precluding trusted data intermediaries from using the data, obtained through the operation of an intermediation service, for other purposes than to put them at the disposal of data recipients.[790] Moreover, the Commission has announced in its *Strategy for data* that it would update its Horizontal Cooperation Guidelines[791] in order to provide more guidance on the compatibility of data pooling agreements with EU competition law.[792] Indeed, *voluntary data sharing*, notably through data pooling, could entail competition problems, as it might lead to "collusion

---

[785] Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication "*Towards a common European data space*", Brussels, 25 April 2018, SWD(2018) 125 final, p. 5-6.
[786] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", 19 February 2020, COM(2020) 66, p. 20.
[787] *Ibid*., p. 12.
[788] *Ibid*., p. 21. These strategic economic sectors and domains of public interest are listed in the Appendix the "European strategy for data" (see p. 26-34).
[789] See the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final.
[790] See Article 11.1 of the Proposal for a Data Governance Act.
[791] Communication from the Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 14 January 2011, 2011/C 11/01.
[792] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 14.

through the exchange of commercially sensitive information among competitors", which is prohibited by Article 101 of the Treaty on the functioning of the European Union[793] (hereafter "TFEU").[794] This will be further detailed below.[795]

[793] Treaty on the functioning of the European Union, *OJ C 326/47*, 26 October 2012.
[794] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 24. See also B. Lundqvist, "Competition and Data Pools", *Journal of European Consumer and Market Law*, 2018, p. 146-154; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit.*, p. 94-98; I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper DP 2019-005*, November 2019, available at https://ssrn.com/abstract=2956308, p. 7-8; H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *op. cit.*, p. 22-23.
[795] See Part III, Chapter 1, Section D, d).

Section B. Two distinct categories of compulsory B2B data sharing initiatives

126. Moving away from the conceptual models of data sharing presented in Section A, which focussed on how *voluntary data sharing* usually occurs in practice, this Section will take a more abstract approach, by focussing on the underlying objectives pursued by *compulsory B2B data sharing initiatives*.

As outlined in Chapter 2, while the debates at the European level usually focus on economic objectives[796], societal objectives could also be pursued through the imposition of compulsory B2B data sharing.[797] Furthermore, compulsory data sharing is also increasingly presented as a way to "empower" individuals.[798] Considering these distinct, but possibly also complementary, objectives leads to the identification of two main categories of *compulsory B2B data sharing initiatives,* namely *"empowerment" initiatives imposing B2B data sharing*, on the one hand, and *economic or societal initiatives imposing B2B data sharing*, on the other hand.

a) "Empowerment" initiatives imposing B2B data sharing

127. *"Empowerment" initiatives imposing B2B data sharing* aim to give more control to individuals on "their" data.[799] As will be outlined in Part II, these empowerment initiatives can pursue two different types of sub-objectives, namely allowing the exercise of fundamental rights, such as the right to personal data protection and informational self-determination, on the one hand[800], or addressing specific market failures, on the other hand.[801] A common point between these two types of empowerment initiatives, which explains why their analysis is combined in Part II, is that they are based on the idea that the best way to achieve the objective pursued is to give more control to the individuals on "their" data, and that the solution thus resides in the sharing of individual level data. Accordingly, they are mostly built as (forms of) portability rights, of which the right to personal data portability, enshrined in Article 20 of the GDPR, is the prime example.[802] Reverting to the above-suggested typology of conceptual data sharing models and to the European legal framework's approach of these models[803], it thus becomes apparent that, by focussing on data portability models, and more

---

[796] See Part I, Chapter 2, Section B. See also Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 3, 5, 8 and 14; Communication from the Commission, "*Shaping Europe's digital future*", *op. cit*., p. 8.
[797] See Part I, Chapter 2, Section C, a). See also Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 942.
[798] See Part I, Chapter 2, Section C, b). See also Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 10. See also p. 20-21.
[799] See Part I, Chapter 2, Section C, b).
[800] See Part II, Chapter 1, Section A.
[801] See Part II, Chapter 1, Section B.
[802] See Part II, Chapter 1, Section A.
[803] See Part I, Chapter 3, Section A. "Conceptual models of data sharing".

recently on PIMS models of data sharing[804], the European legislator has in fact put the accent on these *"empowerment" initiatives imposing B2B data sharing*.[805]

As hinted above, a core difference with the second category of initiatives that will be presented below, other than the types of objectives pursued, is that the amount of data transferred in this first category is relatively small, as it is limited to the data relating to the specific individual at hand. Naturally, the framework, as a whole, that is created by these initiatives can potentially lead to the sharing of data pertaining to a very large number of individuals, but each act of sharing will relate to a specific individual. For instance, a broad use of Article 20 of the GDPR could lead to a situation where one million users request a porting of their data from firm A to firm B. Yet, this would require one million specific and separate acts of sharing, rather than a single act of sharing covering the data of the one million users as a whole. In sum, for *"empowerment" initiatives imposing B2B data sharing*, a framework, potentially applicable to numerous individuals, is created to facilitate the transfer of individual level data. Accordingly, these "empowerment" initiatives mostly benefit a specific individual, but also have indirect benefits for third parties (such as (potential) competitors of the data holder), which is not surprising as some of these initiatives precisely aim at remedying specific market failures through the mean of individual empowerment.[806]

b) Economic or societal initiatives imposing B2B data sharing

128. The second category of B2B data sharing initiatives analysed in this thesis are those pursuing economic or societal objectives.[807] An important common point between these two sub-types of initiatives, which explains why they are analysed together in Part III, is that the focus of these initiatives is not set on the individuals, but rather on broader economic or societal considerations that go beyond individual interests. Accordingly, what will be shared are larger amounts of (aggregated) personal data pertaining to multiple individuals and/or non-personal data, rather than smaller quantities of data linked to a specific individual.

For instance, economic initiatives imposing B2B data sharing, which aim to remedy market failures deriving from a lack of data sharing[808], would allow a single act of sharing from firm A to firm B, covering the data of the one million users as a whole (likely in an aggregated form), rather than one million separate acts of sharing, each pertaining to a specific individual. The objective would notably be to provide competitors with a sufficient amount of data that allows them to compete, in order to avoid the "cold start problem".[809] These initiatives thus

---

[804] See point 174.
[805] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 20. See also Recital 23 and Article 9.1.b) of the Proposal for a Data Governance Act. See also p. 7 of its "Explanatory memorandum".
[806] See Part II, Chapter 1, Section B.
[807] See Part III.
[808] On these market failures see Part I, Chapter 2, Section B, c), 3. "Data market failures".
[809] To be able to offer a quality service, a firm needs a certain amount of data. To collect this data, it needs to attract customers, but the customers will not use its service if the quality is insufficient. Hence the cold start problem, because if the firm does not have enough data to start with, it will be unable to reach a minimal level of quality and will be unable to attract customers. This is also sometimes referred to as the "chicken and egg problem". See, *inter alia*, V. Fast, D. Schnurr and M. Wohlfarth, "Data-Driven Market Power: An Overview of Economic Benefits and Competitive Advantages from Big Data Use", July 2019, available at https://ssrn.com/abstract=3427087, p. 10; J. Krämer, P. Senellart and A. de Streel, "Making data portability more

mostly benefit third parties, but they also have indirect benefits for the individuals' whose data are shared (usually in an aggregated way). In practice, this is mainly tackled through competition law[810], with the exception of a sector-specific data sharing legislation in the automotive sector[811].[812]

The compulsory sharing of larger amounts of (aggregated) personal data pertaining to multiple individuals and/or non-personal data could also be justified by broader societal objectives, as highlighted above.[813] An example of such legislation is the Finnish Act on the Secondary Use of Health and Social Data.[814]

129. For this second category of initiatives, it has been opted not to make a distinction between the initiatives pertaining to personal and non-personal data because, as outlined above, the boundary between these two concepts is porous and often difficult to establish in practice[815], and because what matters are, in fact, the objectives pursued by these categories of compulsory B2B data sharing initiatives. Accordingly, this thesis suggests, for this second category of compulsory B2B data sharing initiatives, to adopt an alternative data typology[816], following a common holistic approach for both personal and non-personal data[817], which will nevertheless take the personal data considerations into account when relevant.[818]

* * *

130. In conclusion, because these two categories of compulsory B2B data sharing initiatives pursue different objectives, they will be addressed separately. This key distinction will therefore structure the remainder of the thesis. Accordingly, **Part II** of the thesis will be dedicated to ***"Empowerment" initiatives imposing B2B data sharing***, while **Part III** will be dedicated to ***Economic or societal initiatives imposing B2B data sharing***.

For both of these Parts, the key underlying economic and/or societal balancing exercises will be studied, and, where relevant, it will be questioned whether these balances need to be

---

effective for the digital economy*"*, *CERRE Report*, 2020, available at https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy, p. 64.

[810] See Part III, Chapter 1.

[811] Regulation (EU) 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, *OJ L 171/1*, 29 June 2007, articles 6 and 7; Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L 151/1*, 14 June 2018. See articles 61 to 66, 86 and annexes X and XI.

[812] See Part III, Chapter 3, Section A, a).

[813] See Part I, Chapter 2, Section C, a) and Part III, Chapter 4. See Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 942.

[814] See point 93. For more information on this Act, see https://stm.fi/en/secondary-use-of-health-and-social-data.

[815] See Part I, Chapter 1, Section B.

[816] See Part I, Chapter 1, Section C.

[817] For a call to follow such a holistic approach see I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, September 2018, available at http://ssrn.com/abstract=3256189, p. 14-18.

[818] See Part III, Chapter 2. "Articulation between data protection and competition law".

adapted for data markets, in light of data's characteristics. Some insights will also be formulated on how these balancing exercises can be addressed.

Finally, it must be clarified from the outset that while these two main categories of compulsory B2B data sharing initiatives pursue different objectives, synergies can be found between them, which explains why they are both addressed in this thesis. Indeed, *empowerment initiatives* will only provide more choice for individuals, and/or more control on their data, if a sufficient number of alternatives to their current situation are available. Accordingly, even if the main objective of these initiatives is to empower individuals, this entails the pursuit of a secondary objective, which could be qualified as economic, namely ensuring the presence of a sufficient number of viable competitors on the markets at hand. Reversely, although *economic initiatives* mainly aim at addressing market failures and at fostering more competition, this will have as a secondary consequence to empower individuals, as they will be offered more alternatives to choose from. The same goes for *societal initiatives*, which mainly aim to pursue general purpose goals (healthier environment, smoother mobility, increased access to healthcare, etc), but which, in doing so, indirectly benefit individuals as well.

Part II. "Empowerment" initiatives imposing B2B data sharing

131. Part II of this thesis will be dedicated to *"empowerment" initiatives imposing B2B data sharing*. As mentioned above, these empowerment initiatives can pursue two different types of sub-objectives.

On the one hand, empowerment initiatives can pursue the objective of allowing the exercise of fundamental rights, such as the right to personal data protection and informational self-determination.[819] The core instrument, adopted at the European level, to pursue this goal is naturally the GDPR[820], which has replaced the previous Directive 95/46[821], and which aims to frame the use of personal data in the European internal market. In order to do so, this instrument aims at reaching an equilibrium between the fundamental right of the protection of personal data and the fundamental right of the freedom to conduct a business.[822] Indeed, technological developments and globalisation have transformed the economy and the GDPR aims at facilitating the free flow of personal data within the European Union in order to support the development of the digital economy across the internal market, while ensuring a high level of personal data protection and creating the necessary trust.[823] To do so, the GDPR grants to the data subjects[824] a certain number of rights[825], among which the right to personal data portability, which improves the power of control that the data subjects have on "their" personal data, and which will be further analysed below.[826]

This "power of control" that data subjects can (re)claim on their data is fundamental as it will facilitate the exercise of their fundamental rights, as increased access to information will improve their decision making and will allow them to take fundamental decisions about all aspects of their life.[827] For instance, they can better understand how they are profiled and the influence this has on the media content or news feed that are presented to them, which may notably influence their electoral choices.

---

[819] See Part II, Chapter 1, Section A.
[820] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4 May 2016.
[821] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281*, 23 November 1995.
[822] Respectively Articles 8 and 16 of the Charter of Fundamental Rights of the European Union, *OJ C 326*, 26 October 2012. See Recital 4 of the GDPR.
[823] Recitals 6 and 7 of the GDPR.
[824] "*Any identified or identifiable natural person*" (Article 4.1 of the GDPR).
[825] Articles 13 to 22 of the GDPR. See point 98.
[826] See Part II, Chapter 1, Section A.
[827] See point 97. ECtHR, *Youth Initiative for Human Rights v. Serbia*, 25 June 2013, App. No. 48135/06, §§ 20 and 24; D. Voorhoof, "Freedom of expression and the right to information: Implications for copyright", *Research Handbook on Human Rights and Intellectual Property*, C. Geiger (ed.), Cheltenham, Edward Elgar, 2015, p. 337. See also C. de Terwangne, "Droit à la vie privée: un droit sur l'information et un droit à l'information", *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 555-579.

Importantly, while the GDPR gives control to the data subjects on "their" data, it does not, by any means, confer any "property" rights over personal data.[828] Indeed, although such data are often used as a "counterpart" in exchange for the use of a "free" service (such as social networks, video platforms or search engines), the fact remains that the right to personal data protection is a fundamental right that cannot be transferred.[829] However, this debate between the legal principles and the reality of the situation in practice remains lively.[830]

132. On the other hand, empowerment initiatives can be adopted to address specific market failures.[831] The underlying idea of these initiatives is that by giving more control to individuals on "their" data, this will allow them to multi-home or to switch more easily between service providers as their searching and switching costs are reduced, and this should reduce the market failures deriving from consumer inertia and lock-in effects.[832] Indeed, the aim is to give more autonomy to the individuals by allowing them to optimise the use of their resources, as illustrated by the UK's Open Banking and Smart Data initiatives, which will be further detailed below.[833] In turn, this should facilitate entry and should foster competition on the targeted markets, which should lead to better services, more choice and lower prices for the individuals.

133. Coming back to the focus of this thesis, **Chapter 1** will be dedicated to the main *"empowerment" initiatives imposing B2B data sharing*, which are, to a large extent, built around (some forms of) data portability rights, whether they aim to allow the exercise of fundamental rights or to address specific market failures.[834] This Chapter will also discuss more recent trends, such as the request to introduce a "continuous portability" right[835], and the adoption of legislations aiming at empowering specific (small) business users.[836] **Chapter 2**

---

[828] For a broader discussion on the "property of data", see *supra* Part I, Chapter 2, Section B, b).

[829] See point 62. European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017, available at https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf, p. 7; European Data Protection Supervisor, *Opinion 8/2018 on the legislative package "A New Deal for Consumers",* 5 October 2018, available at https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf, p. 16-17. See also, S. Gutwirth and G. Gonzalez Fuster, "L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre", *Law, norms and freedom in cyberspace – Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier and R. Queck (eds.), Bruxelles, Larcier, 2018, p. 117-140.

[830] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A New Deal for Consumers"*, Brussels, 11 Avril 2018, COM(2018) 183 final, p. 5.

[831] See Part II, Chapter 1, Section B.

[832] See point 97.

[833] See points 163 to 165 and 171 to 173. Competition and Markets Authority, "The Retail Banking Market Investigation Order 2017", 2017, available at https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-bankingmarketinvestigationorder-2017.pdf; Competition and Markets Authority, "Final Approved Roadmap for Open Banking", 14 May 2020, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885537/Notice_of_proposed_changes_to_the_open_banking_roadmap_-_web_publication_-_cma_gov_uk_---_May_2020_-.pdf; HM Government, "Smart Data: Putting consumers in control of their data and enabling innovation", June 2019, available at https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation.

[834] See Part II, Chapter 1, Sections A and B.

[835] See Part II, Chapter 1, Section C.

[836] See Part II, Chapter 1, Section D.

will then focus on the fundamental balancing exercises entailed by such *"empowerment" initiatives*.

Chapter 1. Main "empowerment" initiatives imposing B2B data sharing and recent trends

134. The most notorious empowerment initiative imposing B2B data sharing is arguably the personal data portability right enshrined in Article 20 of the GDPR.[837] As will be outlined below, this initiative pursues the objective of allowing the exercise of the fundamental rights to personal data protection and to informational self-determination (**Section A**).

However, as outlined above, not all empowerment initiatives pursue such an objective, and in fact, several initiatives have rather been adopted in order to address specific market failures. These are the data retrieval right enshrined in Article 16.4 of the Digital Content Directive[838], and the data access and use rights granted in the revised Directive on payment services in the internal market ("PSD2")[839] and in the Electricity Directive.[840] (**Section B**).

Importantly, it must be underlined that the effectiveness of these data sharing initiatives, and their ability to truly empower individuals, which is their primary aim, is being criticised.[841] Accordingly, the growing call for the creation of a "continuous portability" right, will also be presented (**Section C**).[842]

Then, **Section D** will make a brief digression about the more recent phenomenon of regulatory initiatives aiming at empowering specific (small) business users. These represent the beginning of a move from individual empowerment towards small businesses empowerment, which fits in a broader context of extending consumer protection (B2C) towards small businesses protection (B2b).

---

[837] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), *OJ L 119*, 4 May 2016.
[838] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019.
[839] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015.
[840] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, *OJ L 158/125*, 14 June 2019.
[841] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *CERRE Report*, 2020, available at https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy.
[842] *Ibidem*. See Part II, Chapter 1, Section C.

Section A. "Empowerment" initiatives imposing B2B data sharing in order to allow the exercise of fundamental rights: Personal data portability in the GDPR

135. The main instrument adopted by the European legislator in order to empower individuals through data sharing is, without a shadow of a doubt, the personal data portability right enshrined in Article 20 of the GDPR. This sub-section will present this right by focussing on its definition and objectives, on its scope and on some considerations pertaining to its exercise.

a) Definition and objectives

136. Article 20 of the GDPR provides that:

> "1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
>
> (a) the processing is based on consent pursuant to point (a) of Article 6.1 or point (a) of Article 9.2 or on a contract pursuant to point (b) of Article 6.1; and
> (b) the processing is carried out by automated means.
>
> 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
>
> 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
>
> 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others".

While this provision has marked the apparition of the concept of "portability" in the field of personal data protection law, it is worth mentioning that this concept had already existed for several years in electronic communications law.[843] Indeed, phone number portability had been introduced at the end of the 1990s to facilitate the entry of new operators in the electronic communications market, by allowing subscribers to keep their landline (or mobile) telephone

[843] See Directive 98/61/EC of the European Parliament and of the Council of 24 September 1998 amending Directive 97/33/EC with regard to operator number portability and carrier pre-selection, *OJ L 268/37*, 3 October 1998, article 1; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), *OJ L 108/51*, 24 April 2002, article 30; Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *OJ L 321/36*, 7 December 2018, article 106.

number, if they so requested, when changing providers.[844] The aim was thus to empower the consumers, by encouraging them to switch for cheaper providers without having to worry about the hassle of changing phone number and communicating this new phone number to their family, friends, colleagues, etc.

137. In the same vein, the right to personal data portability aims at strengthening "data subject empowerment", i.e. the power of control that the data subjects have on "their" personal data[845], as this right will enable them to move, copy or transmit personal data easily from one IT environment to another.[846] Indeed, it should "further improve access of individuals to their personal data".[847] In reality, this "data subject empowerment" objective is translated into two sub-objectives.

On the one hand, in a strict conception of the notion of "data subject empowerment", this right to data portability "represents an opportunity to "re-balance" the relationship between data subject and data controllers", and this, "by affirming individuals' personal rights and control over the personal data concerning them".[848] This objective is transversal in the GDPR and goes beyond the right to data portability.[849]

On the other hand, and in a broader conception of the notion of "data subject empowerment", this right to data portability should make it easier for the data subject to change service providers.[850] This demonstrates the influence that phone number portability has had on personal data portability. In the first version of its guidelines on the right to data portability, the Article 29 Working Party (today the European Data Protection Board – EDPB) even indicated that this was the "primary aim" of this new right, as it should facilitate the creation of new services, which is perfectly in line with the strategy of the European legislator to create a digital single market.[851] This echoed the statement made by the Council regarding its position at first reading, where it outlined that the right to portability "also encourages competition amongst controllers".[852] However, in what seems to be a move to position this right as a fundamental rights empowerment tool, rather than as a tool aiming to address

---

[844] See M. Ledger et T. Tombal, "Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ?", *R.D.T.I.*, 2018/3, n°72, p. 26-27.

[845] Recital 68 of the GDPR. See also Recital 68 of the Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/1*, 3 May 2016.

[846] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.

[847] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM/2012/011 final, p. 9.

[848] *Ibidem*.

[849] See T. Tombal, "Les droits de la personne concernée dans le RGPD", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 555-556; L. Somaini, "The right to data portability and user control: ambitions and limitations", *MediaLaws – Rivista dir. media*, 2018/3, p. 172.

[850] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.

[851] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242, 13 December 2016, p. 4.

[852] Statement of the Council's reasons: Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/83*, 3 May 2016, p. 89.

market failures / competition issues[853], the indication that this constituted the "primary aim" of the right was deleted in the revised version of the Article 29 Working Party's guidelines of April 2017, which now state that the main objective of this right is to promote "data subject empowerment" and that the GDPR aims to regulate the processing of personal data, and not to deal with competition law issues.[854]

Nevertheless, the creation of this new right to portability shows the significant impact that the emergence of social networks has had on the reflections leading to the adoption of the GDPR.[855] It reflects the clear desire to prevent the data subjects from being "locked-in" by Internet giants such as Facebook or Google, by allowing them to port their personal data to a new alternative online service. Indeed, in the absence of such a right, one could imagine that the data subjects might refrain from using such alternative services, as, for instance, re-uploading all the personal data that they have already uploaded on Facebook (personal information, photos, etc.) would be time-consuming.

138. Accordingly, in order to achieve this "data subject empowerment", the right to data portability allows the data subject to receive (part of) the personal data concerning her that she has provided to a controller.[856] In this sense, the right to data portability is rather a complement to the right to data access provided in Article 15 of the GDPR, allowing the data subjects to manage and re-use personal data themselves, as these data must be provided to them in a structured, commonly used and machine-readable format.[857] The Article 29 Working Party cites, as an example, the hypothesis in which the data subject wishes to extract her contact list from a Webmail application, in order to build a wedding list.[858]

Although this example is instructive, it must be noted that, in practice, this specific situation, in which the data subject would herself wish to manage and re-use her data, without using a service offered by a third party, will rarely occur. Indeed, a large proportion of the data subjects will not have the necessary technical skills to use these data themselves. For example, if a data subject exercises her data portability right towards Google, in order to receive information that she has provided to this firm, this extensive amount of information will be provided to her in HTML, JSON or OPML format. Although such formats are structured, commonly used and machine-readable, the data is likely to be incomprehensible, as it stands, for the data subject. Indeed, it should not be forgotten that "machine-readable" data will not necessarily be "understandable" for an ordinary person, as this might require appropriate technical skills. In light of the above, the right to data portability will thus most likely not be used by data subjects simply in order to receive personal data concerning them, but rather in order to transfer this data from one controller (hereafter the "data holder") to

---

[853] See Part II, Chapter 1, Section B for examples of empowerment initiatives aiming to address such market failures / competition issues.
[854] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.
[855] D. de Bot, "De uitvoering van de algemene verordening gegevensbescherming – enkele bemerkingen bij de Belgische context", *T.V.W.*, 2016/3, p. 221.
[856] Article 20.1 of the GDPR.
[857] It should be noted that these format requirements are not identical than for the right to data access, which merely requires the use of a "commonly used electronic form" (Article 15.3 of the GDPR).
[858] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 5.

another (hereafter the "recipient"). The right to data portability provides that this should be possible, without hindrance from the data holder.[859] According to the Article 29 Working Party, such hindrance could derive from "fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardisation or accreditation demands".[860]

In this perspective, the right to data portability goes a step further, in that it allows the data subject not only to manage and re-use personal data concerning her, but also to share them with a data recipient, active in the same economic sector, or not, as the original data holder.[861] The underlying idea is to strengthen "data subject empowerment" by avoiding "lock-in" situations and by fostering "opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the control of the data subject".[862] The challenge arising from Article 20.1 of the GDPR is that its use in practice is dependent on whether the data subjects will dedicate time to such data sharing initiatives, and whether they have the technical understanding and storage capacity to port the data on their own system before transferring it themselves to the data recipient.

139. It might be tempting to say that Article 20.2 of the GDPR circumvents this challenge by providing that the data subject shall have the right to have the personal data transmitted directly, without hindrance, from the data holder to a data recipient (for example, transferring a playlist from iTunes to Spotify). Interestingly, this possibility of direct transfer had not been envisaged on the Commission's original proposal.[863] Indeed, this was introduced by the Parliament's position at first reading, where, in fact, the Parliament had deleted the specific provision pertaining to data portability, but had instead requalified it as a "right to obtain data" and had grouped it with the data subject's right of access.[864] The specific provision pertaining to the right to data portability was however reinstated by the Council's position at first reading, and contained the wording of the final versions of Articles 20.1 and 20.2.[865]

However, it must be outlined that such direct transfer can only be required by the data subject "*where technically feasible*", which means that the original data holder has no obligation to ensure this technical feasibility. While the Article 29 Working Party does not clarify in its guidelines what should be considered as being "technically feasible", one could interpret this

---

[859] Article 20.1 of the GDPR.
[860] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 15.
[861] *Ibid*., p. 5.
[862] *Ibid*., p. 5.
[863] Article 18 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM/2012/011 final.
[864] Article 15.2a of the European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 12 March 2014, *OJ C 378/399*, 9 November 2017.
[865] Article 20 of the Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/1*, 3 May 2016.

wording as an implicit reference to the notion of interoperability[866], which is mentioned in Recital 68, but not in Article 20 of the GDPR, so that the data could only be transmitted directly between two interoperable systems.

In this regard, it should be pointed out that Google, Facebook, Microsoft and Twitter contribute, with other actors, to the *Data Transfer Project*, launched in 2017, which aims at creating an open source platform allowing the direct portability of data between the participating data controllers.[867] Such a platform would, according to the members of the project, foster interoperability and reduce the infrastructure burden for portability. This project relies on three main components, namely "Data Models", "Adapters" and "Task Management Libraries". More concretely, "Data Models are the canonical formats that establish a common understanding of how to transfer data. Adapters provide a method for converting each Provider's proprietary data and authentication formats into a form that is usable by the system. Task Management Library provides the plumbing to power the system".[868] Importantly however, it must be underlined that while anyone can contribute to the development of this open source platform, the ability to make use of it requires an authorisation from the Hosting Entities (Google, Facebook, Microsoft or Twitter, depending on the Host Platform, as it is a decentralised model), as they are the ones responsible for granting the API keys that are necessary to access the system.[869] Therefore, this project might not be as open as it seems, as service providers might have to agree to the terms imposed by these powerful Hosting Entities in order to access the platform. Moreover, it cannot be excluded that these Hosting Entities might refuse to give access to the platform to (potential) competitors.[870] Furthermore, it must be outlined that in order to join the platform, the service providers have to agree to a reciprocity obligation, as in order to be able to import data, they also have to allow the export of their own data.[871] Such a reciprocity obligation is not included in the GDPR, and this might deter service providers from joining the platform as they might not want to provide even more data to the large Hosting Entities.

Another project worth mentioning is the *Solid Project*[872], initiated by Sir Tim Berners-Lee, founder of the internet, which aims at allowing "linked data" between different data

---

[866] Interoperability is defined as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems" (Decision 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector, *OJ L 318/1*, 4 December 2015, article 2.1).

[867] See https://datatransferproject.dev/

[868] See https://datatransferproject.dev/documentation. For more information, see Data Transfer Project, "White Paper: Data Transfer Project Overview and Fundamentals", 20 July 2018, available at https://datatransferproject.dev/dtp-overview.pdf.

[869] See Data Transfer Project, "White Paper: Data Transfer Project Overview and Fundamentals", *op. cit.*, p. 12-13.

[870] On these competition law issues, see Part III, Chapter 1.

[871] See Data Transfer Project, "White Paper: Data Transfer Project Overview and Fundamentals", *op. cit.*, p. 17.

[872] See https://solidproject.org/

controllers.[873] In short, *Solid* is a "fully decentralised space for personal information, with data distributed over multiple personal online data stores (pods) located on different hosts, with a mechanism allowing a user to grant third party applications fine-grained access to specific data items on specific pods".[874] More concretely, a Solid Server hosts one or more Solid Pods, which are fully compartmentalised from one another and have their own data and access rules.[875] Through the use of open, standard formats and of a linked data model, interoperability is insured and data can be shared between Pods.

However, these are stand-alone small-scale initiatives, which are still in development, and, in practice, this direct transmission between the data holders and the data recipients is rarely technically feasible as the former are often not willing to tackle the costly issues of technical interoperability, standardisation and security that would need to be solved in order to make this transfer technically feasible.

b) Scope of the right to data portability

140. As apparent from the definition of the right to data portability enshrined in Article 20 of the GDPR, its scope is limited to specific categories of personal data processing and to certain specific categories of personal data.

1. Specific categories of personal data processing

141. Data subjects can only call upon their data portability right for processing carried out by automated means, and which are based either on the data subjects' consent or are necessary for the performance of a contract.[876] There is thus no general right to data portability, since this right does not apply to processing operations necessary for the performance of a task in the public interest vested in the controller, nor to processing operations necessary for the compliance with a legal obligation to which the controller is subject.[877] For instance, a public administration will have no obligation to port personal data that it has collected for its public service mission[878] and a financial institution will have no obligation to respond to a portability request relating to personal data that has been collected in the context of the compliance with its legal obligation to fight money laundering.[879] Similarly, data subjects will not be able to port data that is processed by the data controller on the basis of "legitimate interests".[880] Yet, this can be highly problematic as this legal basis is a "fall-back" option that, in fact, is widely used by data controllers.

However, even for these categories of processing not covered by the data portability right, the Article 29 Working Party calls on controllers to implement best practices to respond quickly

---

[873] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 14.
[874] *Ibid*., p. 46.
[875] See https://solidproject.org/about
[876] Article 20.1 of the GDPR.
[877] Article 20.3 and Recital 68 of the GDPR.
[878] This limitation of the scope of the portability right was included in order to avoid burdening public bodies. See Opinion of the Committee of the Regions on "Data protection package", 18 December 2012, *OJ C 391/127*, p. 129.
[879] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 8.
[880] Article 6.1.f) of the GDPR.

to potential requests for portability, even if they have no obligation to comply with them, citing as an example the creation of a public e-service offered by the tax administrations and allowing the data subjects to easily download all their tax forms.[881]

2. Specific categories of personal data

142. Additionally, data subjects only have the right to receive the personal data concerning them, which they have "provided" to a controller.[882] The GDPR does not provide further clarification in its Article 20 or in its recitals on the categories of personal data in question, and in particular on what is meant by personal data "provided" by the data subject. However, the Article 29 Working Party's guidelines shed light on the matter.

i. Personal data concerning the data subject

143. Only personal data are subject to this right to portability, excluding, *de facto*, non-personal data as well as personal data that have been anonymised.[883] On the contrary, personal data that have simply been pseudonymised[884] remain personal data and will be subject to this right to portability.

Yet, the expression "personal data concerning them" should not be interpreted too strictly.[885] Namely, this expression should not be understood as limiting the scope of the data portability right to personal data "exclusively pertaining to the data subject", as, in a broad number of cases, personal data will not only pertain to a single individual, but rather to several data subjects. For example, the Article 29 Working Party refers to the case of telephone records or other interpersonal messaging systems that may include information about third parties with whom the data subject has been in contact. According to the Article 29 Working Party, while it is true that these records may thus contain personal data relating to third parties, this should not be invoked by the data holder in order to refuse to comply with the request for the portability of these records made by the data subject. This echoes one of the key limits of "empowerment" initiatives imposing B2B data sharing, namely that they must consider and comply with the other data subjects' right to personal data protection[886]. This will be further detailed below.[887]

---

[881] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 8.
[882] Article 20.1 of the GDPR.
[883] The ISO 29100 standard defines anonymisation as the : "process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" (ISO 29100:2011, point 2.2, available at https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en).
[884] "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Article 4.5 of the GDPR).
[885] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 9.
[886] *Ibid*., p. 11-12.
[887] See Part II, Chapter 2, Section A, b) "Considering the other data subjects' right to personal data protection".

ii. Personal data "provided" by the data subject

144. The scope of the data portability right is also limited to personal data "provided" by the data subject.[888] In this regard, the Article 29 Working Party identifies three categories of personal data and considers that only the first two should be considered as data "provided" by the data subject.[889] These categories have already been outlined above (actively provided, observed and inferred/derived data) and have been integrated in the proposed data typology used in the context of this thesis.[890]

The first category of personal data covered by the right to data portability is "data actively and knowingly provided by the data subject".[891] This includes, for instance, information provided by the data subject in a registration form (email address, user name, age…) or posts on social media. On the contrary, data that has been provided by a third party (for example the comments or likes made by a friend on a social media picture) should arguably not be covered, as they are not "provided by the data subject", but by someone else.

The second category of personal data covered by the right to data portability is "observed data provided by the data subject by virtue of the use of the service or the device".[892] Examples of observed data include the data subject's search or web history, or location data generated by the use of a product or service offered by the data controller. This second category of personal data should, according to the Article 29 Working Party, also be considered as being "provided" by the data subject.[893] However, this is criticised by some members of the European Commission, who consider that this goes beyond what has been envisaged by the European legislator.[894] On the contrary, some argue that there is a strong rational to include observed data in the scope of the data portability right, as they are "a valuable input for data-intensive business models in the digital economy".[895] Indeed, as the markets for several key services (search, social networks) are highly concentrated, only a few firms can observe the individuals' activity across the web, and, as a consequence, "observed data is not ubiquitously available, and it is also usually neither feasible nor socially desirable to duplicate the collection of the same observed data".[896]

---

[888] Article 20.1 of the GDPR.
[889] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 9-11.
[890] See Part I, Chapter 1, Sections B and C.
[891] See point 17. Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10.
[892] See point 17. *Ibidem*.
[893] *Ibidem*.
[894] D. Meyer, "European Commission experts uneasy over WP29 data portability interpretation*"*, 25 April 2017, available at https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/.
[895] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 55. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability: Towards a Governance Framework*"*, *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/, p. 16.
[896] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 53.

It should also be pointed out that, while this thesis made a further distinction between first party and third party observed data[897], such a distinction is not made by the Article 29 Working Party. Yet, this distinction is important as the right to data portability might not apply to both types of observed data. In fact, the Article 29 Working Party only seems to consider "first party observed data", namely data collected *directly* by the controller from its users (e.g. the number of steps walked in a day by the owner of a FitBit bracelet).[898] For these types of data, as they are *directly* collected from the data subject by the controller, it does indeed make sense to consider them as "provided" by the data subject. However, third party observed data, on the other hand, are data *indirectly* collected from the users by the data collector, via technologies such as "cookies" installed on the product or service of a third party (e.g. the data collected by Facebook on third party websites that embed the opportunity to "like" a content on that website).[899] For these types of data, there is an uncertainty as to whether they should also be considered as being "provided" by the data subject. Indeed, Article 20.1 of the GDPR seems to solely envisage the possibility for the data subject to exercise her portability right against controllers to which she *directly* provided data.[900] Because third-party observed data are *indirectly* collected by the controller, they might thus fall outside of the scope of the portability right, unless an extensive interpretation of the text is made.[901] This would merit to be clarified, notably because the arguments mentioned in the previous paragraph would also support the inclusion of these third party observed data in the scope of the data portability right.

The third category of personal data, namely "inferred data and derived data" will, on the other hand, not be covered by the data portability right.[902] These are essentially a second generation of data, such as user profiles or health recommendations, which are created, by the data controller, thanks to the analysis of the data "provided" (actively or observed) by the data subject.[903] It makes sense to exclude this type of data, since they have not strictly speaking been "provided" by the data subject, but rather "created" by the controller. Moreover, these types of data will often be the most valuable for data controllers, as this is where the real added-value of their service must be found. This echoes another key balancing exercise underlying "empowerment" initiatives imposing B2B data sharing, namely the balance between the benefits of sharing for the specific individual and the need to preserve the business interests of the data holder.[904] This balance will also be further detailed below.[905]

---

[897] See Part I, Chapter 1, Section C.
[898] OECD, *Consumer Data Rights and Competition - Background note*, June 2020, DAF/COMP(2020)1, available at http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm, p. 16.
[899] *Ibidem*. See also V. Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Common Market Law Review*, 2020, Vol. 57, p. 162.
[900] This could be supported by the fact that Article 20.1 of the GDPR provides that the data should be transmitted "without hindrance from *the controller to which the personal data have been provided*" (emphasis added).
[901] For instance, due to the fact that Article 20.1 mentions data "provided to *a* controller".
[902] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10.
[903] See point 17.
[904] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11-12.
[905] See Part II, Chapter 2, Section A, a) "Finding a balance between the benefits for the specific individual and the business interests of the data holder".

While not being mentioned in the Article 29 Working Party's guidelines, a fourth category of personal data, outlined in this thesis' proposed data typology, shall be discussed, namely "acquired data".[906] These are personal data obtained from third parties on the basis of a voluntary or compulsory data sharing mechanism. These "acquired data" could either be data actively provided by a data subject to a third party, observed data collected from data subjects by this third party or inferred/derived data created by this third party.[907] For this fourth category of data, which is overlooked by the legal literature dealing with the data portability right, there is an uncertainty on whether they fall within the scope of this right. Or rather, while it seems non-controversial that "acquired inferred/derived data" shall not be covered, as it has never been "provided" by the data subject, it is much less certain whether "acquired actively provided data" and "acquired observed data" should fall within the scope of the data portability right. This is because these data have been "provided" by the data subject to a first controller before being acquired by another party. Yet, the GDPR is mute on whether the data subject should only be able to exercise her right against the original controller to whom she provided the data, or whether it can also be used against subsequent "acquirers" of these "provided" data. Indeed, Article 20.1 mentions data "provided to *a* controller" (emphasis added). It is very likely that the European legislator did not consider this hypothesis and solely envisaged the possibility for the data subject to exercise her portability right against the original controller to whom she "directly" provided the data. This interpretation could be supported by the fact that Article 20.1 of the GDPR provides that the data should be transmitted "without hindrance from *the controller* to which the personal data have been provided" (emphasis added). However, some doubt remains on whether "acquired actively provided data" and "acquired observed data" could fall within the scope of the data portability right. This would also merit to be clarified.

145. Even if this uncertainty around "acquired data" is set aside, the above-mentioned distinction between the first three categories of personal data (actively provided, observed and inferred/derived data) raises two difficulties in practice. On the one hand, it will not be easy for the controller to technically isolate, in its IT system, the third category of data from the other two, in anticipation of the exercise by a data subject of her portability right. On the other hand, and this further accentuates this technical difficulty, it may not always be clear whether certain data have been "provided" (actively or observed) by the data subject, or whether, on the contrary, these data have been "inferred" by the controller. To illustrate this, an overly simplified example can be used: on a timespan of one month, a person does several searches on Google in order to buy blue sports shoes, blue shirts and blue pants, because that person's favourite colour is blue. Based on this search history, Google starts to present her with a majority of advertisements related to blue clothing. To which category of data does the information that this person is only interested in blue clothes correspond? It is obviously not actively provided data (1st category), as the data subject has never explicitly indicated that she was only looking for blue clothes. It is, however, less clear whether this information falls into the category of "observed data" provided by the data subject through the use of the

[906] See point 17.
[907] See point 22.

controller's service (2nd category), or whether, this information has been "inferred" by the controller (3rd category). All of the above shows that even if the scope of the data portability right seems, to a large extent, rather clear from a theoretical point of view, its application in practice will not always be straightforward.

c) Exercise of the right to data portability

146. This thesis will now turn to some considerations pertaining to the exercise of this right (cost and deadline to respond to a portability request, data format and "temporality" of the right). Another important consideration pertaining to the exercise of this right is contained in Article 20.4 of the GDPR, which provides that this right to data portability needs to be articulated with the rights and freedoms of others, *in casu* the data holder and other data subjects, that it shall not affect. Such a provision was absent in the Commission's original proposal[908] and was first included in the Council's position at first reading.[909] As these considerations are at the heart of the balances underlying "empowerment" initiatives imposing B2B data sharing, they will be addressed in a separate Section below.[910]

1. Cost and deadline to respond to a portability request

147. Like for any other data subject's right contained in the GDPR, the data controller must act on a data portability request without undue delay and in any event within one month of the receipt of the request, except in more complex cases, where the maximum response time is three months.[911] It is important to stress that, in any case, the controller cannot remain silent and will have to react within one month of the receipt, either to grant the request, to indicate that it refuses the request, or to inform the data subject that her request is complex and that, accordingly, it will need to extend the response deadline by two months. In the latter case, it must provide the reasons for this delay.[912]

148. Regarding the costs of the right, the controller may not request any payment from the data subject exercising her right to data portability, unless the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive character.[913] For information society services specialised in the automated processing of personal data, this exception should rarely be met, even if the controller is confronted with multiple requests for portability.[914] Indeed, the notion of "repetitive character" used in Article 12 of the GDPR refers to repeated requests from the same data subject, and not to the total number of requests for portability that the controller could receive from several data subjects. Accordingly, "the

---

[908] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM/2012/011 final.
[909] Article 20.4 of the Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/1*, 3 May 2016.
[910] See Part II, Chapter 2, Section A.
[911] Article 12.3 of the GDPR.
[912] *Ibidem*.
[913] Article 12.5 of the GDPR.
[914] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 15.

overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests".[915]

Moreover, the "repetitive character" of the request should not be interpreted too strictly, otherwise this right will be deprived of its effectiveness. Thus, the mere fact of renewing the request to port the same data a second time, for example to forward them to a different recipient, should not be sufficient to conclude that the request is "repetitive". In doing so, it will be necessary to make a case-by-case assessment of the repetitive or non-repetitive nature of the request, and therefore of the possibility for the controller to claim payment. Similarly, if the data subject exercises her right to portability again, towards the same controller, in order to port the data that has been updated since the first request (new data, modified data, etc.), this request should not be considered as repetitive as, by assumption, the data concerned will be different from the data ported the first time.

2. Data format

149. As the objective of the right to data portability is to allow the data subject or a recipient to re-use the ported data, it is essential that the data format allows such re-use. This is why Article 20 of the GDPR states that these data have to be provided in a structured, commonly used and machine-readable format. Interestingly, this latter requirement of a "machine-readable" format was absent from the Commission's original proposal[916] and was first included in the Council's position at first reading.[917] According to the Article 29 Working Party, "the terms structured, commonly used and machine-readable are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome".[918] In fact, Recital 68 of the GDPR adds that this format should also be interoperable, although this requirement does not appear in the text of Article 20. This notion of "interoperability" must not be confused with the notion of "compatibility", as Recital 68 of the GDPR indicates that the data portability right should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. This might seem somewhat contradictory at first sight. Yet, the interoperability is suggested at the "data format" level, while no compatibility is required at the "processing systems" level. Said otherwise, each data holder is free to work with the processing systems it prefers (no requirement of compatibility), but they are encouraged to produce, store and share their data in an interoperable format, which can be re-used by data recipients, independently of the processing systems they use. Indeed, requiring

---

[915] *Ibidem*.
[916] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM/2012/011 final, p. 9.
[917] Article 20.1 of the Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/1*, 3 May 2016.
[918] *Ibid*., p. 17.

technical compatibility of processing systems could have limited too strongly the emergence of technological developments.

Beyond these requirements, the GDPR does not impose specific recommendations as to the format to be used. This is left to the discretion of the controllers, who must nevertheless bear in mind that it is desirable that the chosen format should allow interoperability. In doing so, the use of proprietary formats should be avoided, and priority should be given to commonly used open/free formats (such as XML, JSON or CSV).[919]

Additionally, the data controllers should also provide metadata[920] that is as accurate and exhaustive as possible, in order to best describe the meaning of the ported data.[921] This is fully in line with the European legislator's desire to facilitate the re-use of the ported data, as well as with the invitation made to controllers to propose, if possible, several types of formats to the data subject, while clearly explaining to her the consequences of choosing one or the other of these formats.[922]

Finally, the Article 29 Working Party "strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability ".[923] To do so, these stakeholders could find inspiration in the European Interoperability Framework[924], which establishes a set of common elements in terms of vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.[925] Arguably, this coordination in order to implement these interoperability standards will have a greater chance of success if it is organised at sectoral level, as this makes it possible to have a reasonable number of partners around the table. Standards having a more horizontal application, and based on these sectoral standards, could then be discussed in a second phase.

3. "Temporality" of the right

150. In recent years, growing discussions have emerged regarding the "temporality" of the data portability right, i.e. whether Article 20 of the GDPR could be used as a basis to establish a continuous flow of personal data, pertaining to a specific individual, between a data holder and a data recipient, or whether this Article only enables "one-shots".[926]

In this regard, it is important to specify that the exercise of the right to data portability does not automatically imply an obligation for the controller to erase the ported data.[927]

---

[919] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 17-18.
[920] "Metadata is "data information that provides information about other data". Many distinct types of metadata exist, including descriptive metadata, structural metadata, administrative metadata, reference metadata and statistical metadata" (https://en.wikipedia.org/wiki/Metadata).
[921] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 18.
[922] *Ibidem*.
[923] *Ibidem*.
[924] See https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.
[925] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 18.
[926] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*
[927] Article 20.3 of the GDPR.

Nevertheless, if the data subject decides to exercise her right to erasure in parallel to her right to data portability[928], the controller will have to erase it.[929] Reversely, if the data subject exercises her right to erasure without ever having exercised her right to data portability beforehand, she should no longer be able to exercise her right to portability in a post-erasure situation. Indeed, the right to data portability does not impose any obligation on the controller to store the data after their erasure solely for the purpose of the potential future exercise of that right by a data subject.[930]

Accordingly, when Article 20.1 of the GDPR indicates that the data subject has the right to receive the data, this should be understood as meaning that the data subject has a right to receive a "copy" of this data, which is implicitly confirmed by the Article 29 Working Party's guidelines.[931] This is because, after the exercise of this portability right, the data subject may, in fact, wish to continue to use and benefit from the services of the data holder to whom she submitted the portability request.[932] The right to data portability can thus not only be called upon to stop using a service in order to join another, but also to start using another service by "recycling" personal data already provided to a first service, while continuing to use that first service. In light of the growing possibilities for data subjects to "multi-home", i.e. to use several similar platforms/services at the same time, it is very likely that the right to data portability will mainly be relied upon in cases where the data subject wishes to continue to use the original controller's services. It can therefore not be excluded that the same data subject might exercise her right to data portability several times towards the same original controller. This right to portability should therefore not be solely seen as a "one-shot" mechanism.

151. Although the formulation of Article 20 of the GDPR leaves no doubt about the fact that the right to personal data portability is not merely a "one-shot", it is more obscure whether this article could be used as a basis to establish a continuous portability of personal data, which would imply that data can be constantly transferred between the original holder and the recipient.[933] Indeed, the wording of Article 20.1 merely evokes "the right to receive the data in a structured, commonly used and machine-readable format", but is mute about the "temporality" of such porting. Yet, one could argue that nothing prevents a data subject from relying on Article 20.2 of the GDPR to request a continuous flow of the data, pertaining to her, between the data holder and a data recipient "where technically feasible". In that perspective, the data holder would then have one month (three if the case is complex) to reply to this request and to set in place the continuous flow of data.[934] That being said, it seems unlikely that the drafters of the GDPR had this continuous porting possibility in mind. This is because this right has been designed to enable switching between service providers rather than

---

[928] E.g. a data subject decides to unsubscribe from Facebook and requests to transfer all her personal data to a new social network and, at the same time, to delete all the personal data concerning her held by Facebook.
[929] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 7.
[930] *Ibid*., p. 6.
[931] *Ibid*., p. 4.
[932] *Ibid*., p. 7.
[933] See Part II, Chapter 1, Section C. J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 81.
[934] Article 12.3 of the GDPR.

to enable data re-use in a wider digital ecosystem.[935] Yet, the fact that such a possibility has likely not been considered by the drafters of the GDPR, nor by the Article 29 Working Party[936], does not mean that the text of Article 20 could not be read as allowing such continuous portability.

Nevertheless, due to this uncertainty, some authors argue that Article 20, in its current form, does not allow for the continuous porting of personal data; that this makes it highly burdensome for data subjects to use their data portability right as they have to repeat their requests; and that this limits its effectiveness and the potential benefits they can derive from it.[937] As a consequence, there are growing calls for the establishment of such near real-time continuous porting initiatives.[938] This will be further detailed in Section C.

[935] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 10.
[936] None of the examples provided by the Article 29 Working Party in its guidelines on the right to data portability addresses continuous porting (Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017).
[937] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 13; Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 10.
[938] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 20; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 81.

Section B. "Empowerment" initiatives imposing B2B data sharing in order to address specific market failures

152. While the revised version of the Article 29 Working Party's guidelines on the GDPR's data portability right now state explicitly that the main objective of this right is to promote the exercise of fundamental rights and not to deal with market failure / competition law issues[939], several other empowerment initiatives have, on the contrary, precisely been adopted in order to address specific market failures, through the strengthening of the individuals' control on their data. Such initiatives, to which this thesis will now turn, are contained in the Digital Content Directive[940], in the revised Directive on payment services in the internal market ("PSD2")[941], and in the Electricity Directive.[942]

a) Data retrieval right in the Digital Content Directive

153. The first "empowerment" initiative imposing B2B data sharing in order to address a specific market failure is the data retrieval right enshrined in Article 16.4 of the Directive on the supply of digital content and digital services ("Digital Content Directive").[943] This Article provides that, in the event of the termination of a contract between a trader[944] and a consumer[945] for the supply of digital content[946] or digital services[947], the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader.[948] Furthermore, the consumer shall be entitled to retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format.[949]

Article 16.4 thus grants the consumers with a "data retrieval right", but does not allow the direct transmission of data between two firms, since it only aims to establish the consumer's

---

[939] See point 137. Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.
[940] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019.
[941] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015.
[942] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, *OJ L 158/125*, 14 June 2019.
[943] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019.
[944] "Any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive" (Article 2.5 of Directive 2019/770).
[945] "Any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession" (Article 2.6 of Directive 2019/770).
[946] "Data which are produced and supplied in digital form" (Article 2.1 of Directive 2019/770).
[947] "A service that allows the consumer to create, process, store or access data in digital form; or that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service" (Article 2.2 of Directive 2019/770).
[948] Article 16.4, al. 1 of Directive 2019/770.
[949] Article 16.4, al. 2 of Directive 2019/770.

right to recover the data personally after the termination of the contract.[950] In this sense, it is closer to the right of access contained in the GDPR, which allows a data subject to obtain a copy of her personal data.[951] The trader is thus required to share the data with the consumer, but not with other undertakings. There is thus no equivalent of Article 20.2 of the GDPR in the Digital Content Directive. Naturally, the consumer is, herself, free to share the data she has recovered through the data retrieval right with another content or service provider. The regime created by Article 16.4 of the Digital Content Directive thus diverges from the regime created by Article 20 of the GDPR, although they present some similarities.[952]

1. Objectives and scope of application

154. The objective of the data retrieval right contained in the Digital Content Directive is to tackle market failures deriving from consumer lock-in on the digital content markets, through the means of consumer empowerment.[953] More concretely, it aims at giving more control to consumers on their data and at making it easier for consumers to change service providers. Indeed, the proposal at the origin of the Directive outlined that, in order to promote competition, it is necessary to ensure that consumers can easily switch content providers, by reducing legal, technical and practical obstacles, such as the inability to recover all the data that the consumer has produced or generated through her use of digital content.[954] This is because the consumer could be deterred from terminating a contract for digital content or a digital service if she cannot recover access to the content in question as a result of such termination.[955]

155. Article 16.4 of the Digital Content Directive applies to "any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader".[956] It therefore only applies to non-personal data that the consumer has (actively) provided or created (e.g. data that she has generated through her use of the content or service, i.e. "observed data" in this thesis' typology), but not to inferred/derived data nor to acquired data. Indeed, here, and contrary to Article 20 of the GDPR, the wording of Article 16.4 does not leave room for doubt on the fact that "acquired provided data" and "acquired observed data" do not fall in the scope of this article, as it explicitly refers to data provided "when using the digital content or digital service supplied by the trader", which thus excludes data provided when using a third party's content or service.

---

[950] Article 16.4 of Directive 2019/770; I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, Alphen aan den Rijn, Kluwer, 2016, p. 148.
[951] Article 15.3 of the GDPR.
[952] For more information on the comparison between this data retrieval right and the data portability right enshrined in Article 20 of the GDPR see also: I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *German Law Journal*, 2018, Issue 19(6), p. 1359-1398; I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper DP 2019-005*, November 2019, available at https://ssrn.com/abstract=2956308; M. Ledger et T. Tombal, "Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ?", *R.D.T.I.*, 2018/3, n°72, p. 25-44.
[953] Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634 final, p. 3.
[954] *Ibid*., p. 22.
[955] Recital 70 of Directive 2019/770.
[956] Article 16.4 of Directive 2019/770.

Moreover, it does not apply to data that has no utility outside the context of the digital content or digital service supplied by the trader (for instance, the consumer's login and password); to data that only relates to the consumer's activity when using the digital content or digital service supplied by the trader (for instance, data about the fact that the consumer has stopped watching in the middle of the movie, so that when she returns, she can start over from that point and does not have to restart from the beginning); or to data that has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts (for instance, data that contributed to the identification of viewing or listening trends in a specific country).[957] These exceptions are justified by the fact that, in those cases, the content is of little practical use to the consumer, who therefore has a limited interest in retrieving such data, particularly in view of the fact that requiring such a mechanism would be costly for the trader.[958]

The scope of application of the Directive is thus complementary to that of the right to data portability in the GDPR, which applies to personal data "provided" by the data subject.[959] This is explicitly stated in the text of the Directive, which provides that the trader remains bound by the obligations of the GDPR[960], which prevails over this Directive in the event of a conflict of provisions.[961] It therefore seems that the objective of the final text of this Directive was to avoid any overlap with the regime of Article 20 of the GDPR.[962] However, this distinction between personal and non-personal data is problematic in practice. This is because it is difficult to imagine situations in which content provided by the consumer would not qualify as personal data. Indeed, given the GDPR's broad definition of this concept, namely "any information relating to an identified or identifiable natural person"[963], the vast majority (if not all) of the data provided or created by the consumer will likely be considered as personal data.[964]

Although the scope of application of the Directive and of the GDPR are complementary, none of these instruments apply to inferred/derived data. This echoes a key balancing exercise underlying "empowerment" initiatives imposing B2B data sharing, namely between the benefits of sharing for the specific individual and the need to preserve the business interests of the data holder, which will be further detailed below.[965]

---

[957] Article 16.3 of Directive 2019/770.
[958] Recital 71 of Directive 2019/770.
[959] See points 144 and 145.
[960] Article 16.2 of Directive 2019/770.
[961] Article 3.8 of Directive 2019/770.
[962] On the contrary, the proposal at the origin of the Directive targeted "all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content" (Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634 final, articles 13.2.c) and 16.4.b)). The reference to "any data" would have thus potentially covered personal data. Accordingly, the wording of this provision seems to have been adapted in order to avoid any overlap with the GDPR and its right to data portability, which would apply in parallel (see Recital 38 of Directive 2019/770).
[963] Article 4.1 of the GDPR.
[964] See Part I, Chapter 1, Section B. See also N. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, 2018, Vol. 10, Issue 1, p. 40-81.
[965] See Part II, Chapter 2, Section A, a) "Finding a balance between the benefits for the specific individual and the business interests of the data holder".

2. Exercise of the right

156. Similarly to Article 20 of the GDPR[966], the Digital Content Directive also provides that the consumer shall be entitled to retrieve the data free of charge.[967] Regarding the deadline to process the requests, the Directive only provides that the data should be given to the consumer "within a reasonable time" after the termination of the contract.[968] While the Directive does not provide any further information as to how these terms must be interpreted, the deadline of one month provided in the GDPR (three months for complex cases)[969] could arguably be used to assess this "reasonable" character.

157. As a welcome development, the format requirements contained in the final text of the Digital Content Directive have been aligned with those contained in the GDPR, as the data must be returned to the consumer "in a commonly used and machine-readable format".[970] This was not the case in the proposal at the origin of the Directive, which had less stringent data format requirements than Article 20 of the GDPR, as this initial text provided that the data had to be returned to the consumer in a "commonly used data format".[971] In this sense, the proposal was closer to the format requirement for the right of access in the GDPR, according to which the data had to be delivered in a "commonly used electronic form".[972] It should however be noted that the requirement for a "structured format" is not mentioned in the Directive, whereas it appears in Article 20 of the GDPR.[973] Moreover, the Digital Content Directive does not make any reference to the need for interoperability, while Recital 68 of the GDPR adds that the format should also be interoperable (although this requirement does not appear in the text of Article 20).[974]

158. Regarding the influence of the exercise of the right on the data holder's ability to keep using the data, the Digital Content Directive provides that, when the consumer terminates the contract, the trader must refrain from using the non-personal data provided or created by the consumer, and will thus have to erase them.[975] This is a clear difference with the right to personal data portability in the GDPR, which does not automatically imply an obligation for the data holder to stop using the ported data.[976] Indeed, the right to data portability is not limited to "one-shot" data transfers.[977] The exercise of the data retrieval right, on the other

---

[966] See point 148.
[967] Article 16.4 of Directive 2019/770.
[968] *Ibidem*.
[969] See point 147.
[970] Article 16.4 of Directive 2019/770.
[971] Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634 final, articles 13.2.c) and 16.4.b).
[972] Article 15.3 of the GDPR.
[973] See point 149.
[974] See point 149.
[975] Article 16.3 of Directive 2019/770. The trader can however continue to use some of the data that had been provided or created by the consumer, namely the data that has no use outside the context of the content or service; that only relates to the consumer's activity when using the content or service; that has been aggregated with other data by the trader and cannot be disaggregated or can only be disaggregated with disproportionate effort; or that has been generated jointly by the consumer and other persons who continue to use the content or service (Article 16.3 of Directive 2019/770).
[976] Article 20.3 of the GDPR.
[977] See points 150 and 151.

hand, amounts to a "one-shot" transfer. The difference between the two regimes can be explained by the fact that data can be ported at any time under the GDPR, while the data retrieval right can only be used after the termination of the contract by the consumer.[978]

159. To sum up, the Digital Content Directive creates an "empowerment" compulsory B2B data sharing mechanism that is analogous, yet non-identical, to Article 20 of the GDPR. Indeed, these mechanisms have complementary scopes of application. Moreover, they are aligned in terms of costs and deadline to process the request, and in terms of format requirements, even if the Digital Content Directive does not mention the "structured format" requirement. However, these mechanisms diverge when it comes to the objective that they pursue, to the consequences of the exercise of the right and to the temporality of requests. More importantly, Article 16.4 of the Digital Content Directive only requires the trader to share the data with the consumer, but not with other undertakings. There is thus no equivalent of Article 20.2 of the GDPR in the Digital Content Directive, which makes it a much less efficient "empowerment" compulsory B2B data sharing mechanism.

b) PSD2 and Open Banking

160. The second "empowerment" initiatives imposing B2B data sharing in order to address a specific market failure are the data access and use rights granted in Articles 65 to 67 of the revised Directive on payment services in the internal market ("PSD2").[979] In the UK, PSD2 has been further refined by the Open Banking initiative[980], which is worth presenting here as well.

1. Access to and use of banking data in PSD2

161. PSD2 allows the providers of payment initiation services and the providers of account information services[981] to access and use the payment account information[982] of the users of their services (the consumers), if the latter have explicitly consented to it.[983] Thus, thanks to PSD2, a service provider creating a smartphone payment application, for example called "Easypay", will be able to obtain access to, and to use, the bank account data of the users of

---

[978] I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit.*, p. 148.
[979] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015.
[980] Competition and Markets Authority, "The Retail Banking Market Investigation Order 2017", 2017, available at https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-bankingmarketinvestigationor der-2017.pdf; Competition and Markets Authority, "Final Approved Roadmap for Open Banking", 14 May 2020, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885537/Notice_of_proposed_changes_to_the_open_banking_roadmap_-_web_publication_-_cma_gov_uk_---_May_2020_-.pdf.
[981] Respectively defined as "a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider" and as "an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider" (Articles 4.15 and 4.16 of the Directive 2015/2366).
[982] Defined as "account held in the name of one or more payment service users which is used for the execution of payment transactions" (Article 4.12 of the Directive 2015/2366).
[983] Articles 65 to 67 of the Directive 2015/2366.

this application who wish to carry out a transaction, in order to ensure that they have sufficient funds and to validate the transaction. However, such access may only be granted if the service provider has obtained the explicit consent of the user of the mobile application (generally via adherence to the services' terms and conditions). Moreover, there is no correlative obligation for the banks to erase or stop processing the data, and the providers of payment initiation services and of account information services shall only process (e.g. access, use and store) personal data necessary for the provision of their services, in full compliance with the data minimisation principle of the GDPR.[984]

PSD2 notably aims at tackling the consumer lock-in and consumer inertia market failures that have been observed in the banking sector, through the empowerment of these consumers by giving them more control on their banking data and operations, and by providing them with more choice and transparency.[985] Indeed, by allowing the access to, and the use of, the payment account information of the incumbent banks, PSD2 promotes the development of innovative payment services through increased competition on the market, and the consequence should be that consumers are no longer "locked-in" the services of their traditional bank, as they are provided with alternative choices and better offers of payment services.[986] Moreover, this access and use can give rise to complementary account information services, which the consumers can use in order to have an aggregated view of their accounts (that could be spread out across several banks), and this would allow them to have a clearer visibility on their finances and empowers them to manage them more efficiently.[987]

162. In fact, it is argued that the data access and use rights granted in Articles 65 to 67 of PSD2 could be seen as a sector-specific complement to Article 20.2 of the GDPR, as it compels the banks (data holders) to make the direct transmission of the data subjects' personal banking information to recipients "technically feasible". [988] This is a key difference with Article 20.2 of the GDPR, which contains no such technical feasibility obligation.[989] Another key difference with Article 20 of the GDPR is that PSD2 expressly provides for continuous portability through the use of APIs.[990] Indeed, the European Commission adopted regulatory technical standards, based on a draft of the European Banking Authority, which

[984] Article 94.2 of the Directive 2015/2366. The data minimisation principle is enshrined in Article 5.1.c) of the GDPR.
[985] Recitals 5 and 6 of the Directive 2015/2366.
[986] Recital 67 of the Directive 2015/2366.
[987] Recital 28 of the Directive 2015/2366.
[988] G. Colangelo and O. Borgogno, "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule", *Stanford-Vienna European Union Law Working Paper No. 35*, 2018, available at https://law.stanford.edu/publications/no-35-data-innovation-and-transatlantic-competition-in-finance-the-case-of-the-access-to-account-rule/, p. 3; S. Vezzoso, "Fintech, Access to Data, and the Role of Competition Policy", 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106594, p. 12-13.
[989] See *supra* point 139.
[990] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 32.

notably impose the obligation for banks to set in place at least one API to support this data sharing mechanism.[991]

In light of these two differences, the data sharing mechanism in PSD2[992] might thus, at first sight, seem much more effective than the one contained in Article 20 of the GDPR. Yet, much like for data portability, while Recital 93 of PSD2 provides that the interoperability of the different technological communication solutions should be ensured, none of the articles of PSD2 refer to this necessary interoperability. As a consequence, each banking institution holding these payment account data is free to set up its own API allowing continuous portability. This may lead to interoperability problems if each of these institutions develops a mechanism based on different technical standards.[993] Indeed, while the European Commission's regulatory technical standards mentioned above list minimal technical requirements that must be met by the various APIs (notably in terms of identification and authentication)[994], and provides that the APIs should be based on existing international or European standards[995], it does not in any way require the various banks to use a single common standard for their APIs. This is why it is relevant here to mention the UK's Open Banking initiative[996], which went further in this regard than PSD2.

2. The UK's Open Banking initiative

163. In the UK, as a result of its market investigation in the banking sector[997], the Competition and Markets Authority required the nine major UK banks to build and ensure the maintenance of common and open APIs, based on common technical standards, to allow data sharing with providers of payment initiation services and of account information services.[998] This avoids the interoperability issue outlined above as the payment initiation service providers and account information service providers only have to develop specific technical solutions to connect to these common APIs for all nine banks, rather than having to develop a multitude of technical solutions to connect to various non-interoperable APIs (one API per bank).

---

[991] Commission Delegated Regulation 2018/389 of 27 November 2017 supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, *OJ L 69/23*, 13 March 2018, articles 30 to 36.

[992] PSD2 can indeed be considered as creating a data sharing mechanisms as the payment account information may not only be accessed, but also used and stored by the providers of payment initiation services and of account information services (see Articles 66.3, g) and 67.2, f) of the Directive 2015/2366).

[993] G. Colangelo and O. Borgogno, "Data, Innovation and Transatlantic Competition in Finance", *op. cit.*, p. 25.

[994] Articles 30.1 and 30.2 of the Commission Delegated Regulation 2018/389.

[995] Article 30.3 of the Commission Delegated Regulation 2018/389.

[996] Competition and Markets Authority, "The Retail Banking Market Investigation Order 2017", *op. cit.*; Competition and Markets Authority, "Final Approved Roadmap for Open Banking", *op. cit.*

[997] Competition and Markets Authority, "Retail Banking Market Investigation – Final Report", 26 February 2016, available at https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk.

[998] Competition and Markets Authority, "The Retail Banking Market Investigation Order 2017", *op. cit.*; Competition and Markets Authority, "Making Banks Work Harder for You", 9 August 2016, available at http://www.agefi.fr/sites/agefi.fr/files/fichiers/2016/08/cma_overview-of-the-banking-retail-market_9_aout_.pdf. See also Open Data Institute and Fingleton, "Open Banking, Preparing for lift off: Purpose Progress and Potential", 16 July 2019, available at https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf.

As for PSD2, the goal behind this common API is to foster the development of new services that will be better tailored to consumer's specific needs, and this should empower them to better manage their finances, notably by being able to manage accounts held in several banks through a single application, by moving funds between their various accounts in order to avoid overdraft charges or higher interest payments, or by being able to make simple, safe and reliable price and service quality comparisons in order to select those that are the best tailored to their financial profile.[999] Indeed, the Competition and Markets Authority's investigation in the banking sector[1000] showed that this market was gangrened by "consumer inertia", as "more than half of retail banking customers stayed with their bank for more than 10 years and three-quarters of them did not look for more efficient alternatives on the market in the previous year".[1001] The goal is thus to give consumers more control over their banking data by allowing them to securely share it with third parties, in order to be offered better financial services, more choice and lower prices.[1002] Consumers are thus empowered to compare services, which should facilitate multi-homing and service switching.[1003] They have an active role to play in the digital ecosystem, provided that their searching and switching costs are reduced.[1004]

164. More concretely, these nine banks were required to fund, and cooperate with, the Open Banking Implementation Entity (OBIE), which is the independent body responsible for building and maintaining these common and open APIs.[1005] In substance, the role of the OBIE is to: "(i) design the specifications for the APIs that banks use to securely provide Open Banking, (ii) support regulated third party providers and banks to use the Open Banking standards, (iii) create security and messaging standards, (iv) manage the Open Banking Directory which allows regulated participants like banks and third party providers to enrol in Open Banking, (v) produce guidelines for participants in the Open Banking ecosystem and (vi) set out the process for managing disputes and complaints".[1006]

Interestingly, the OBIE followed a "minimum viable product" approach, through which the APIs were made live as early as possible in order to receive quick user feedback allowing to adapt the APIs through iteration.[1007] This approach contributed to the success of the initiative. Another factor that contributed to its success is that recipients have to be authorised by the Financial Conduct Authority (FCA) to get access to the banks' data.[1008] The goal is to protect the consumers by ensuring that these entities are secure and that their services and processing

---

[999] Competition and Markets Authority, "Making Banks Work Harder for You", *op. cit.*, p. 6-8.
[1000] Competition and Markets Authority, "Retail Banking Market Investigation – Final Report", *op. cit.*
[1001] O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking", 3 January 2020, available at SSRN: https://ssrn.com/abstract=3513514, p. 5.
[1002] Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit.*, p. 6.
[1003] *Ibid*., p. 4.
[1004] O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance", *op. cit.*, p. 4 and 12.
[1005] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 32.
[1006] *Ibid*., p. 32-33. See also Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit.*, p. 22-25.
[1007] Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit.*, p. 4.
[1008] *Ibid*., p. 25.

activities are legitimate and lawful. There are now 135 entities approved by the FCA to offer services that use Open Banking, and these are listed in the "Open Banking Directory", which serves the role of a whitelist.[1009]

165. To conclude on this empowerment" initiatives, it should be mentioned that the Open Banking initiative, similarly to PSD2, is currently limited to banking (accounts) information. However, the aim of some organisations, such as the Open Data Institute, is to expand this initiative to "Open Finance" (mortgages, pensions, insurances) and to other sectors such as energy and telecoms[1010], as it is argued that this would also empower consumers in these fields by offering them more control on their data in order to be offered more choices.[1011] For instance, as outlined by the Open Data Institute, "if smart meter data was accessible it may make switching easier and enable customers to easily take advantage of cheaper tariffs and off-peak energy pricing".[1012]

c) Electricity Directive

166. In fact, this expansion towards other sectors has already started as Article 20 of the Directive on common rules for the internal market for electricity ("Electricity Directive") provides that "it shall be possible for final customers to retrieve their metering data or transmit them to another party at no additional cost and in accordance with their right to data portability".[1013] This is a third "empowerment" initiative imposing B2B data sharing in order to tackle a specific market failure, as its goal is to strengthen competition on the energy market. More specifically, this article provides that "if final customers request it, data on the electricity they fed into the grid and their electricity consumption data shall be made available to them through a standardised communication interface or through remote access, or to a third party acting on their behalf, in an easily understandable format allowing them to compare offers on a like-for-like basis".[1014] Moreover, "non-validated near real-time consumption data shall also be made easily and securely available to final customers at no additional cost, through a standardised interface or through remote access, in order to support automated energy efficiency programmes, demand response and other services".[1015]

This Directive also provides that the parties responsible for data management of the final costumer's data (metering and consumption data as well as data required for customer switching, demand response and other services) should provide access to it to any "eligible party" in a non-discriminatory manner.[1016] Surprisingly, while the Commission's proposal provided that "eligible parties" shall include at least "customers, suppliers, transmission and

---

[1009] *Ibid*., p. 24 and 35. See p. 26-32 for a list of Open Banking use cases.
[1010] On the portability of data in the telecoms and pay TV services, see Ofcom, "Update on Open Communications: Enabling people to share data with innovative services", 7 July 2021, available at https://www.ofcom.org.uk/consultations-and-statements/category-1/open-communications.
[1011] Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit*., p. 4-5.
[1012] *Ibid*., p. 5.
[1013] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, *OJ L 158/125*, 14 June 2019, article 20, al. 2.
[1014] Article 20, al.1, e) of the Directive 2019/944.
[1015] Article 20, al.1, a) of the Directive 2019/944.
[1016] Articles 23.1 and 23.2 of Directive 2019/944.

distribution system operators, aggregators, energy service companies, and other parties which provide energy or other services to customers"[1017], the final text of the Directive does not define this notion, which creates uncertainties as to who can benefit from this access.[1018] While these eligible parties can be charged a fee for this access, the access should be free for the final costumers.[1019] The Member States have a role to play in promoting this data access, as they should ensure efficient and secure data access and exchange, as well as data protection and data security.[1020] They should also facilitate the full interoperability of energy services by ensuring that electricity undertakings apply the interoperability requirements and procedures for access to data, which will be adopted by the Commission in implementing acts of the Directive.[1021] Moreover, Article 34 of this Directive provides that if smart metering systems[1022] have been deployed in a Member State, and that distribution system operators[1023] are involved in the management of this smart meter data, this Member State shall ensure that all eligible parties (suppliers and service providers) have non-discriminatory access to this smart-meter data under clear and equal terms, in accordance with the relevant data protection rules.

167. The above could be seen as another sector-specific complement to Article 20.2 of the GDPR, aiming at solving market failures through the empowerment of individuals, which creates a form of continuous individual-level data sharing. Indeed, this provides individuals with the tools to participate more actively in the energy market[1024], thanks to accurate and near real-time feedback on their energy consumption[1025], which allows them to better manage their consumption and to benefit from affordable energy through the facilitated possibility to switch for suppliers offering lower tariffs.[1026]

[1017] Article 23.1 of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast), 30 November 2016, COM/2016/0864 final.
[1018] See C. Ducuing, "Data as infrastructure? A study of data sharing legal regimes", *Competition and Regulation in Network Industries*, Vol. 21, Issue 2, 2020, p. 124–142.
[1019] Article 23.5 of Directive 2019/944.
[1020] Article 23.2 of Directive 2019/944.
[1021] Article 24 of Directive 2019/944.
[1022] "An electronic system that is capable of measuring electricity fed into the grid or electricity consumed from the grid, providing more information than a conventional meter, and that is capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication" (Article 2.23 of Directive 2019/944).
[1023] "A natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity" (Article 2.29 of Directive 2019/944).
[1024] Recital 10 of the Directive 2019/944.
[1025] Recital 52 of the Directive 2019/944.
[1026] Recitals 43, 48 and 52 of the Directive 2019/944.

Section C. Growing call for a new "empowerment" initiative imposing B2B data sharing: "continuous portability"

168. So far, this thesis has presented the existing "empowerment" initiatives imposing B2B data sharing, which either aim to allow the exercise of fundamental rights or to address specific market failures.[1027] However, there are growing criticisms about the effectiveness of these initiatives, and about their ability to truly empower individuals.[1028] This is, for instance, the case with Article 20 of the GDPR, which fails to impose direct portability[1029], and which, according to some authors, falls short of requiring continuous portability.[1030] This is also the case with Article 16.4 of the Digital Content Directive, which only grants to the consumer a data retrieval right at the termination of the contract with the trader.[1031] Accordingly, there have been calls for the creation of a new "empowerment" initiative imposing B2B data sharing, namely the introduction of a "continuous portability" right.[1032] In the UK, this is sometimes referred to as "Data mobility".[1033]

"Continuous portability" implies that data can be transferred – usually via application programming interfaces ("APIs")[1034] – in a timely and frequent manner from a data holder to a data recipient, on a constant basis and in (near) real-time.[1035] Rather than merely providing for bulk transfers, such continuous portability would allow, with the consent of the individual whose data is shared, for a continuous flow of data between data holders and data recipients. This would allow the individuals to benefit immediately from the services of the recipient, as the latter would receive immediate and continuous access to the data that it needs to offer this service, rather than having to wait for a bulk transfer of data from the data holder or from the individual.[1036]

[1027] See Part II, Chapter 1, Sections A and B.
[1028] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 79.
[1029] Article 20.2 of the GDPR only provides that the data subject has the right to have the personal data transmitted directly from one controller to another *where technically feasible* (emphasis added).
[1030] See Part II, Chapter 1, Section A, c), 3. This thesis however argues that Article 20.2 of the GDPR could be read as enabling a data subject to request a continuous flow of the data, pertaining to her, between the data holder and a data recipient "where technically feasible".
[1031] See Part II, Chapter 1, Section B, a).
[1032] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 20; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*
[1033] See CtrlShift, "Data mobility: The personal data portability growth opportunity for the UK economy", 2018, available at https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf.
[1034] "An application programming interface (API) is an interface or communication protocol between a client and a server intended to simplify the building of client-side software. It has been described as a "contract" between the client and the server, such that if the client makes a request in a specific format, it will always get a response in a specific format or initiate a defined action" (https://en.wikipedia.org/wiki/Application_programming_interface).
[1035] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 81.
[1036] *Ibid*., p. 79.

169. In practice, this could be done either through an extension of Article 20 GDPR[1037], or through the adoption of a new legal instrument. Yet, as a modification of the GDPR seems highly unlikely, in light of the complicated negotiations it entailed and of its recent entry into force, the second option seems more realistic. This second option itself opens an alternative between the adoption of a participative and non-binding approach via the establishment of codes of conducts, on the one hand, and the adoption of a binding regulatory instrument making it compulsory for (certain categories of) data holders to implement the necessary standards and APIs enabling continuous portability.[1038] However, as participative and non-binding approaches are strongly criticised[1039], while compulsory instruments (such as PSD2, the Open Banking initiative and the Energy Directive) are praised for the empowering effects they have on individuals[1040], it would be preferable to opt for the latter. In this regard, it is worth underlining that the European Commission's proposal for a Digital Markets Act[1041] provides that "gatekeepers"[1042] will have to provide tools facilitating continuous portability[1043], while its inception impact assessment on its future "Data Act" hints at the fact that certain undertakings, notably those selling smart home appliances, wearables and home assistants, could be required to create technical interfaces allowing real-time portability.[1044]

170. The creation of a continuous portability right would arguably entail benefits for the individual whose data is ported. Indeed, in order to empower individuals by offering them more choice, it is necessary to ensure that large data holders are not the only ones having the most up-to-date data about individuals.[1045] In this perspective, continuous portability, rather than bulk transfers of historic data, could further lower switching costs and facilitate multi-homing, by ensuring that seamless and real-time access to the individuals' data is only one

---

[1037] This thesis however argues that Article 20.2 of the GDPR could already be read as enabling a data subject to request a continuous flow of the data, pertaining to her, between the data holder and a data recipient "where technically feasible". See Part II, Chapter 1, Section A, c), 3.
[1038] *Ibid*., p. 81-82.
[1039] See below point 179. B. Lundqvist, "Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law", *Stockholm Faculty of Law Research Paper Series n° 54*, 2018, available at https://ssrn.com/abstract=3103870, p. 43-46. See also L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability", *EDPL*, 2020/1, p. 90-93.
[1040] See Part II, Chapter 1, Section B, b) "PSD2 and Open Banking" and c) "Electricity Directive".
[1041] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.
[1042] See Articles 2.1 and 3 of the Proposal for a Digital Markets Act. For more details on the designation of these gatekeepers, see points 397 and 398.
[1043] Article 6.1.h) of the Proposal for a Digital Markets Act.
[1044] European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 6.
[1045] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 80.

click away, which is necessary to offer truly valuable services.[1046] In turn, this could entail wide-scale switching[1047], as individuals would be offered alternative options in real-time.[1048]

171. Looking at the example of PSD2 in general, and of the UK's Open Banking initiative in particular, the requirement to build and ensure the maintenance of common and open APIs, based on common technical standards, to allow data sharing with providers of payment initiation services and of account information services, opens the room for continuous portability.[1049] Arguably, this would generate more switching possibilities, would allow consumers to avoid "loyalty penalties", as they end up paying more for essential services such as banking, energy and telecoms when they do not switch providers.[1050] This is because incumbents often charge higher prices to long-term consumers, due to a combination of behavioural biases, asymmetry of information and lack of bargaining power.[1051]

172. Such continuous portability could also be envisaged in other fields, as illustrated by Article 20 of the Electricity Directive presented above[1052], or the UK's Smart Data initiative.[1053] The aim of this initiative, which expressly states that it is an extension of the GDPR's data portability right, is to make data about consumers more easily and instantly accessible to them, and to allow them to be able to transfer it securely via APIs to third parties who can use it to provide them with innovative services.[1054] In turn, this would reduce the efforts required from consumers in order to find deals that best suit them.[1055] Indeed, presently, consumers need to engage in significant effort in order to understand if they benefit from the best deals available, and searching for, and switching to, better alternatives is highly time consuming.[1056] Some therefore call for more proactive approaches in order to incentivise individuals to port their data, as due to strong consumer inertia[1057], "simply relying on

---

[1046] *Ibid*., p. 9 and 80; OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 43. See also J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era – Final report*"*, 2019, available at http://ec.europa.eu/competition/publications/reports/ kd0419345enn.pdf.

[1047] OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 44. See also M. Gal and O. Aviv, "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*, September 2020, Volume 16, Issue 3, p. 349-391.

[1048] Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit*., p. 6.

[1049] See point 163. Competition and Markets Authority, "Retail Banking Market Investigation – Final Report", *op. cit*.; Competition and Markets Authority, "The Retail Banking Market Investigation Order 2017", *op. cit*.; Competition and Markets Authority, "Making Banks Work Harder for You", *op. cit*. See also Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit*.

[1050] *Ibid*., p. 39.

[1051] O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance", *op. cit*., p. 1 and 6.

[1052] See point 166. See Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, *OJ L 158/125*, 14 June 2019, article 20, al. 2.

[1053] See HM Government, "Smart Data: Putting consumers in control of their data and enabling innovation", June 2019, available at https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation.

[1054] *Ibid*., p. 9 and 11.

[1055] *Ibid*., p. 11.

[1056] *Ibid*., p. 13.

[1057] See point 97.

engaging consumers by providing them with more information has proven to be a rather ineffective approach".[1058]

173. In this perspective, (continuous) portability could enable third parties to be more proactive and to actively inform the individual about the fact that it is in a position to provide her with a better and/or cheaper product/service, and this could reduce the hassle of switching. Coming back to the example of the Smart Data initiative, it outlines that individuals should be able to use a single product/service developed by a third party, which could monitor their various consumption and/or financial data and, on that basis, could actively suggest to them to switch towards the product/service of an alternative undertaking that better matches their needs and preferences, ideally by proposing "one click switching" possibilities.[1059] Third parties could even go a step further, by offering automatic switching services "that enable consumers to set their preferences and let the service switch them automatically if a better deal appears".[1060] Such automatic switching services are already available in the UK's energy market and they automatically select the best tariffs available for the individual, on the basis of parameters that she has set.[1061] Some argue that this would especially be valuable for vulnerable individuals who, for instance, have difficulties managing their finances.[1062] Naturally, the sharing of the individual's data should be secure and subject to her consent and to the verification of her identity through a secure authentication process, and this could be coupled with the requirement, for data recipients, to obtain an accreditation in order to ensure that their services are legitimate, secure and comply with the personal data protection requirements.[1063] Moreover, it is fundamental to underline that these potential individual short-term gains that are promised to individuals via these "empowerment" initiatives will have to be balanced with the potential long-term costs and collective costs in terms of control, autonomy and self-determination.[1064]

174. In fact, the third parties mentioned in the previous paragraph could be Personal Information Management Systems (PIMS)[1065], as these can offer a centralised dashboard for monitoring and controlling the uses of an individual's data[1066], which can be managed either by the individual herself, or by an independent intermediary acting on her behalf.[1067] In

---

[1058] O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance", *op. cit.*, p. 2.
[1059] HM Government, "Smart Data: Putting consumers in control of their data and enabling innovation", *op. cit.*, p. 13.
[1060] *Ibidem*.
[1061] *Ibid*., p. 16.
[1062] *Ibid*., p. 22.
[1063] *Ibid*., p. 28. On this point see Part II, Chapter 2, Section C, c).
[1064] See Part I, Chapter 2, Section C, b) and Part II, Chapter 2, Section A, c).
[1065] For more information on these PIMS, see point 109.
[1066] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 13. See also, CtrlShift, "Data mobility: The personal data portability growth opportunity for the UK economy", *op. cit.*; Competition and Markets Authority, "Online platforms and digital advertising: Market study interim report – Appendix L: Potential approaches to improving personal data mobility", 18 December 2019, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.
[1067] S. Delacroix and N. Lawrence, "Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance", *International Data Privacy Law*, November 2019, Volume 9, Issue 4, p. 236-252. See also C.

substance, a PIMS allows an individual to build an integrated view of her data, which is normally spread across different services, in a system that she controls and trusts, via high-performance APIs.[1068] In this regard, the introduction of a continuous portability right could enable the efficient functioning of such PIMS, through seamless and real-time access to the individual's data.

However, caution should be exercised in view of the potential "centralisation" of personal data that such initiatives may represent. Indeed, it would be inappropriate to gather all the personal data in question in a single database, however secure it may be, otherwise a "Single Point of Failure" could be created. It is therefore imperative to consider decentralised data storage models for the technical implementation of these PIMS.[1069] Although these decentralised models heavily rely on the availability of powerful APIs, they are more scalable than centralised models as they do not require as much local storage and computational capacity.[1070] An example of such decentralised PIMS is the *Solid Project* mentioned above.[1071]

The introduction of a continuous portability right enabling seamless and real-time access to the individual's data could boost the prospect of the emergence of such PIMS. However, some have questioned whether the business model of a privately-financed PIMS is sustainable.[1072] Indeed, "privately funded PIMS, which rely on revenue generation from users, from the data controllers or on the data markets, may either not be sustainable or not have a significant impact on the data ecosystem".[1073] There might thus be a need for publicly funded or non-for-profit open-source PIMS, the creation of which could be facilitated by the setting of common standards, which are currently lacking.[1074] It should however be outlined that, independently of this concern, one of the aims of the European Commission's proposal for a Data Governance Act is precisely to stimulate the emergence of such PIMS, by increasing trust in data sharing and by lowering transaction costs.[1075]

Wendehorst, "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 349-353.

[1068] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 45 and 67.

[1069] T. Tombal, "Les droits de la personne concernée dans le RGPD", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 509-510.

[1070] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 45.

[1071] See point 139. See https://solidproject.org/

[1072] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 66-73.

[1073] *Ibid*., p. 72.

[1074] *Ibid*., p. 67 and 72-73.

[1075] See Recital 23 and Article 9.1.b) of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final. See also p. 7 of its "Explanatory memorandum". See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final, p. 11-12; B. Martens, A. de Streel, I. Graef, T.

Section D. The recent phenomenon of regulatory initiatives pertaining to specific (small) business users: from individual empowerment towards small businesses empowerment

175. So far, Sections A to C have focussed on "empowerment" initiatives imposing B2B data sharing that aim to empower individuals. It is however necessary to briefly discuss a more recent phenomenon, namely regulatory initiatives aiming at "empowering" specific (small) business users. These represent the beginning of a move from individual empowerment towards small businesses empowerment, which fits in a broader context of extending consumer protection (B2C) towards small businesses protection (B2b). At the European level, a clear example of this broader trend is the Directive on unfair trading practices in business-to-business relationships in the agricultural and food supply chain.[1076] At the national level, Belgium adopted a law on the abuse of economic dependence, abusive clauses and unfair trading practices in business-to-business relationships.[1077] In the same vein, in the Netherlands, Article 6:235(1) of Civil Code (*Burgerlijk Wetboek*) provides that the list of black and grey unfair clauses for B2C contracts also applies to standard form contracts concluded with SMEs in B2b settings.[1078] Moreover, several Member States have extended the scope of the Unfair Commercial Practices Directive[1079] to B2b settings.[1080]

Importantly, it should be outlined from the outset that while the word "empowerment" is used for both individuals and small business users in this thesis, this word should not be understood exactly in the same way in these two situations. Indeed, as outlined above[1081], "empowering" individuals means giving them more control on their data, in order for them to be able to take appropriate decisions about *all aspects of their lives*. On the other hand, initiatives "empowering" small business users should be understood in a narrower way, as a solely *economic "empowerment"* to operate freely and efficiently on the market, which derives from their freedom to conduct a business. Indeed, as will be shown below, such initiatives mainly attempt to rebalance the strong discrepancies in bargaining power that these small users suffer

---

Tombal and N. Duch-Brown, "Business to business data sharing: an economic and legal analysis", *EU Science Hub*, 2020, available at https://ssrn.com/abstract=3658100, p. 25-27.

[1076] Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, *OJ L 111/59*, 25 April 2019.

[1077] Loi du 4 avril 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *M.B.*, 24 mai 2019.

[1078] G. Sulija, *Standard Contract Terms in Cross-Border Business Transactions – A Comparative Study from the Perspective of European Union Law*, Frankfurt am Main, Peter Lang, 2011, p. 63.

[1079] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), *OJ L 149/22*, 11 June 2005.

[1080] A. Renda, F. Cafaggi, J. Pelkmans, P. Iamiceli, A. Correia de Brito, F. Mustilli, L. Bebber, S. Clavel, J. Ignacio Ruiz Peris and C. Estevan, "Study on the legal framework covering business-to-business unfair trading practices in the retail supply chain – Final report*"*, DG MARKT/2012/049/E, 26 February 2014, available at https://op.europa.eu/en/publication-detail/-/publication/c82dc8c6-ec15-11e5-8a81-01aa75ed71a1/language-en, p. 64; A. de Streel, "Online Intermediation Platforms and Fairness: An assessment of the recent Commission Proposal", September 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248723, p. 16.

[1081] See point 97.

from against several large actors. Despite this difference, it was nevertheless decided to use the word "empowerment" in both situations in this thesis, as both types of "empowerment" initiatives aim to reinstate some form of *control* for weaker actors (individuals in the first case, small business users in the second). However, for small business users, this is only a form of *economic control*, while, for individuals, this control relates to *all aspects of their lives*, and is thus broader than sole economic control.

In this Section, two recent regulatory initiatives will be briefly presented. These will, however, not be analysed in depth, as they do not create *compulsory* B2B data sharing, which is the focus of this thesis, but rather either call for the adoption of self-regulatory codes of conduct for the porting of non-personal data (Article 6 of the Regulation on the Free-flow of non-personal data)[1082] or merely impose transparency obligations (but no sharing obligations) in terms of the access to data from and for (small) business users of online intermediation services (Article 9 of the Platform to Business Regulation).[1083]

a) Regulation on the free-flow of non-personal data

176. The first data initiative pertaining to specific (small) business users is Article 6 ("Porting of data") of the Regulation on the free flow of non-personal data:[1084]

> "1. The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, the following aspects:
>
> (a) *best practices for facilitating the switching* of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;
>
> (b) *minimum information requirements* to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;
>
> (c) *approaches to certification schemes* that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management;

[1082] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018.
[1083] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019.
[1084] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018.

(d) *communication roadmaps* taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders" (emphasis added).

The objective of this provision is to tackle cloud service providers' lock-in practices and to empower "professional users"[1085] of these services by allowing them to switch more easily between service providers.[1086] Indeed, cloud service providers can resort to legal, contractual and technical restrictions in order to hinder or prevent users from porting their data from one service provider to another or back to their own IT systems, even after the termination of the contract.[1087] This is especially true for small business users who have very limited bargaining power – as they are often presented with a "take it or leave it" alternative –[1088], and who face very high switching costs.[1089] This has led to a lack of competition between cloud service providers, to lock-in issues, and to a serious lack of data mobility.[1090] Yet, the ability to port data without hindrance is a key factor in order to ensure the small business users' choice and to ensure effective competition in the cloud markets.[1091] Small business users should be empowered to make informed choices by comparing the cloud services offered in the market, and more specifically their terms and conditions pertaining to the porting of their data upon the termination of the contract.[1092]

177. The scope of this "porting right" is limited to non-personal data, which are residually defined as all data other than personal data[1093], either because they have never been personal data to begin with, or because they have been anonymised.[1094] The decision to opt for such a residual definition has been vividly criticised, as, in practice, it will be complex to determine precisely what constitutes personal data, and thus, by exclusion, what constitutes non-personal data.[1095] This could pose serious issues in terms of the determination of the concrete scope of this "porting right" in practice.

178. Importantly, and contrary to what was originally envisaged[1096], the Regulation falls short of establishing a compulsory portability right for non-personal data. Rather, the European

---

[1085] "A natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service for purposes related to its trade, business, craft, profession or task" (Article 3.8 of Regulation 2018/1807.

[1086] Recitals 2 and 31 of Regulation 2018/1807. See also Communication from the Commission to the European Parliament and the Council, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", Brussels, 29 May 2019, COM(2019) 250 final, p. 16-19.

[1087] Recital 5 of Regulation 2018/1807.

[1088] L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability", *EDPL*, 2020/1, p. 92; B. Lundqvist, "Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law", *Stockholm Faculty of Law Research Paper Series n° 54*, 2018, available at https://ssrn.com/abstract=3103870, p. 10.

[1089] B. Lundqvist, "Regulating Competition and Property in the Digital Economy", *op. cit.*, p. 9.

[1090] Recital 6 of Regulation 2018/1807. See also B. Lundqvist, "Regulating Competition and Property in the Digital Economy", *op. cit.*, p. 4.

[1091] Recital 29 of Regulation 2018/1807.

[1092] Recital 30 of Regulation 2018/1807.

[1093] Article 1 of Regulation 2018/1807.

[1094] See point 18.

[1095] See points 19 and 20.

[1096] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Building a European Data Economy*", Brussels, 10 January 2017, COM(2017) 9 final, p. 17-18.

legislator opted to promote the development of self-regulatory codes of conduct to address the relationship between cloud service providers and their (small) business users.[1097] These codes of conduct should enable the porting of these users' non-personal data in order to empower them to switch easier between service providers. In order to ensure a sufficient degree of representativeness of the undertakings collaborating to the creation of these codes of conduct, the European Commission had to ensure that all relevant stakeholders (including associations of SMEs and start-ups, users and cloud service providers) were involved in its creation.[1098] In practice, two codes of conduct (for the Infrastructure as a service (IaaS) and Software as a Service (SaaS) markets) have been developed by the SWIPO (Switching and Porting) industry working group.[1099] Their effects on the competitiveness of the cloud market, through the facilitation of portability they should entail, will be assessed by the European Commission before November 2022.[1100]

179. Some authors have, however, expressed some serious doubts about the efficiency of such a self-regulatory approach relying on non-binding codes of conduct that merely set best practices, and call for the introduction of compulsory sharing obligations instead.[1101] Indeed, the self-regulatory approach echoes the cloud providers' fear that B2B data sharing obligations would hamper innovation[1102], but such an approach might in fact reinforce the existing network effects to the benefit of large cloud providers, and would thus not be a workable solution to tackle the small business users' lock-in.[1103]

To a certain extent, this is probably due to the fact that, since the aim is to empower (small) business users rather than individual consumers/data subjects, the European legislator is more reluctant to hamper the cloud providers' business interests. The result of the balance between the benefits for the (small) business users and the (incentive) costs for the cloud providers thus seems to lean more towards the latter than in situations where the data holders' business interests are weighed against benefits that compulsory B2B data sharing would entail for individuals/data subjects.[1104] However, as a result, strong doubts can be casted on whether this self-regulatory approach can truly empower (small) business users. The European Commission seems to be aware of this issue, as it suggests, in its inception impact assessment on its future "Data Act", that this act "could introduce a binding obligation for cloud computing service providers to offer data and application portability (…) for free or against an additional, but modest specified maximum fee".[1105]

[1097] S. Vezzoso, "Competition Policy in Transition: Exploring Data Portability's Roles", *15th ASCOLA (Virtual) Conference*, June 2020, available at https://ssrn.com/abstract=3634736, p. 6.
[1098] Article 6.2 of Regulation 2018/1807.
[1099] See https://swipo.eu/download-section/
[1100] S. Vezzoso, "Competition Policy in Transition: Exploring Data Portability's Roles", *op. cit.*, p. 6-7.
[1101] See B. Lundqvist, "Regulating Competition and Property in the Digital Economy", *op. cit.*, p. 43-46. See also L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU", *op. cit.*, p. 90-93.
[1102] L. Somaini, "Regulating the Dynamic Concept of Non-Personal Data in the EU", *op. cit.*, p. 91.
[1103] B. Lundqvist, "Regulating Competition and Property in the Digital Economy", *op. cit.*, p. 45.
[1104] See Part II, Chapter 2, Section A.
[1105] European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 6.

b) Platform to Business Regulation

180. The second data initiative pertaining to specific (small) business users is Article 9 ("Access to data") of the Platform to Business Regulation:[1106]

> "1. Providers of online intermediation services[1107] shall include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users[1108] to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services.
>
> 2. Through the description referred to in paragraph 1, providers of online intermediation services shall adequately inform business users in particular of the following:
>
> (a) whether the provider of online intermediation services has access to personal data or other data, or both, which business users or consumers provide for the use of those services or which are generated through the provision of those services, and if so, to which categories of such data and under what conditions;
>
> (b) whether a business user has access to personal data or other data, or both, provided by that business user in connection to the business user's use of the online intermediation services concerned or generated through the provision of those services to that business user and the consumers of the business user's goods or services, and if so, to which categories of such data and under what conditions;
>
> (c) in addition to point (b), whether a business user has access to personal data or other data, or both, including in aggregated form, provided by or generated through the provision of the online intermediation services to all of the business users and consumers thereof, and if so, to which categories of such data and under what conditions; and
>
> (d) whether any data under point (a) is provided to third parties, along with, where the provision of such data to third parties is not necessary for the proper functioning of the

---

[1106] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019. See also European Commission, Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council, *OJ C 424/1*, 8 December 2020.

[1107] "Any natural or legal person which provides, or which offers to provide, online intermediation services to business users" (Article 2.3 of Regulation 2019/1150). Online intermediation services are "services which meet all of the following requirements: (a) they constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council; (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers" (Article 2.2 of Regulation 2019/1150).

[1108] "Any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession" (Article 2.1 of Regulation 2019/1150).

online intermediation services, information specifying the purpose of such data sharing, as well as possibilities for business users to opt out from that data sharing".

Article 9 of the Platform to Business Regulation thus merely imposes transparency obligations[1109], but no compulsory data sharing obligations, to the benefit of (small) business users of online intermediation services. Indeed, the online intermediation service provider must solely specify if, and to what extent:

- It has access to (personal or non-personal) data provided by the business user or consumers for the use of the service or to data generated through the use of this service (actively provided and observed data);[1110]
- The business user has access to such actively provided and observed data;[1111]
- The business user has access to (personal or non-personal) data, including in aggregated form, that has been derived, by the service provider, from the data provided by or generated through the provision of the online intermediation services to all of the business users and consumers thereof (derived data).[1112]

The providers of online intermediation services should also specify whether they offer a preferential access to this data to themselves and/or to business users that they control.[1113] In such case, they shall refer to the main economic, commercial or legal considerations for such differentiated treatment.[1114]

181. This provision addresses the fact that online intermediation services, through strong data-driven indirect network effects, play a crucial role for the success of (small) business users that resort to their services to reach consumers, but this also leads to an increased dependence of these business users, especially SMEs, on their services.[1115] As outlined by Martens:

> "Platforms are both a blessing and a curse in the data economy. They are necessary intermediaries to generate benefits from data aggregation, realize data-driven positive network externalities and thereby enable the emergence of new markets that were not feasible prior to the arrival of digital data. At the same time, exclusive control over the data allows gatekeepers to control the ecosystem and generate significant value for their

[1109] For a similar type of transparency obligation, but this time pertaining to "recommender systems", see Article 29 of the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM(2020) 825 final. Recommender system "means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed" (Article 2.o) of the Proposal).
[1110] Article 9.2.a) of Regulation 2019/1150.
[1111] Article 9.2.b) of Regulation 2019/1150.
[1112] Article 9.2.c) of Regulation 2019/1150.
[1113] Article 7.3.a) of Regulation 2019/1150. On this issue of "differentiated treatment", see Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports, p. 39-40; Expert Group for the Observatory on the Online Platform Economy, "Work stream on Differentiated Treatment: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports.
[1114] Article 7.1 of Regulation 2019/1150.
[1115] Recital 2 of Regulation 2019/1150.

intermediation services. They can impose excessive entry and access conditions, and exclusive dealing rules preventing sellers from promoting their offers outside the gatekeeper's platform".[1116]

Because of this increased dependence, these business users have extremely limited bargaining power and often cannot negotiate the access conditions to the actively provided, observed and derived data mentioned above. Yet, the ability to access and use such data could enable important value creation in the online platform economy.[1117] Accordingly, Article 9 aims at empowering (small) business users by requiring providers of online intermediation services to be transparent regarding the scope, nature and conditions of their access to, and use of, the actively provided, observed and derived data mentioned above.[1118] This information should be proportionate and "should enable business users to understand whether they can use the data to enhance value creation".[1119] This should, in turn, allow these (small) business users to make an informed decision on whether the conditions offered by this service provider are fair, or whether they should opt for the services of an alternative provider.

182. Yet, while this provision reduces the asymmetry of information between the services providers and the (small) business users[1120], it might be insufficient, on its own, to tackle the bargaining power asymmetry between the service providers and the (small) business users, and to truly empower the latter. Indeed, even if these service providers are transparent about the scope and conditions of access, this will only empower the business users, who consider these terms as unfair, if they are able to resort to alternative services. Yet, there could be situations in which these online intermediation service providers are the only viable channel through which the business users can reach the consumers (gatekeeping position)[1121], because of entry barriers and because of these providers' strong market power.[1122] In such cases, the business users will have no other choice than to accept these terms – even if they consider them to be unfair –, or to resort to competition law in order to establish the illegality of the service providers' practices (abuse of dominant position or abuse of economic dependence).[1123]

The extent to which (small) business users are truly empowered by Article 9 of the Platform to Business Regulation is thus uncertain, as there is no compulsory obligation for the providers of online intermediation services to provide access to business users to the actively provided, observed and derived data mentioned above.[1124] Yet, these providers may very well

---

[1116] B. Martens, "An economic perspective on data and platform market power", *JRC Digital Economy Working Paper 2020-09*, February 2021, available at https://www.researchgate.net/publication/349179464, p. 13.
[1117] Recital 33 of Regulation 2019/1150.
[1118] *Ibidem*.
[1119] *Ibidem*.
[1120] See point 78.
[1121] European Commission, "Questions and Answers – Establishing a fair, trusted and innovation driven ecosystem in the Online Platform Economy", 9 July 2020, available at https://ec.europa.eu/digital-single-market/en/business-business-trading-practices, p. 8.
[1122] Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", *op. cit*., p. 4.
[1123] See Part III, Chapter 1, Sections A and B.
[1124] Recital 35 of Regulation 2019/1150.

opt to protect their own business interests, by refusing to provide access to these data to business users that are already competing with them, or that could grow and compete with them in the future.[1125]

Once again, this makes it apparent that the European legislator is more reluctant to hamper the service providers' business interests in order to empower (small) business users, than in order to empower individual consumers/data subjects.[1126] This leads to stronger claims by (small) business users to implement compulsory B2B data sharing mechanisms, as they argue that they lack access to individualised data about their own business activity and consumers (actively provided and observed data), and to aggregated data that has been derived, by the service provider, from the data provided by or generated through the provision of the online intermediation services to all of the business users and consumers thereof (derived data).[1127]

In fact, these claims seem to have been heard by the European Commission, which recently adopted a proposal for a Digital Markets Act[1128], which contains the obligation for "gatekeepers" to share with their business users or with third parties authorised by them, free of charge, the data that has been provided or generated by these business users, or their end users, through their activity on the gatekeeper's core service, in an effective, high-quality, continuous and real-time manner.[1129] "Gatekeepers" should also allow their business users to continuously port such actively provided and/or observed data, in compliance with personal data protection law.[1130]

[1125] Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", *op. cit*., p. 7.
[1126] See, by analogy, point 179.
[1127] Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", *op. cit*., p. 29 and 38.
[1128] Proposal for a Digital Markets Act. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.
[1129] See Recitals 54 and 55 and Article 6.1.i) of the Proposal for a Digital Markets Act.
[1130] See Article 6.1.h) of the Proposal for a Digital Markets Act. On continuous portability for end users, see point 169.

Chapter 2. Key balancing exercises entailed by "empowerment" initiatives imposing B2B data sharing

183. Like any other data sharing initiative, *"empowerment" initiatives imposing B2B data sharing* entail balancing exercises. Firstly, the benefits that the specific individual will derive from the data sharing must be articulated with the rights and freedoms of others (the data holder and other data subjects) that it shall not adversely affect.[1131] This will be analysed in Section A, a) and b). Secondly, there is a need to consider the potential long-term and collective costs in terms of control, autonomy and self-determination that such "empowerment" initiatives could entail.[1132] This will be analysed in Section A, c). Moreover, it will be outlined that the competitive effects of such "empowerment" initiatives imposing B2B data sharing are ambiguous (Section B). On that basis, some insights on how future similar types of initiatives could be constructed will be formulated (Section C).

Section A. Balancing the benefits from these "empowerment initiatives" with their potential costs

a) Finding a balance between the benefits for the specific individual and the business interests of the data holder

184. Any "empowerment" initiative imposing B2B data sharing necessarily implies finding a balance between the benefits that this initiative will entail for the specific individual (empowerment, reduced lock-in, etc.) and the potential negative effects that this could have on the data holder's business interests. Indeed, data sharing may have an economic impact on the data holder's business strategy.[1133] As will be outlined below, this balance is internally embedded in the existing "empowerment" initiatives imposing B2B data sharing that have been described above. This is apparent from the fact that the data holders' (intellectual property and trade secret) rights should not be affected, that the scope of the data covered by the data sharing initiatives is limited, and that they can keep using (some of) the data despite the sharing.

1. The data holders' (intellectual property and trade secret) rights should not be affected

185. "Empowerment" initiatives imposing B2B data sharing, such as the GDPR's data portability right, should not affect the data holder's intellectual property rights or trade secrets.[1134] Indeed, although many of the data held by the data holders will not qualify for any type of IP protection, some of the data may meet the required thresholds of protection.[1135] As outlined above[1136], while data, as such, cannot be protected by copyright[1137], it will often be

[1131] Article 20.4 of the GDPR.
[1132] See Part I, Chapter 2, Section C, b) and Part II, Chapter 2, Section A, c).
[1133] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *German Law Journal*, 2018, Issue 19(6), p. 1375.
[1134] See Recital 63 of the GDPR.
[1135] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1377.
[1136] See points 58 to 60.

included in databases and could therefore be subject to the *sui generis* right granted, to the maker of the database, on the content of the database.[1138] Moreover, individual data can benefit from the protection granted to trade secrets if they meet the requirements defined in the Trade Secret Directive[1139].[1140] In substance, individual data (or a dataset) will be considered as a trade secret if:[1141]

- It is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- It has commercial value because it is secret; and
- It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Importantly, this Trade Secret Directive only protects the trade secret holders[1142] against the unlawful acquisition, use and disclosure of trade secrets.[1143] Thus, the protection of trade secrets is constructed as a set of defensive rights, rather than as a right *in rem* enforceable *erga omnes*. When applied to data, this means that this legislation authorises lawful data access, while reassuring trade secrets owners by granting them a series of rights in the event of illegal use of their data by third parties, equating to a protection of *de facto* possession of data rather than to a protection of the "ownership" of data.[1144] As pointed out by Drexl, this defensive perspective "can be considered as better suited to serve the purposes of the data economy, by focussing on the particular way in which a third party has in particular acquired access to the data instead of granting exclusive protection against the use of data".[1145]

186. "Empowerment" initiatives imposing B2B data sharing can thus not be used to commit unfair commercial practices or to infringe an intellectual property right.[1146] In fact, there are three areas of friction with IP/trade secrets rights as data sharing initiatives "can force disclosure of data that could otherwise be kept away from competitors and thus be preserved as an advantage in the process of competition; can prescribe sharing of data where exclusivity

---

[1137] N. Duch-Brown, B. Martens and F. Mueller-Langer, "The economics of ownership, access and trade in digital data", *Digital Economy Working Paper 2016-10*, JRC Technical Reports, 2016, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914144, p. 7.

[1138] Articles 7 to 11 of the Directive 96/9/EC. This thesis however outlined that the evolution of the European Court of Justice's case law has arguably slipped towards the protection of some individual data in the set, namely those which required a substantial investment to obtain (see points 59 and 60).

[1139] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157*, 15 June 2016.

[1140] J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975, p. 23.

[1141] Article 2.1 of Directive 2016/943.

[1142] "Any natural or legal person lawfully controlling a trade secret" (Article 2.2 of Directive 2016/943).

[1143] Article 1.1 of Directive 2016/943.

[1144] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the Communication "*Building a European data economy*", Brussels, 10 January 2017, SWD(2017) 2 final, p. 33-34.

[1145] J. Drexl, "Designing Competitive Markets for Industrial Data" - Between Propertisation and Access*", op. cit.*, p. 24.

[1146] See Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 12.

was previously promised as a reward; [and] can undermine revenue that the potential beneficiary expected from her licensing activity and thus broadly innovation incentives".[1147]

However, the potential risks that this initiative might entail for the data holder's business interests and (IP/trade secret) rights cannot, in and of itself, serve as the basis for a refusal to apply such data sharing initiatives.[1148] Indeed, taking the example of Article 20.4 of the GDPR, Drexl outlines that the mere existence of a *sui generis* database right of the data controller should not, in and of itself, constitute an obstacle to the right to data portability, as otherwise this would compromise the effectiveness of this right.[1149] Rather, a concrete analysis of the adverse effects that data sharing could entail for the data holders' IP/trade secrets rights must therefore be carried out, and some suggest that the standard should be higher than mere "interference" with these rights.[1150] In this regard, this thesis makes the argument that while the adverse effects for the data holder may be extremely small (or even inexistent) regarding data actively provided by the data subject, these effects might be bigger regarding some of the observed data that the data holder has collected. For instance, observed data about the data subjects' behaviour (what content does she consult, how long did she stay on a specific page, what link did she click on, etc.) could be considered as being highly valuable from a commercial point of view (targeted recommendations, targeted advertising, etc.).

If an adverse effect does occur, the Article 29 Working Party (today the European Data Protection Board) nevertheless argues that this should not lead to a plain and simple refusal to share, but rather that the data holder shall ensure that (a part of) the data can be transmitted in a form that does not affect these (IP/trade secret) rights.[1151] However, the Article 29 Working Party remained mute on what should be done if the form of the data cannot be adapted and this generates uncertainties that must be addressed by the European legislator.[1152]

187. In this regard, some authors suggest that the possibility to refuse sharing data covered by IP/trade secrets rights with the data subject/consumer herself should be extremely limited, while there could be more leeway for data holders to refuse the sharing with third party recipients.[1153] Indeed, in the latter case, these authors argue that "a reconciliation of the interests might particularly confine the follow-on use of ported data to [a] specific set of

---

[1147] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1378.
[1148] See Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 12.
[1149] J. Drexl, "Data Access and Control in the Era of Connected Devices", *Study on Behalf of the European Consumer Organisation (BEUC)*, 2019, available at https://www.beuc.eu/publications/beuc-x-2018 121_data_access_and_control_in_the_area_of_connected_devices.pdf, p. 84-85.
[1150] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1379.
[1151] See Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 12.
[1152] I. Graef, "Paving the Way Forward for Data Governance: a Story of Checks and Balances", *Technology and Regulation*, Special issue: Governing Data as a Resource, 2020, p. 28. See also I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1378.
[1153] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1379.

socially justifiable purposes of re-use, possibly with schemes of fair remuneration".[1154] To do so, the idea of whitelists of data recipients, as done in the Open Banking initiative through the "Open Banking Directory", could be explored.[1155] However, it must be outlined that, in that case, the goal of this list is not to protect the data holder's interests, but rather to protect the consumers by ensuring that these recipients are secure and that their services and processing activities are legitimate and lawful.

This suggestion does not seem to have been picked up, and it is therefore uncertain whether a data holder would be entitled to limit the purposes for which the data pertaining to a specific individual can be re-used by third parties, on the grounds of IP/trade secrets rights. It can also be questioned whether this would be desirable. Indeed, if given the possibility to limit the purposes of re-use by third parties, the data holder will likely limit the possibility for third parties to develop competing products on the basis of the shared data pertaining to a specific individual. However, this would run contrary to the very essence of these data sharing initiatives, which precisely aim at empowering the individuals by allowing them to share their data in order to be offered better services, and to be able to multi-home and to switch more easily between services. Such possibilities to refuse data sharing should thus be envisaged with great caution.

The uncertainty of this articulation with the (IP and trade secrets) rights of the data holder is however attenuated by the fact that the scope of the data covered by the "empowerment" initiatives imposing B2B data sharing is limited, and by the fact that the data holder can keep using (some of) the data despite the sharing.

2. Limitation of the scope of the data covered

188. The balance between the benefits for the specific individual and the business interests of the data holder is also embedded in the scope of the data covered by the main data sharing initiatives mentioned above.

Indeed, the personal data portability right of Article 20 GDPR is limited to data "provided" by the data subject[1156], namely actively provided and observed data.[1157] While there is a doubt on whether "acquired actively provided data" and "acquired observed data" could fall within the scope of this right[1158], what is certain is that "inferred data and derived data" created by the data controller on the basis of the data "provided by the data subject" are not be covered by the data portability right.[1159] Yet, these types of data will often be the most valuable for data holders. Similarly, the data retrieval right of Article 16.4 of the Digital Content Directive only applies to "any content other than personal data, which was provided or created by the

[1154] *Ibid*., p. 1359. For more detailed explanations, see p. 1380-1388.
[1155] See point 164. Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit*., p. 24 and 35.
[1156] Article 20.1 of the GPDR.
[1157] See Part II, Chapter 1, Section A, b), 2.
[1158] See point 144.
[1159] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10.

consumer when using the digital content or digital service supplied by the trader".[1160] It therefore only applies to non-personal data created or provided by the consumer (actively provided or observed), but not to inferred/derived data nor to acquired data.[1161] The scope of PSD2's data access and use rights granted in Articles 65 to 67 is, arguably, also limited to actively provided data (the identification data pertaining to the client) and observed data (the amount of funds available on the payment account and the transactions made, which are observed on the basis of the use made of this account by the client), excluding inferred/derived data.[1162] In the same vein, the access right contained in Article 20 of the Electricity Directive is limited to final customers' metering data and to their electricity consumption data.[1163] These are also observed data and not inferred/derived data.

189. It is thus clear from the above that the scope of the data covered by "empowerment" initiatives imposing B2B data sharing is limited to actively provided and observed data, and excludes inferred/derived data, in order to preserve the business interests of the data holder. Indeed, this prevents potential competitors of the data holders from benefiting from the data subject/consumer profiles in which the data holder invested heavily, as this is where the true value of their services lies, and these competitors will need to create these profiles themselves on the basis of the actively provided/observed data.[1164] This should stimulate innovation.[1165] Yet, it must be outlined that these competitors could nevertheless try to use this actively provided/observed data in order to reverse-engineer these profiles (inferred data).[1166] This would however be a time-consuming task and these competitors might actually prefer to create their own profiles. Accordingly, exempting inferred/derived data from the scope of these data sharing initiatives protects the investment and collection incentives of the data holders, and thus provides an appropriate balance between the benefits for the specific individual and the business interests of the data holder.[1167]

190. However, it must be added that providing this inferred/derived data to the individuals would empower them and would enhance their informational self-determination.[1168] This is where the existence of the data access right contained in Article 15 of the GDPR must be reminded, which now explicitly provides that the data subject has the right to receive a copy of her personal data undergoing processing.[1169] Importantly, the scope of this data access right is broader than the scope of the data sharing initiatives mentioned above, as the data subject

---

[1160] See point 155. Article 16.4 of Directive 2019/770.
[1161] Indeed, here, and contrary to Article 20 of the GDPR, the wording of Article 16.4 does not leave room for doubt on the fact that "acquired provided data" and "acquired observed data" do not fall in the scope of this article, as it explicitly refers to data provided "when using the digital content or digital service supplied by the trader", which thus excludes data provided when using a third party's content or service.
[1162] See point 161.
[1163] See point 166.
[1164] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1375.
[1165] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 9.
[1166] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1384.
[1167] OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 45.
[1168] See point 97.
[1169] Article 15.3 of the GDPR.

can receive a copy of all of the data processed by the data controller, which also includes inferred/derived data.

However, the effect of this data access right on the business interests of the data holder is limited, as it does not provide for the direct transmission of the data to a recipient. Only the data subject will receive a copy of this data. Naturally, the data subject could then be inclined to transfer the received data to a recipient, but the re-use possibilities will likely be limited by the format of such data. Indeed, Article 15.3 of the GDPR provides that the data shall be provided in a commonly used electronic form. Yet, a PDF file will probably be considered as meeting the condition of "commonly used electronic form", but it will not allow the recipient to easily extract the data contained therein. This is a major difference with the data sharing initiatives mentioned above, who precisely aim at facilitating re-use by imposing the sharing of data in structured, commonly used and machine-readable formats.[1170] The impact of the data access right on the business interests of the data holder is thus limited, as this right mainly aims at enabling data subjects to understand what it done with their data, and not at allowing the technical re-use of such data.

3. Possibility for the data holders to keep using the data despite the sharing

191. Finally, the balance between the benefits for the specific individual and the business interests of the data holder is also embedded in the possibility for the data holders to keep using the data despite the sharing. Indeed, data are a non-rivalrous resource and this allows, from a technical aspect, data holders to keep to using the data for their own business activities, even if they have to share (some of) it.[1171] Their business interests are thus preserved.

In this regard, the data sharing initiatives contained in the GDPR, in PSD2, and in the Electricity Directive do not prevent the data holder from keeping to use the (actively provided/observed data) data pertaining to a specific individual that it has to share.[1172] This is because the obligation to share does not entail a correlative obligation to erase or stop processing the data.[1173]

The situation is slightly different for the data retrieval right contained in the Digital Content Directive. This right is exercised by the consumer at the termination of the contract[1174], and the Directive provides that, when the consumer terminates the contract, the trader must refrain from using the non-personal data provided or created by the consumer.[1175] However, there are

---

[1170] See points 149 and 157.
[1171] See point 52. OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications, 2015, available at https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm, p. 179-180. See also N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age: The limits of the analysis*, London, Routledge, 2013, p. 61.
[1172] See points 150, 161 and 166.
[1173] See for example Article 20.3 of the GDPR.
[1174] Article 16.4 of Directive 2019/770.
[1175] Article 16.3 of Directive 2019/770.

exceptions to this principle, which illustrate the balance analysed here and the consideration for the data holder (trader)'s business interests.[1176]

b) Considering the other data subjects' right to personal data protection

192. Any "empowerment" initiative imposing B2B data sharing also implies to consider the "adverse effects"[1177] that this sharing could have on other data subjects' right to personal data protection. Indeed, although the compulsory B2B data sharing initiative pertains to a specific individual, the data that will be shared as a result of it will often not solely pertain to this individual. This is because this data might also contain information about other individuals. For instance, porting a picture from one social network to another is not problematic if the person requesting the transfer is alone on the picture, but this might be more problematic if other people are tagged on the picture, as their rights might be adversely affected by the transfer. According to the Article 29 Working Party, such an "adverse effect" would occur if the sharing would prevent these other data subjects "from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.)".[1178]

Solving this issue is one of the core challenges of "empowerment" initiatives imposing B2B data sharing, and it is often pointed out as one of the key obstacles to their wider use.[1179] Naturally, the importance of this issue will be particularly exacerbated in social media and communication services markets where the value of data is, to some extent, determined by the social interactions between data subjects.[1180] Indeed, in those cases, what is valuable is not so much the content of a post or of a message sent by a specific individual, but rather with whom it was shared or to whom is was sent, as this allows to paint the individual's "social graph".[1181] On the other hand, this will be less of a problem in markets where the data only concerns a specific individual and where interactions with others are not so important (for example music and video streaming preferences and habits).[1182]

193. If the data covered by the "empowerment" initiatives imposing B2B data sharing also contains data about other data subjects, sharing this data with the individual or with recipients

---

[1176] Even after the termination of the contract, the trader can continue to use data that has no utility outside the context of the content or service supplied by the trader; that only relates to the consumer's activity when using the content or service; that has been aggregated with other data by the trader and cannot be disaggregated or can only be disaggregated with disproportionate effort; or that has been generated jointly by the consumer and other persons who continue to use the content or service (Article 16.3 of Directive 2019/770).

[1177] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11. See also Article 20.4 of the GDPR: "The right [to data portability] shall not *adversely affect* the rights and freedoms of others" (emphasis added).

[1178] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11.

[1179] See for example E. Egan, "Data Portability and Privacy", *Facebook White Paper*, September 2019, available at https://iapp.org/media/pdf/fb_whitepaper_sep_2019.pdf; S. Martinelli, "Sharing data and privacy in the platform economy: the right to data portability and "porting rights"", *Regulating New Technologies in Uncertain Times*, L. Reins (ed.), The Hague, T.M.C. Asser Press, 2019, p. 133-152.

[1180] OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 45. See also G. Nicholas and M. Weinberg, "Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?", 2019, available at https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition, p. 3.

[1181] See G. Nicholas and M. Weinberg, "Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?", *op. cit.*, p. 12.

[1182] OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 45.

creates tensions with two fundamental principles of the GDPR, namely the purpose limitation[1183] and data minimisation[1184] principles.[1185] Accordingly, these two principles have to be considered when implementing "empowerment" initiatives imposing B2B data sharing, in order to determine whether the other data subjects' rights might be "adversely affected" by the transfer.

According to the purpose limitation principle, personal data can only be processed for specified, explicit and legitimate purposes, and cannot be further processed in a manner that is incompatible with those purposes.[1186] This means that other data subjects' personal data that have been collected for a specific purpose cannot be shared with the individual or with recipients if this further processing does not fit within this initial purpose of processing.

According to the data minimisation principle, only the adequate, relevant and necessary data for the fulfilment of the specific purpose of processing shall be processed.[1187] This implies that, in combination with the purpose limitation principle, the categories and amount of data that can be shared with the individual or with recipients should be limited to what is necessary to meet the purpose pursued by the compulsory B2B data sharing initiative. If the other data subjects' personal data is not necessary for this purpose, it shall not be transferred.

194. There is thus a necessity to articulate the benefits for the specific individual whose data is shared, with the need to avoid causing "adverse effects" for other data subjects, and this should be done prior to the sharing. Indeed, while the individual whose data is shared has given her consent to the transfer, this is not the case for the other data subjects whose data could be intertwined with this individual's data. Therefore, this transfer can only take place if the purpose for which the transfer is made is compatible with the data holders' initial purpose of processing.[1188] If the transfer is deemed to be "incompatible" with the initial purpose for which the data has been collected, it can only be carried out if the other data subjects consented to it or if this transfer is necessary to comply with a legal obligation.[1189] While collecting the consents from all of these other data subjects might be infeasible in practice, the data holder could probably argue that the act of sharing is necessary to comply with a legal obligation, *in casu* the *"empowerment" initiatives imposing B2B data sharing* (for example Article 20 of the GDPR, Articles 65 to 67 of PSD2 or Article 20 of the Electricity Directive).

[1183] Article 5.1.b) of the GDPR.
[1184] Article 5.1.c) of the GDPR.
[1185] See I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper DP 2019-005*, November 2019, available at https://ssrn.com/abstract=2956308, p. 25-26.
[1186] Article 5.1.b) of the GDPR.
[1187] Article 5.1.c) of the GDPR.
[1188] Article 5.1.b) of the GDPR.
[1189] Article 6.4 of the GDPR. See also C. de Terwangne, "Article 5. Principles relating to processing of personal data", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 316; W. Kotschy, "Article 6. Lawfulness of processing", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 343; F. Gaullier, "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *Communication commerce électronique*, 2018/4, p. 51.

However, this is not sufficient in itself, as, according to the principle of separate justification, which provides that "each transaction in data requires a legal basis at two levels: the level of the supplier of the data and the level of the recipient"[1190], the recipient of the other data subjects' personal data also needs a lawful basis for the further processing of this data. In the context of "empowerment" initiatives imposing B2B data sharing, this recipient could be either the individual at the origin of the sharing (Article 20.1 of the GDPR) or a recipient with which the individual wants to share the data (Article 20.2 of the GDPR, PSD2 or the Electricity Directive). In the first case, the individual will actually likely process the other data subjects' data for purely personal or household activities, and will thus not have to apply the GDPR.[1191] In the second case, the recipient will need its own specific lawful basis for the processing of the other data subjects' personal data.[1192] In practice, the recipient will rely either on these other data subjects' consent or on "legitimate interests".[1193]

Indeed, the recipient could attempt to argue that processing these other data subjects' personal data is necessary for the purposes of the legitimate interests pursued by the individual at the origin of the sharing, namely "individual empowerment".[1194] Indeed, Article 6.1.f) of the GDPR provides that a personal data processing is lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller *or by a third party*" (emphasis added). In this case, it could be argued that the individual at the origin of the sharing is such a *third party*.

To take an example, an individual uses the compulsory B2B data sharing mechanism contained in PSD2 in order to share some of its payment account information (for example the list of the transactions she has made) with a provider of an account information service (the recipient), in order to be empowered to better manage her finances. The data at hand (the list of transactions) will necessarily contain personal data about other data subjects, who were at the other end of some of these transactions. In that case, the recipient could argue that the processing of these other data subjects' personal data is necessary for the purposes of the legitimate interests (i.e. the empowerment goal) pursued by the individual at the origin of the sharing.

However, such a processing will only be lawful if these legitimate interests of the individual at the origin of the sharing are not overridden by the interests or fundamental rights and freedoms of the other data subjects.[1195] A case-by case assessment of the "adverse effects" on these other individuals will thus have to be conducted. Coming back to the example mentioned above, the rights and freedoms of the other data subjects appearing on the individual's bank transactions are unlikely to be adversely affected by the sharing of the bank

---

[1190] C. Wendehorst, "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 334-337.
[1191] Article 2.2.c) of the GDPR.
[1192] C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit.*, p. 334-337.
[1193] Article 6.1.f) of the GDPR. See Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11.
[1194] See point 183.
[1195] Article 6.1.f) of the GDPR.

account information with the provider of an account information service.[1196] In such case, the other data subjects' rights should not be an obstacle to the compulsory B2B data sharing mechanism, as the balance between the interests of the individual at the origin of the sharing and the interests of the other data subjects weigh in favour of the former, as the latter are not "adversely affected" by the sharing. These potential "adverse effects" should indeed be the key criteria to have in mind when considering this balance.

195. In order to avoid these "adverse effects", the Article 29 Working Party (today the European Data Protection Board) suggests that the processing of these other data subjects' personal data should be authorised only insofar as these data remain under the sole control of the individual at the origin of the sharing, and that they should only be processed for the purposes determined by this individual.[1197] In this perspective, if the data is shared with a recipient, this recipient could therefore not process the other data subjects' personal data for purposes that have not been defined by the individual at the origin of the data sharing, such as marketing purposes.[1198] Moreover, the Article 29 Working Party invites both the data holder and the recipient to implement technical tools allowing the individual to select the personal data she wishes to share, while excluding, where possible, the personal data of other data subjects.[1199] This would make it possible to avoid, upstream, any "adverse effect" on the rights of these other data subjects. Yet, it is not unimaginable that some of these other data subjects' personal data may pass through this filter or might necessarily have to be shared. Alternatively, the Article 29 Working Party also invites to reflect on the implementation of consent mechanisms for these other data subjects, in order to facilitate the empowerment initiative imposing B2B data sharing.[1200]

196. Naturally, identifying lawful bases for the processing of these other data subjects' personal data and complying with the purpose limitation principle are only the first steps in order to avoid these "adverse effects". Like for any other processing of personal data, the recipient will also have to comply with the general principles of personal data protection.[1201] Namely, it will have to inform the other data subjects about the further processing in a fair and transparent manner.[1202] In this regard, it will notably have to inform the data subjects about the categories of personal data concerned, about the purposes of the processing for which the personal data are intended and about the period for which the personal data will be stored.[1203] Moreover, it will have to ensure that these other data subjects' rights (such as their right to object to the processing[1204]) are given their fullest effect[1205], and that it has implemented appropriate technical and organisational measures in order to ensure the security

---

[1196] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11.
[1197] *Ibid*., p. 12.
[1198] *Ibidem*.
[1199] *Ibidem*.
[1200] *Ibidem*.
[1201] For more details, see, by analogy, points 363 to 368.
[1202] Articles 5.1.a) and 12 to 14 of the GDPR.
[1203] Articles 14.1.c) and d) and 14.2.a) of the GDPR.
[1204] Article 21 of the GDPR.
[1205] Articles 13 to 22 of the GDPR.

of these other data subjects' data.[1206] Finally, it will have to document how it has complied with all of the above-mentioned principles, in light of the accountability principle.[1207]

197. In light of the above, it is suggested that the key criteria to have in mind when considering the protection of other data subjects' personal data, is the assessment of the potential "adverse effects" that the *"empowerment" initiatives imposing B2B data sharing* could have on these other data subjects. Said otherwise, the other data subjects' right to personal data protection should not be an obstacle to the compulsory B2B data sharing mechanism if they are not "adversely affected" by the sharing. This suggestion could be a way to solve the uncertainty surrounding this issue, which has, for instance, not been sufficiently considered by the European legislator when establishing the data portability right of Article 20 GDPR, and which is often pointed out as one of the key obstacles to a wider use of "empowerment" initiatives imposing B2B data sharing.[1208]

Finally, it is worth underlining that any "adverse effect" could potentially be exacerbated by the creation of a continuous portability right[1209], as it would entail continuous flows of information about other individuals, rather than merely periodic bulk transfers. This thus increases the risks of potential data breaches, abuses and frauds.[1210]

c) Finding a balance between the potential individual short-term gains of "empowerment" initiatives and their potential long-term costs and collective costs in terms of control, autonomy and self-determination

198. As it has been extensively explained above[1211], great caution will have to be exercised in the adoption of *"empowerment" initiatives imposing data sharing*, as a specific attention will have to be paid to the risks that they could entail in terms of individual's control and autonomy. In fact, if these initiatives are not strictly circumscribed, they might actually entail a severe loss of control for the individuals. This is because, due to strong asymmetries of information, there is a risk that the numerous data that the individuals are asked to divulge, in the name of "empowerment", could be further disseminated with an important number of actors, thus generating a loss of control on these data[1212], as they will often not know which data are used by whom and for which purposes.[1213] Consequently, these data could be used to influence their decision-making without their knowledge, raising serious issues in terms of

---

[1206] Article 5.1.f) and 32 of the GDPR.
[1207] Article 5.2 of the GDPR.
[1208] See for example E. Egan, "Data Portability and Privacy", *op. cit.*
[1209] See Part II, Chapter 1, Section C.
[1210] O. Borgogno and G. Colangelo, "Consumer Inertia and Competition-Sensitive Data Governance", *op. cit.*, p. 10.
[1211] This detailed explanation will not be repeated here and the interested reader is invited to consult Part I, Chapter 2, Section C, b).
[1212] A. Rouvroy, ""Of Data and Men": Fundamental Rights and Liberties in a World of Big Data", *Report for the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)*, T-PD-BUR(2015)09REV, Council of Europe, Strasbourg, 11 January 2016, p. 8; A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *Sloan Foundation Economics Research Paper No. 2580411*, 8 March 2016, available at https://ssrn.com/abstract=2580411, p. 3.
[1213] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", *Reinventing Data Protection: Proceedings of the International Conference (Brussels, 12-13 October 2007)*, Dordrecht, Springer, 2009, p. 68.

autonomy and self-determination.[1214] It is thus of paramount importance to see beyond the potential short-term gains that are promised to individuals, and to consider with great care these potential long-term costs.

199. Moreover, it is important to understand the necessary collective approach of autonomy and (informational) self-determination.[1215] Indeed, an individual's decision to share data will create negative externalities, as it also reveals information about other individuals, which potentially did not share any data themselves, as this data could be used to draw correlations about them.[1216] In light of this relational and collective nature of data[1217], it will also be fundamental to factor these potential collective costs for other individuals, in order to preserve their autonomy.

200. In order to assess these long-term and collective costs that could potentially derive from the adoption of empowerment initiatives imposing B2B data sharing, legislators could engage in a case-by-case risk assessment of the "systemic risks" that these initiatives could entail, by analogy with the proposal for a Digital Services Act (DSA) that requires very large platforms to manage systemic risks.[1218]

In this regard, legislators should first consider the economic risks that such data sharing initiatives could entail for (other) individuals. To illustrate this, one could imagine a scenario where individuals can consent to the collection and sharing of IoT sensor data from their car or from a connected watch, in order to be offered a lower price for their car or health insurance. While this might bring short-term benefits to the consenting individual, this might also create higher costs for the other individuals if the insurers increase the normal premiums in order to compensate for this price reduction. Hence, there is a risk of negative economic consequences for other individuals that must be factored.

[1214] A. Acquisti, C. Taylor and L. Wagman, "The Economics of Privacy", *op. cit.*, p. 44.

[1215] See point 101. A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 57.

[1216] D. Acemoğlu, A. Makhdoumi, A. Malekian and A. Ozdaglar, "Too much data: prices and inefficiencies in data markets", *NBER Working Paper No. 26296*, 2019, available at https://www.nber.org/system/files/working_papers/w26296/w26296.pdf, p. 3 and 36-37; J.A. Fairfield and C. Engel, "Privacy as a public good", *Duke Law Journal*, 2015, Volume 65, Issue 3, p. 385-457; M. MacCarthy, "New directions in privacy: Disclosure, unfairness and externalities", *Journal of Law and Policy for the Information Society*, 2011, Volume 6, p. 425–512.

[1217] A. Rouvroy, "*Homo juridicus* est-il soluble dans les données ?", *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 429.

[1218] See, by analogy, Articles 25 and 26 and Recital 57 of the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM(2020) 825 final. Article 26.1 of the DSA provides that: "This risk assessment (…) shall include the following systemic risks: (a) (a) the dissemination of illegal content through their services; (b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively; (c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security".

In fact, such practices could also lead to broader "surveillance capitalism" risks[1219], which will also need to be considered by legislators. Indeed, in a scenario such as the one mentioned above, the other individuals might feel like they have to consent to the use of such IoT devices and to the sharing of their data as well in order to avoid these additional costs, even if they would have preferred not to. As a result, this could not only lead to a broad dissemination with third parties of the data shared by the individual that consented to the sharing, but also to increased data sharing that does not accurately represent the individuals' privacy preferences. In turn, this would increase these surveillance capitalism risks, as individuals would become increasingly transparent, and this could lead to their economic manipulation in the future.[1220]

Indeed, it cannot be excluded that the shared data will feed into AI systems that could be detrimental to the individuals. In this regard, it is worth underlining here that the European Commission's proposal for an AI Act provides that the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness, or that exploits any of the vulnerabilities of a specific group of people due to their age or (physical or mental) disability, in order to materially distort a person's behaviour, is prohibited if this "is likely to cause that person or another person *physical or psychological harm*" (emphasis added).[1221] As emphasised, the deployment of AI techniques that could influence the behaviour of individuals, or exploit their vulnerabilities, would only be prohibited if this leads to "physical or psychological harm". Reversely, this means that AI techniques, fed with the shared data, could potentially be deployed in order to influence the economic behaviour of individuals, through subliminal manipulation or through the exploitation of vulnerabilities identified via the data sharing. For instance, if an individual shares her financial history data with a payment service provider in order to be offered better prices, there is a risk that this data could be further disseminated with advertisers. The latter could then use this data in order to materially distort the individual's behaviour in a matter that causes her to buy things that she might not need, because the advertising companies have learned from the data that this person is a reckless spender due to her young age. They could thus exploit this vulnerability and deploy subliminal techniques nudging her to buy more products. It is thus fundamental for legislators to question whether a risk of increased surveillance capitalism is an acceptable price to pay in order to gain a short-term benefit from the data sharing initiative.

Furthermore, legislators will also have to take into consideration the systemic risks that such data sharing initiatives could have on the exercise of fundamental rights by individuals, such as their possibility to take fundamental decisions about their health, their family life or their professional life. Once again, inspiration can be drawn in this regard from the proposal for an AI Act, which lists in its Annex 3 several "high-risk" AI systems. For instance, AI systems

---

[1219] See S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, New York, PublicAffairs, 2019.

[1220] A. Rouvroy and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*, p. 45-46.

[1221] Articles 5.1.a) and 5.1.b) of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21 April 2021, COM(2021) 206 final.

intended to be used to evaluate the creditworthiness of natural persons or establish their credit score are considered as "high-risk".[1222] Yet, data shared through empowerment initiatives could contribute to the elaboration of such systems. Indeed, if an individual shares her energy consumption data in order to get better energy prices, this data might be further shared with banks. In turn, this might affect the creditworthiness of this individual if she is deemed to be using much more energy than a "reasonable" person. As a result, a bank might consider that this person spends too much money on energy and will thus not have enough means to pay back a loan, or more globally that she is not careful and sensible about the management of her financial resources, and is thus not trustworthy. This could thus have an impact on this person's faculty to take fundamental decisions about her private life, if the further sharing of her data leads to her inability to buy a house as banks refuse to grant her loans.

Building on the previous example, one could imagine that the energy consumption data, as well as the banking or telecommunications data, that has been shared by the individual in order to get lower prices for these services, might be shared with creditworthiness institutions that, themselves, further share it with educational institutions or recruitment agencies. As a result, such creditworthiness data might be integrated in the AI systems that these educational institutions use in order to determine who can have access to, and register to, their institution (e.g. to ensure that the individual can pay her fees or those of her children), and/or in the AI systems that recruitment agencies use in order to select the appropriate candidate (e.g. a person having a low creditworthiness might be considered as being insufficiently reliable), which are both considered as "high-risk" AI applications.[1223] Furthermore, in such a scenario, the fact that these educational institutions or recruitment agencies do not have any creditworthiness data about a specific individual, because she has refused to share the above-mentioned data, might be used as a criterion to deny the access to the institution or to decide not to offer the job opportunity to this person. This is because these institutions / recruitment agencies might consider that there is too much uncertainty regarding this person's profile due to the lack of data, while such information is available about other applicants / candidates that have agreed to share their data, and that it would thus be "safer" to offer the opportunity to a person from the second category. This illustrates, once again, that the choice of individuals to share data can entail both long-term risks for themselves, as well as collective risks for others, in terms of the ability for individuals to take fundamental decisions about their private life (e.g. education and job opportunities). In assessing these risks, as well as the economic and capitalism surveillance risks mentioned above, particular consideration should thus be given to the potentially rapid and wide dissemination of the data shared by individuals.[1224]

201. On the basis of this risk assessment, legislators should then integrate – in the instrument creating the empowerment initiative –, reasonable, proportionate and effective measures aimed at mitigating the specific long-term and collective risks that will have been identified.[1225] An interesting example of such a mitigation measure can be found in a 2020

[1222] Annex III, point 5.b) of the Proposal for an Artificial Intelligence Act.
[1223] Annex III, points 3.a) and 4.a) of the Proposal for an Artificial Intelligence Act.
[1224] See, by analogy, Article 26.2 of the Proposal for a Digital Services Act.
[1225] See, by analogy, Article 27 and Recital 58 of the Proposal for a Digital Services Act.

modification of the Belgian legislation on insurances.[1226] Indeed, the Belgian legislator indicated that, in the context of the conclusion of a life insurance or of a health insurance contract, the refusal, by the insurance candidate, to acquire or use a connected object collecting personal data about her lifestyle or her health may not lead to a refusal to insure the candidate nor to a price increase of the insurance product.[1227] Similarly, the fact that the insurance candidate does not agree to the sharing of her personal data collected by the said connected object may not lead to a refusal to insure the candidate, to a price increase of the insurance product, nor to a reduction of the scope of the insurance coverage.[1228] Hence, such mitigation measures should address the economic risks mentioned above. Moreover, these mitigation measures should also address the capitalism surveillance and fundamental rights risks mentioned above, for example by providing that the data that has been shared by an individual with a service provider, in order to be offered a better price, cannot be further shared with third parties, in order to avoid the loss of control on the data that could lead to the undesirable effects for individuals presented in the previous paragraphs.

202. Finally, the empowerment initiative should also provide that external and independent audits can be conducted in order to verify the compliance with these mitigation measures.[1229] To understand why this is important, it can be reverted to the Belgian insurance law mentioned above, as these provisions might be circumvented. Indeed, if instead of raising the insurance price for those who do not want to share data (the prohibited practice), the "normal" price is raised for everyone, and a "price reduction" is given to those who share data, the economic effect will, in fact, be the same than if a higher price was charged to those who do not consent to the collection/sharing of their data, as people will pay more if they do not want to share data, and are thus incentivised to share it. Accordingly, including in the empowerment initiative the possibility to conduct external and independent audits that could reveal such practices is fundamental, as it will reduce the risk of circumvention of the mitigation measures adopted by the legislator. Similarly, these audits could reveal practices where the data is further shared with third parties, while this is expressly prohibited by the empowerment initiative.

[1226] Loi du 10 décembre 2020 modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir dans le domaine de l'assurance maladie et de l'assurance individuelle sur la vie une restriction de traitement des données à caractère personnel concernant le mode de vie ou la santé issues des objets connectés, *M.B.*, 15 janvier 2021.
[1227] Articles 46/1 and 46/2 of the Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014.
[1228] Articles 46/3 of the Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014.
[1229] See, by analogy, Article 28 and Recitals 60 to 61 of the Proposal for a Digital Services Act.

Section B. The ambiguous competitive effects of "empowerment" initiatives imposing B2B data sharing

203. While "empowerment" initiatives imposing B2B data sharing primarily aim at empowering the individual whose data is shared, such initiatives should also arguably stimulate competition and innovation by third parties.[1230] This is even an explicit objective of some empowerment initiatives that precisely aim at tackling specific market failures deriving from a lack of competition.[1231] Indeed, they should, in theory, have indirect competition-enhancing effects, as they would stimulate competition and innovation by third parties in order to offer complementary services that compete with those offered by the incumbent data holders, or to offer services on secondary markets.[1232] They should arguably lower individual's switching costs[1233], which in turn should facilitate market entry by making it easier for new players to collect the necessary (actively provided and observed) data to jump-start their service.[1234] Moreover, they should arguably allow third parties to "overcome network effects which cause markets to tip".[1235]

204. Yet, whether the theoretical findings outlined above will be translated in practice "will also depend on whether consumers actually make use of [these initiatives], and whether data is actually imported by other services".[1236] Indeed, due to the fact that, in order to ensure a balance with the data holders' business interests, the scope of these initiatives should be limited to actively provided and observed data and should exclude inferred/derived data[1237], there is a risk that the shared data would provide too little context or would be too closely tied to the incumbent data holder's service design, which might, in turn, make it complex for the recipient to build new products/services that directly compete with the incumbent's.[1238] As outlined by Nicholas and Weinberg, "trying to use exported user data to reproduce Facebook would be like trying to use furniture to reproduce the office building it came from".[1239]

[1230] S. Vezzoso, "Competition Policy in Transition: Exploring Data Portability's Roles", *15th ASCOLA (Virtual) Conference*, June 2020, available at https://ssrn.com/abstract=3634736, p. 9 and 11.
[1231] See Part II, Chapter 1, Section B.
[1232] S. Vezzoso, "Competition Policy in Transition", *op. cit.*, p. 9 and 11; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 13.
[1233] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 56.
[1234] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1359. For more detailed explanations, see p. 1386.
[1235] J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel, p. 57; S. Vezzoso, "Competition Policy in Transition: Exploring Data Portability's Roles", *op. cit.*, p. 21; G. Nicholas and M. Weinberg, "Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?", *op. cit.*, p. 1.
[1236] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 57. See also L. Somaini, "The right to data portability and user control: ambitions and limitations", *MediaLaws – Rivista dir. media*, 2018/3, p. 189.
[1237] See Part II, Chapter 2, Section A, a), 2.
[1238] G. Nicholas and M. Weinberg, "Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?", *op. cit.*, p. 2 and 6.
[1239] *Ibid*., p. 2.

Rather, these initiatives may better serve the development of complementary services on secondary markets.[1240]

Moreover, third parties might be hesitant to build products/services relying on the continuous porting of data through an incumbent's API[1241] out of fear that the incumbent might "monitor how competitors use their APIs and potentially use that information to copy them, (…) limit or cut off API access to competitors as they see fit, [or] change the data or the structure of the data they make available, creating technical overhead or even destroying the business model for competitors".[1242]

205. Furthermore, the *ratione personae* scope of the "empowerment" initiatives imposing B2B data sharing could, in fact, potentially generate anti-competitive effects. Indeed, if, similarly to Article 20 of the GDPR, they are applied symmetrically to all data holders, irrespective of their size or of the scale of their processing activities, this might in fact benefit large data holders, who could better sink the compliance costs than smaller players that would be disproportionally burdened.[1243] This could negatively affect competition and consequently harm consumers[1244] if these initiatives are overly burdensome for emerging SMEs.[1245]

Additionally, there is a risk that this might further reinforce the strong market position of large data holders, if individuals mostly use them to share data from smaller competitors towards the incumbent, rather than the other way around.[1246] Indeed, this "may strengthen economies of scope in data aggregation when a major market player manages to leverage portability rights to collect data from smaller and fragmented service providers and aggregate them in a larger data pool that generates efficiencies in service production compared to the original holders of fragmented datasets. In such cases data aggregation may lead to increased market concentration and efficiency losses because of reduced competition".[1247] This might also increase large data holders' network effects.[1248]

[1240] G. Nicholas, "Taking It With You: Platform Barriers to Entry and the Limits of Data Portability", 6 March 2020, available at https://ssrn.com/abstract=3550870, p. 16.
[1241] See Part II, Chapter 1, Section C.
[1242] G. Nicholas and M. Weinberg, "Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?", *op. cit.*, p. 8; G. Nicholas, "Taking It With You: Platform Barriers to Entry and the Limits of Data Portability", *op. cit.*, p. 16.
[1243] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1359. For more detailed explanations, see p. 1386. See also L. Somaini, "The right to data portability and user control", *op. cit.*, p. 181.
[1244] OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 43. See also D. Lyons, "GDPR: Privacy as Europe's tariff by other means?", 3 July 2018, available at https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/; P. Swire and Y. Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique", *Maryland Law Review*, 2013, Vol. 72/3, p. 335-380.
[1245] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 11.
[1246] *Ibid*., p. 13.
[1247] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 9.
[1248] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 60.

206. Despite this, it could nevertheless still be argued that these "empowerment" initiatives imposing B2B data sharing would likely mainly benefit smaller competitors than larger data holders, as the marginal benefits that will be derived from the collection of additional data will likely be higher for the former (who currently have limited data and could thereby gain access to a substantially larger amount of it) than for the latter (who already have troves of data and might only get little more data out of these initiatives). Moreover, these large data holders often have many consumer facing products/services and can thus easily collect (actively provided and observed) data from individuals without relying on these initiatives, while smaller competitors struggle to collect (actively provided and observed) data from individuals and are deeply in need of such compulsory B2B data sharing initiatives to expand their databases in order to improve their services and to be able to compete with the large data holders.

207. In light of the above, it can be concluded that the competitive effects of "empowerment" initiatives imposing B2B data sharing are ambiguous. Accordingly, any potential initiative of this kind will have to be carefully tailored and will have to take these considerations into account. Moreover, this finding sheds light on the fact that "empowerment" initiatives imposing B2B data sharing are therefore probably not the right tool to address market failures linked to data. Rather, other types of data sharing initiatives should be favoured if the main goal is to promote competition, namely economic initiatives imposing B2B data sharing, to which this thesis will turn in Part III.

Section C. Insights on how potential future "empowerment" initiative imposing B2B data sharing should be constructed

208. In Chapter 1, this thesis has presented the existing "empowerment" initiatives imposing B2B data sharing.[1249] It was also outlined that, because these initiatives present some effectiveness issues (for instance, Article 20 of the GDPR fails to impose direct portability as[1250] and, according to some authors, falls short of requiring continuous portability[1251]), there have been calls for the creation of new "empowerment" initiatives imposing B2B data sharing, for instance a "continuous portability" right.[1252] Other than imposing continuous portability, these initiatives could also go a step further in creating the obligation for the data holder to enable direct portability towards the data recipient, at the request of the data subjects, whether in new sectors (other than the banking or the electricity sector), or horizontally across sectors.

In this perspective, the aim of this Section is to draw insights on how such potential future *"empowerment" initiatives imposing B2B data sharing* should be constructed, in light of the balancing exercises presented in Section A and of the ambiguous competitive effects of such initiatives outlined in Section B. These insights pertain to the *rationae materiae* (types of data covered) and *ratione personae* (symmetric or asymmetric) scope of the initiative (a), to remuneration considerations (b), and to the potential requirement for data recipients to be certified/accredited (c). Finally, it will be outlined that (continuous) data sharing will not always, in and of itself, be sufficient to empower the individuals to switch services, and that, for some types of services, it will be needed to go further, towards more interoperability (d).

a) Scope of the regulatory initiative

1. *Ratione materiae*: types of data covered?

209. A first key element to consider is the determination of the types of data that should be covered by an *"empowerment" initiative imposing B2B data sharing*. As outlined above[1253], the *ratione materiae* scope of such an initiative should be limited to actively provided and observed data, and should exclude inferred/derived data.[1254] Indeed, as inferred/derived data will often be the most valuable for the data holder[1255], this would strike a good balance between safeguarding the data holders' economic interests and the objective of "individual empowerment" which underlies the adoption of such an initiative. Nevertheless, it must be

---

[1249] See Part II, Chapter 1, Sections A and B.
[1250] Article 20.2 of the GDPR only provides that the data subject has the right to have the personal data transmitted directly from one controller to another *where technically feasible* (emphasis added).
[1251] See Part II, Chapter 1, Section A, c), 3. This thesis however argues that Article 20.2 of the GDPR could be read as enabling a data subject to request a continuous flow of the data, pertaining to her, between the data holder and a data recipient "where technically feasible".
[1252] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 20; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*
[1253] See Part II, Chapter 2, Section A, a), 2.
[1254] See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability: Towards a Governance Framework*", CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/, p. 10 and 62-63. See also, in this sense, Recitals 54 and 55 and Article 6.1.i) of the Proposal for a Digital Markets Act. See point 182.
[1255] See point 189.

reminded that inferred/derived data can be obtained by the data subject through her data access right, although in a different format.[1256]

Moreover, it should be made explicit that data holders have the possibility to keep using the data despite the data sharing obligation.[1257] Indeed, due to data's non-rivalrous nature, this allows the data holders and the data recipients to use the data at the same time.[1258] This, in turn, also preserves the data holder's business interests, while empowering individuals.

210. So far as possible, the *ratione materiae* scope of such an initiative should also be limited to the data pertaining to the specific individual making the sharing request, and it should only enable an individual to share her data to the extent that this does not "adversarily affect" other data subjects' right to personal data.[1259] This thus requires to limit the "adverse effects"[1260] that this sharing could have on other data subjects' right to personal data protection. Such an "adverse effect" would notably occur if the sharing would prevent these other data subjects from exercising their data subject rights (right of information, access, erasure, opposition, etc.).[1261] In this regard, it must be underlined that the continuous flows of data that might result from the creation of a continuous portability right could potentially intensify the risk of the materialisation of such "adverse effects".

2. *Ratione personae*: symmetric or asymmetric regulatory initiative?

211. A second key element to consider is the determination of the *ratione personae* scope of the *"empowerment" initiatives imposing B2B data sharing*, i.e. the determination of the data holders that should be mandated to share data. In this regard, it should be reminded that the competitive effects of such initiatives are ambiguous.[1262] Indeed, they could potentially generate anti-competitive effects if they were to apply symmetrically to all data holders, irrespective of their size or of the scale of their processing activities, as small players could be disproportionally burdened.[1263]

Accordingly, some authors have argued that such initiatives should not apply symmetrically and indistinctively to all data holders processing this individual's data, and that their scope should thus be less extensive than the scope of the GDPR.[1264] In this regard, some argue that it should only apply to large data holders benefitting from strong market power[1265], while others call for an exemption of SMEs which only have a limited market share and/or turnover, in

---

[1256] See point 190. Article 15.3 of the GDPR.
[1257] See point 191.
[1258] See point 52. OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, *op. cit.*, p. 179-180. See also N. Elkin-Koren and E. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age: The limits of the analysis*, London, Routledge, 2013, p. 61.
[1259] See Part II, Chapter 2, Section A, b).
[1260] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11. See also Article 20.4 of the GDPR: "The right [to data portability] shall not *adversely affect* the rights and freedoms of others" (emphasis added).
[1261] Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 11.
[1262] See Part II, Chapter 2, Section B.
[1263] See point 205.
[1264] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 10 and 56.
[1265] See B. Engels, "Data portability among online platforms", *Internet Policy Review*, 2016, Vol. 5, Issue 2, available at https://policyreview.info/articles/analysis/data-portability-among-online-platforms.

order to avoid overburdening them.[1266] In this perspective, the Open Banking model should be preferred to the GDPR/Electricity Directive model, as the former only creates a B2B data sharing obligation on a specific set of actors (i.e. the nine major UK banks)[1267], while the latter implies B2B data sharing obligations for all data controllers/electricity providers, independently of their size, market share or turnover.[1268]

212. Yet, it would arguably make sense to impose them symmetrically, so the individual can have more control on all of her data, and not just on the data that is held by a limited amount of data holders. Such initiatives should facilitate the individual's ability to switch towards the product/service of an alternative energy provider (gas, electricity, water), bank, insurer, etc. that better matches her needs and preferences, independently of the size or market power of her current service provider. Indeed, even if, for instance, the individual currently uses the services of a smaller energy provider, she should also, from an individual empowerment perspective, be able to (continuously) share her consumption data with a third-party intermediary, which could thereby monitor her consumption and could actively suggest to her to switch towards the product/service of an alternative provider that better matches her needs and preferences.

A clear balance will thus have to be struck between maximising the individuals' empowerment and avoiding the potentially anti-competitive effects mentioned above when determining the *ratione personae* scope of such initiatives (symmetric applications to all data holders or asymmetric application to a limited amount of data holders). When assessing this balance, it is nevertheless important to keep in mind that the core objective of such initiatives is to empower the individuals whose data is shared, and more weight should thus arguably be given to this objective than to competition considerations. Indeed, this thesis argues that other types of data sharing initiatives should be considered if the main goal is to promote competition, namely *economic initiatives imposing B2B data sharing*, as will be apparent from the analysis in Part III of this thesis.

b) Remuneration considerations

213. The third key element to consider is whether the data holder should be compensated for the compulsory sharing. Indeed, data sharing creates (incentive) costs for the data holder.[1269] The question is thus whether the data holder should be remunerated in order to preserve these incentives.

As the aim of *"empowerment" initiatives imposing B2B data sharing* is to empower individuals, it could be argued that such initiatives should not entail any cost for the individuals, at least in principle, as otherwise this could deter them from invoking them. Such an approach would be consistent with most of the existent "empowerment" initiatives imposing B2B data sharing. Indeed, the data holder may not request any payment from the

[1266] See A. Diker Vanberg and M. Ünver, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", *European Journal of Law and Technology*, 2017, Vol. 8, Issue 1, p. 1-22; OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 43.
[1267] See Part II, Chapter 1, Section B, b).
[1268] See Part II, Chapter 1, Section A and Section B, c).
[1269] See Part I, Chapter 2, Section B, c), 5.

data subject exercising her GDPR right to data portability, unless the request is manifestly unfounded or excessive.[1270] Similarly, the Digital Content Directive's data retrieval right also provides that the consumer shall be entitled to retrieve the data free of charge[1271], and PSD2's data access and use rights do not provide for any type of fee for the data holder either.[1272]

214. Yet, as outlined above[1273], any *"empowerment" initiative imposing B2B data sharing*, must consider the (intellectual property and trade secret) rights that a data holder might have on the data, and a balance must thus be found between the benefits for the specific individual and the business interests of the data holder. Accordingly, some authors suggest that while the individual should be able to share her data at no cost, the data holders should be entitled to require a fair remuneration from third party recipients to which the data would be directly transferred, if this data is covered by IP/trade secrets rights.[1274] In this regard, it is interesting to point out that the Electricity Directive makes such a distinction.[1275] While it provides that final customers should be able to retrieve their metering and consumption data or to transmit them to an "eligible party" at no additional cost[1276], these "eligible parties" (i.e. the data recipients), on the other hand, can be charged a fee for the direct access to the data.[1277]

215. At first sight, this distinction is appealing, as it seems to preserve both the interests of the individual whose data is shared (as she is empowered to share her data by not being charged for the sharing) and of the data holder (who can charge a fee to the data recipient in case of direct transfer). Yet, two caveats must be expressed here.

First, if the data recipient is charged for this access and if the product/service that it offers to the individual whose data is shared implies the payment of a monetary price (utility provider, bank, insurer, etc.), then this recipient will more than likely pass-on the cost of this access to the individual, in the price of its product/services. Therefore, in such situations, the sharing will, in fact, entail an indirect cost for the individual, and it can be questioned whether this is a desirable outcome. Indeed, as the aim of such initiatives is to empower individuals, it could be argued that they should not entail any cost for them, even an indirect one, as otherwise this could deter them from relying on such initiatives.

Second, if the data recipient can be charged by the data holder, there is a risk that the data holder might set a high price in order to deter the recipients from building alternative services on the basis of the shared data. In turn, this might prevent such initiatives from truly empowering the individuals, as they might be provided with less switching opportunities than in a situation where recipients are not charged for this access.

[1270] Article 12.5 of the GDPR. See point 148.
[1271] Article 16.4 of Directive 2019/770. See point 156.
[1272] Articles 65 to 67 of the Directive 2015/2366. See points 161 and 162. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 78.
[1273] See Part II, Chapter 2, Section A, a), 1.
[1274] I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1359. For more detailed explanations, see p. 1379-1388.
[1275] See point 166.
[1276] Article 20 and 23.5, al. 1 of the Directive 2019/944.
[1277] Article 23.5, al. 2 of Directive 2019/944.

One way to limit these caveats would be to limit the fee that can be required by the data holder from the data recipient. For instance, the Electricity Directive provides that the charges for access for "eligible parties" (i.e. the data recipients), should be "reasonable and duly justified".[1278] This could indeed preserve the recipients' incentives to develop alternatives by limiting their cost of data access and this would also avoid that high costs are passed-on to the individual whose data is shared. Yet, this would generate a lot of uncertainties on what constitutes a "reasonable and justified" cost of access. This uncertainty could slow down the apparition of alternative services for the individuals, due to endless disputes between the data holders and the data recipients regarding the "reasonable and justified" cost of access. Therefore, even "reasonable and justified" fees might hamper the empowerment objective of such initiatives.

216. Finally, it is important to outline that some authors support, on the contrary, the idea that "empowerment" initiatives imposing B2B data sharing should not imply any form of payment, even from the data recipient.[1279] This is because these initiatives mainly pursue individual empowerment objectives and because the potential costs that this might entail on the data holders' incentives to collect and process the data will, in fact, be minimal as the volumes of data that will be transferred through such mechanisms are quite low.[1280] Indeed, they only entail the sharing of data pertaining to one specific individual, and not the sharing of aggregated data pertaining to multiple individuals, which, on the other hand, should imply some form of remuneration for the data holder, as it is more likely to affect its business interests.[1281]

217. In light of all of the above, there is a strong argument to be made that "empowerment" initiatives imposing B2B data sharing, such as a continuous portability right, should not imply any form of payment, neither from the individual whose data is shared, nor from a potential data recipient.

c) Potential certification of data recipients?

218. The fourth key element to consider is whether the individuals should be able to (continuously) share their data with any data recipient whatsoever (the GDPR data portability right model), or whether they should only be able to (continuously) share their data with data recipients that have obtained a "certification" for the re-use (the Open Banking model).

Indeed, as outlined above[1282], one of the factors that contributed to the Open Banking initiative's success is that recipients have to obtain an authorisation from the Financial Conduct Authority (FCA) in order to get access to the banks' data.[1283] The goal is to protect the consumers by ensuring that these entities are secure and that their services and processing activities are legitimate and lawful. Similarly, the Smart Data initiative seems to support the

[1278] Article 23.5, al. 3 of Directive 2019/944.
[1279] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 10 and 79-80. See also, in this sense, Recitals 54 and 55 and Article 6.1.i) of the Proposal for a Digital Markets Act. See point 182.
[1280] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 80.
[1281] *Ibid*., p. 11 and 77-79. See Part III, Chapter 3, Section B, b), 4.
[1282] See point 164.
[1283] Open Data Institute and Fingleton, "Open Banking, Preparing for lift off", *op. cit.*, p. 25.

requirement, for data recipients, to obtain an accreditation if they want to access "high risk" data – i.e. "data where the consequences of loss or misuse are likely to be greatest" –, in order to ensure that their services are legitimate, secure and comply with the personal data protection requirements.[1284]

There is thus a case to be made for the inclusion of such a certification/accreditation scheme in potential "empowerment" initiatives imposing B2B data sharing, as this would protect the individuals' interests. Moreover, this would generate more trust from the individuals' whose data is shared, which is fundamental as, absent this trust, these individuals would probably not make use of these initiatives.[1285] While such certification/accreditation procedure will necessarily entail some administrative red-tape in order to verify that the recipients present the guarantees mentioned above, this burden should be reduced as much as possible, as otherwise this could deter the recipients from building alternative services on the basis of the shared data. In turn, this would likely prevent these initiatives from truly empowering the individuals, as they would be provided with less switching opportunities if this certification/accreditation procedure is too cumbersome.

In this regard, it is interesting to point out that, in the context of the Smart Data initiative, it is suggested that the accreditation process should be cross-sectoral, in order to avoid unnecessary burdens and duplicative procedures for recipients acting across several sectors.[1286] Following the advocates of this initiative, such an accreditation system would be appropriate and proportionate as "this would provide reassurance to consumers that [recipients] seeking access to personal data have been vetted, while also simplifying the process for [recipients] that operate across markets".[1287]

Moreover, it should be outlined that, in the context of its proposal for a Data Governance Act, the European Commission reflected on whether a voluntary or compulsory certification/labelling mechanism should be created for trusted data intermediaries.[1288] The advantage of compulsory certification over voluntary certification is that it would generate more trust in the data sharing process, but the downside is that it could have a prohibitive costs on SMEs and start-ups and could thus have a negative effect on their willingness and ability to provide such services.[1289] Interestingly, in order to address this balance, the

---

[1284] HM Government, "Smart Data: Putting consumers in control of their data and enabling innovation", June 2019, available at https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation, p. 28. See also European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 March 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_fr, p. 34.

[1285] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 59-60.

[1286] HM Government, "Smart Data: Putting consumers in control of their data and enabling innovation", *op. cit.*, p. 29.

[1287] *Ibidem*.

[1288] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final, p. 5. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*, p. 25-27, 38-42, 46 and 52-53.

[1289] Proposal for a Data Governance Act, p. 5.

Commission eventually proposed an intermediary solution, consisting of a "notification obligation with *ex post* monitoring of compliance with the requirements to exercise the activities by the competent authorities of the Member States[1290]".[1291]

219. Such an intermediary solution could also be proposed in the context of *"empowerment" initiatives imposing B2B data sharing*, where, in order to be entitled to receive the data, the recipient would be required to notify a description of the product/service that it intends to provide to competent authorities to be appointed in each Member State.[1292] These national authorities would then be competent to assess, *ex post*, the trustworthiness of the recipients and whether they offer sufficient guarantees in terms of privacy and security (in collaboration with the data protection authorities[1293]).[1294] Moreover, such initiatives could impose harmonised requirements/obligations on the recipients for the provision of their products/services, in order to ensure their trustworthiness, to be monitored *ex post* by these competent authorities.[1295] In order to avoid an unnecessary multiplication of regulatory authorities, this thesis suggests that these regulatory authorities should be the same as the ones created in the context of the Data Governance Act in order to monitor trusted data intermediaries.

While such a "notification obligation with *ex post* monitoring of the compliance" could be perceived, by the data recipients, as being too cumbersome and as delaying the benefits of the data sharing, it is certainly less burdensome than requiring a prior certification for the re-use. On the other hand, the option not to subject the re-use to any prior formality should arguably be excluded, as it is vital to ensure that the data is not shared openly with anyone without any limits, as this could have dramatic consequences in terms of the individuals' personal data protection and informational self-determination.[1296] Moreover, as what is required from the data receiver is a simple notification, and not a request for a prior authorisation, these notification forms could be standardised in order to streamline and simplify the process. Then, it would be up to the data recipient to document appropriately the use that it makes of the data, as well as the steps that it has taken to comply with the above-mentioned harmonised requirements/obligations, in order to be able to demonstrate this *ex post* to the relevant regulatory authorities, by analogy with the "accountability" principle contained in Article 5.2 of the GDPR.

Following this logic, if the regulatory authorities receive a complaint (from an individual, the data holder or a third party) regarding the fact that a data recipient has provided false information in its notification or that it has breached the requirements/obligations contained in

---

[1290] The alternative of the creation, at the European level, of a new independent structure with legal personality (similar to the European Data Protection Board) was also suggested, but this was abandoned due to the high costs and the issues of political feasibility that it implied (Proposal for a Data Governance Act, p. 6). See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*, p. 28-29, 40, 43 and 52-53.
[1291] Proposal for a Data Governance Act, p. 6.
[1292] See, by analogy, Article 10.6.f) of the Proposal for a Data Governance Act.
[1293] See, by analogy, Recitals 28 and 29 and Article 12.3 of the Proposal for a Data Governance Act.
[1294] See, by analogy, Article 13 of the Proposal for a Data Governance Act. See also point 408.
[1295] See, by analogy, Recitals 22 to 34 and Articles 9 to 14 of the Proposal for a Data Governance Act.
[1296] See Part II, Chapter 2, Section A, c).

the data sharing initiative, these authorities should be able to request, *ex post*, further information to the data recipient in order to verify this, and should also be able to audit its systems. This could notably lead to sanctions ranging from fines, for minor breaches, to the imposition of the deletion of the data that has been received (or of the interruption of the API access to the data holder's data), for the most serious breaches. To be sure, this could give rise to quite "interventionistic" practices by these authorities, and data recipients might be required to divulge more information about their business model than they would want to, but this is arguably the necessary price to pay in order to generate trust in the data sharing, by both the individuals' whose data are shared and the data holders. Furthermore, this is also arguably a necessary price to pay to make sure that the data is not shared openly with anyone without any limits, as that would amount to opening Pandora's box and is thus not a viable solution.

220. Finally, it should be added that, in the same perspective of limiting/controlling the potential recipients, some authors have suggested that, in order to preserve the data holders' business interests, they should be able to "confine the follow-on use of ported data to [a] specific set of socially justifiable purposes of re-use".[1297] However, it would arguably be undesirable to enable the data holder to limit the data re-use purposes, as this could potentially limit the alternatives offered to individuals, and thus their empowerment. Great caution should thus be applied before creating such limitations.

d) Beyond (continuous) data sharing: (full protocol) interoperability

221. Finally, it should be outlined that an "empowerment" initiative imposing (continuous) B2B data sharing will not always, in and of itself, be sufficient to empower the individuals to switch services. Indeed, while this may be sufficient for services that mainly rely on the individual's own profile and preferences, and where interactions with others are not so important (e.g. utility, banking, insurance or music and video streaming services), this will not be the case for social media and communication services where the ability to interact with other individuals is key. This is because such services are characterised by network effects, which create a coordination problem as their value will directly or indirectly depend on the number of other individuals that also use them.[1298]

Yet, while (continuous) data sharing might reduce individual's switching costs, it does not remedy the lock-in effects deriving from network effects' coordination problem.[1299] Taking the example of social media, even if an individual has the possibility to request the continuous sharing of her data with another social media, she will only be willing to do so if a sufficient number of other individuals (friends, family, colleagues...) also switch at the same time.[1300] In this regard, Nicholas suggests the implementation of "functional group portability", which

---

[1297] See point 187. I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *op. cit.*, p. 1359. For more detailed explanations, see p. 1380-1388.

[1298] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 58.

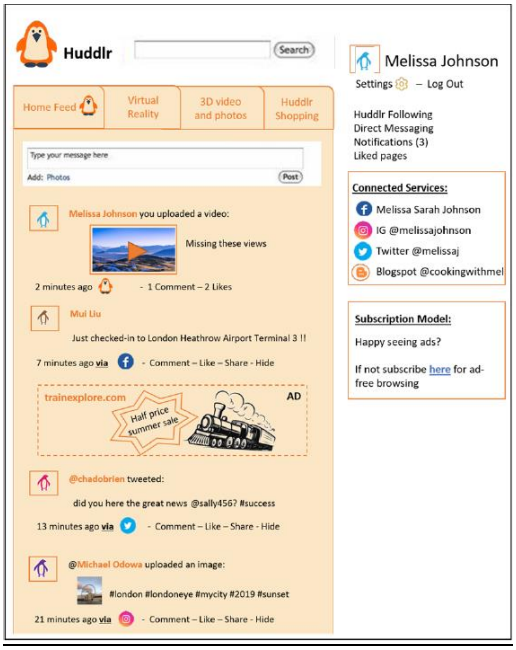
[1299] *Ibidem*. See also G. Nicholas, "Taking It With You: Platform Barriers to Entry and the Limits of Data Portability", 6 March 2020, available at https://ssrn.com/abstract=3550870, p. 3.

[1300] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 58.

would allow groups of individuals to coordinate in order to switch, all at once, towards a new service provider.[1301]

Accordingly, several authors have outlined that there is a necessity to move beyond (continuous) data sharing, towards more interoperability, in order to tackle these network effects and to truly empower the individuals to switch services.[1302] More precisely, this would require "full protocol interoperability", which implies that "services interoperate to a degree where ultimately users can interact seamlessly albeit being on different networks – like users of different telecom networks can communicate with each other. Then users can switch to a new provider without losing access to the network effect exerted by users who remain with the old provider".[1303] This is also sometimes qualified as "content interoperability".[1304] To give an example, such interoperability would enable a former Facebook user, which decided to switch to a new social network, to continue to view her former Facebook friends' posts and to discuss with them. Figure 10 provides a visual representation of what this could look like.

Figure 10: Visual representation of "full protocol interoperability" / "content interoperability"



Source: CMA, Final report on online platforms and digital advertising, Figure 8.1[1305]

[1301] G. Nicholas, "Taking It With You: Platform Barriers to Entry and the Limits of Data Portability", *op. cit.*
[1302] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 58-60 and 83-85; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 58. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*, p. 21.
[1303] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 58. See also, OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 45; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 85.
[1304] See Competition and Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, p. 372-374.
[1305] *Ibid.*, p. 373.

However, such "full protocol interoperability" might entail risks of barriers to innovation, as the various service providers will be constrained by the technical standards selected to implement it.[1306] Moreover, there is the potential risk of being locked in inefficient standards.[1307] Therefore, this requirement for "full protocol interoperability" should only be considered for service markets where the ability to interact with other individuals is key, as, for those types of services, the benefits of interoperability (the benefits of network effects are shared among competitors and this increases competition in the market) are likely to outweigh its costs (reduced innovation due to strong standardisation, which could in turn weaken or even eliminate competition).[1308]

In this regard, it is worth pointing out that the European Commission indicated that it would explore, in the context of its future "Data Act" proposal, the possibility to define essential requirements enabling interoperability, notably through the increased use of standardised smart contracts.[1309] Moreover, the European Commission's proposal for a Digital Markets Act[1310] includes obligations for "gatekeepers" to enable some form of interoperability.[1311] Indeed, according to Article 6.1.c) of the proposal, gatekeepers shall "allow the installation and effective use of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the core platform services of that gatekeeper. [This should not prevent these gatekeepers] from taking proportionate measures to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper"; while Article 6.1.f) provides that they shall also "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services". It is however, important to underline that this Article 6.1.f) is limited to "ancillary services", namely services provided in the context of, or together with, core platform services, such as payment, fulfilment, identification or advertising services.[1312] Accordingly, third parties could not rely on this provision in order to develop a directly competing service, e.g. another social network where it would still be possible for users to interact with their "friends" on Facebook, as illustrated on Figure 10 above.

* * *

[1306] See J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 58; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 59.
[1307] OECD, *Consumer Data Rights and Competition*, *op. cit.*, p. 46.
[1308] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 59-60; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 58.
[1309] European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 6.
[1310] Proposal for a Digital Markets Act. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.
[1311] See Articles 6.1.c) and 6.1.f) of the Proposal for a Digital Markets Act.
[1312] Article 2.14 of the Proposal for a Digital Markets Act.

222. To conclude this Section, the above-mentioned insights regarding the key elements that *"empowerment" initiatives imposing B2B data sharing* should consider are summarised in Table 1.

Table 1: Insights on the key elements to consider for "empowerment" initiatives imposing B2B data sharing

	"Empowerment" initiatives imposing B2B data sharing
Data holders subject to the sharing obligation	Symmetric application to all data holders.[1313]
Data recipients entitled to benefit from the sharing obligation	Recipient could be required to notify a description of the product/service that it intends to provide.[1314] *Ex post* assessment of the trustworthiness of the recipients and of whether they offer sufficient guarantees in terms of privacy and security.[1315] Imposition of harmonised obligations on the recipients for the provision of their products/services, to be monitored *ex post* as well.[1316]
Types of data covered by the sharing obligation	Only actively provided and observed data (not acquired, nor inferred/derived data).[1317] However, inferred/derived data can be obtained through the exercise of the GDPR data access right.[1318] So far as possible, only the data of the specific individual making the sharing request, and to the extent that this does not "adversarily affect" other data subjects' right to personal data.[1319]
Remuneration of the data holder as compensation for the sharing obligation	Should, in principle, not imply any form of payment, neither from the individual whose data is shared, nor from a potential data recipient.[1320]
Technical implementation of the sharing obligation	Depending on the cases, it could be necessary to move beyond (continuous) data sharing, towards more interoperability, in order to truly empower the individuals to switch services.[1321]

[1313] See Part II, Chapter 2, Section C, a), 2.
[1314] See Part II, Chapter 2, Section C, c).
[1315] See point 218.
[1316] See point 218.
[1317] See Part II, Chapter 2, Section C, a), 1.
[1318] See point 190. Article 15 of the GDPR.
[1319] See Part II, Chapter 2, Section C, a), 1.
[1320] See Part II, Chapter 2, Section C, b).
[1321] See Part II, Chapter 2, Section C, d).

Part III. Economic or societal initiatives imposing B2B data sharing

223. While Part II of the thesis focussed on *"empowerment" initiatives imposing B2B data sharing*, **Part III of the thesis** will be devoted to *economic or societal initiatives imposing B2B data sharing*. These two types of initiatives are grouped together in this Part, as their focus is not set on the individuals, but rather on broader economic or societal considerations that go beyond individual interests. Therefore, and contrary to the empowerment initiatives presented in Part II, these economic or societal initiatives will not lead to the sharing of small quantities of data linked to a specific individual, but rather to the sharing of larger amounts of (aggregated) personal data pertaining to multiple individuals and/or non-personal data.

Most of the analysis conducted in this Part III will be dedicated to economic initiatives imposing B2B data sharing, which aim to remedy market failures deriving from a lack of data sharing (concentrated data markets, high entry barriers and lack of contestability…).[1322] Indeed, a small number of large firms currently hold a significant part of the world's data, and this might diminish the incentives of smaller data-driven firms to emerge, grow and innovate, due to high entry barriers.[1323] The high degree of market power deriving from this "data advantage" could also affect the contestability of some markets.[1324] Similarly, some platforms have acquired significant scale, effectively allowing them to act as "private gatekeepers", which might endanger the fairness and openness of the markets.[1325] Accordingly, compulsory data sharing could be imposed to ensure the contestability of data markets and to level the competitive playing field, by proving competitors with a sufficient amount of data to address the "cold start problem".[1326]

At present, these market failures are mainly tackled through competition law, with the exception of a sector-specific data sharing legislation in the automotive sector[1327].[1328] This

---

[1322] On these market failures see Part I, Chapter 2, Section B, c), 3. "Data market failures". Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", 19 February 2020, COM(2020) 66, p. 3, 5, 8 and 14. See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Shaping Europe's digital future*", Brussels, 19 February 2020, COM(2020) 67, p. 8.

[1323] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 3.

[1324] *Ibid*., p. 8.

[1325] Communication from the Commission, "*Shaping Europe's digital future*", *op. cit.*, p. 8.

[1326] To be able to offer a quality service, a firm needs a certain amount of data. To collect this data, it needs to attract customers, but the customers will not use its service if the quality is insufficient. Hence the cold start problem, because if the firm does not have enough data to start with, it will be unable to reach a minimal level of quality and will be unable to attract customers. This is also sometimes referred to as the "chicken and egg problem". See, *inter alia*, V. Fast, D. Schnurr and M. Wohlfarth, "Data-Driven Market Power: An Overview of Economic Benefits and Competitive Advantages from Big Data Use", July 2019, available at https://ssrn.com/abstract=3427087, p. 10; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *CERRE Report*, 2020, available at https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy, p. 64.

[1327] Regulation (EU) 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, *OJ L 171/1*, 29 June 2007, articles 6 and 7; Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L 151/1*, 14 June 2018. See articles 61 to 66, 86 and annexes X and XI.

strong reliance on competition law is explained by the fact that a balance must be found between the benefits and costs of sharing.[1329] In this regard, **Chapter 1** will analyse whether the existing competition law balances pertaining to refusals to share a resource are equally suitable for data, or whether the results of these balancing exercises need to be rethought in light of data's characteristics. Then, **Chapter 2** will shed light on the articulation between competition and data protection law, and will emphasise two core issues that emerge at the intersection of these two fields of law. Finally, **Chapter 3** will move beyond competition law, and will discuss the creation of potential *ex ante* legislations imposing B2B data sharing for economic purposes.

224. While most of the discussions, in the policy and legislative circles, pertaining to compulsory B2B data sharing revolve around economic objectives, compulsory B2B data sharing initiatives could also pursue societal objectives (tackling environmental challenges, contributing to healthier and more sustainable societies, improving mobility, etc).[1330] For instance, data sharing between navigation technology service providers and freight and logistics businesses can assist the latter in their transition towards more sustainable, efficient and secure transport services.[1331] However, the reflections around the creation of societal initiatives imposing B2B data sharing are still in their infancy. Accordingly, they will be addressed in a shorter prospective **Chapter 4**, which will not aim for exhaustivity on this growingly important topic, but will rather have as main objective to launch avenues of exploration on why such initiatives could be envisaged and on how they could be constructed in the future.

[1328] See Part III, Chapter 3, Section A, a).

[1329] P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *Antitrust Law Journal*, 2008, n° 75, p. 616-620. See Part I, Chapter 2, Section B, c), 5. "Need for a balance between the benefits and costs of data sharing".

[1330] See Part I, Chapter 2, Section C, a). See Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 942.

[1331] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 28. See also https://www.aisin.com/en/product/mobility/cs-s/. For other examples, see point 93.

Chapter 1. Balancing exercises in competition law: incentivising innovation *versus* maximising social welfare through large dissemination

225. The category of B2B data sharing initiatives analysed in this Part III mostly focus on economic objectives, and are mainly tackled through competition law. The goal of competition law is to protect consumer welfare by ensuring that competition is not distorted by practices that harm consumers directly, or by practices that are indirectly detrimental to them as they impact the effective structure of competition.[1332] Its goal is thus not to protect competitors, but rather competition in order to ensure that consumers are provided with sufficient choices, notably in terms of price and quality. While digital innovations have entailed profound revolutions in some industries and have given birth to the digital economy, the goals of competition law are still very much relevant and do not need to be changed. However, this digital revolution might require an adaptation of the theories of harm justifying competition law intervention.[1333]

Indeed, the competition law balances applied to "brick and mortar" industries might not be appropriate to address competitive issues in the digital economy. This is because data have different characteristics than "traditional resources".[1334] Indeed, as outlined above, data can be characterised as an "infrastructural resource", as they are non-rivalrous, capital and general-purpose goods.[1335] Due to data's characteristics, the digital economy is characterised by network effects and by strong economies of scale, scope and speed.[1336] Data therefore plays a prominent role, as being able to use data to develop or improve innovative products or services is a key competitive parameter.[1337] Conversely, these characteristics might create entry barriers, which will make it very difficult to contest the position of incumbent data holders relying on "data advantages".[1338] Consequently, data concentration and data conglomeration market failures might appear.[1339] To remedy these market failures,

---

[1332] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era – Final report", 2019, available at http://ec.europa.eu/competition/publications/reports/ kd0419345enn.pdf, p. 40. See also Protocol (No 27) on the internal market and competition annexed to the Treaty on the Functioning of the European Union, *OJ C 115/309*, 9 May 2008.

[1333] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 40-41.

[1334] See Part I, Chapter 2, Section B, a).

[1335] See point 52. B. Frischmann, *Infrastructure: The Social Value of Shared Resources*, Oxford, Oxford University Press, 2012, cited in OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications, 2015, available at https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm, p. 179-182.

[1336] See Part I, Chapter 2, Section B, c), 1. "Data collection and production incentives". See M. Stucke and A. Grunes, *Big Data and Competition Policy*, Oxford, Oxford University Press, 2016; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 339-381.

[1337] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 19-24.

[1338] See Part I, Chapter 2, Section B, c), 2. "Entry barriers to data markets". See M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 339-381.

[1339] See Part I, Chapter 2, Section B, c), 3. "Data market failures". For a broader analysis of all of the potential types of data market failures, see M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability: case studies and data access remedies", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing: an economic and legal analysis", *EU Science Hub*, 2020,

competition intervention imposing B2B data sharing[1340] is increasingly considered in numerous policy reports across the globe.[1341] On the contrary, because they primarily aim at empowering individuals, the "empowerment" initiatives imposing B2B data sharing, analysed in Part II, cannot solve these market failures.[1342] Finally, it is important to keep in mind that while they can generate competitive benefits, compulsory B2B data sharing remedies entail incentives costs in terms of data collection and processing for both the data holder and the recipients.[1343]

226. Accordingly, from an economic perspective, a balance must be found between the benefits and costs of data sharing, taking into consideration the incentives of the various

---

available at https://ssrn.com/abstract=3658100; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *CERRE Report*, March 2019, available at http://www.crid.be/pdf/public/8377.pdf; B. Martens, "An economic perspective on data and platform market power", *JRC Digital Economy Working Paper 2020-09*, February 2021, available at https://www.researchgate.net/publication/349179464.

[1340] Importantly, compulsory B2B data sharing is not the only available remedy to tackle these market failures and other options are suggested in the legal doctrine (see point 86). However, as this thesis focusses on compulsory B2B data sharing, these alternatives will not be further detailed here.

[1341] See Part I, Chapter 2, Section B, c), 4. "Benefits from sharing". See (EU) J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*; (Germany) H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *Report by the Commission "Competition Law 4.0" for the German Federal Ministry for Economic Affairs and Energy*, 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competitionframework.pdf? blob=publicationFile&v=2; (Germany) H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, Baden-Baden, Nomos, 2018 (also available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtigeunternehmen.html (an executive summary in English is available at https://ssrn.com/abstract=3250742)); (France) Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf; (BeNeLux) J. Steenbergen, M. Snoep and P. Barthelmé, "Joint memorandum of the Belgian, Dutch and Luxembourg competition authorities on challenges faced by competition authorities in a digital world", 2 October 2019, available at https://www.belgiancompetition.be/en/about-us/publications/joint-memorandum-belgian-dutch-and-luxembourg-competition-authorities; (UK) J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel; (UK) UK Competition & Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study; (USA) Stigler Committee on Digital Platforms, "Final Report*"*, September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report; (Australia) Australian Competition and Consumer Commission, "Digital Platforms Inquiry – Final Report", 26 July 2019, available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report. For a comparative analysis of some of these reports, see W. Kerber, "Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia", September 2019, available at https://ssrn.com/abstract=3469624; and S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", 31 March 2020, available at https://ssrn.com/abstract=3565491.

[1342] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf, p. 8-9.

[1343] See Part I, Chapter 2, Section B, c), 5. "Need for a balance between the benefits and costs of data sharing". B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.

parties.[1344] Said otherwise, a balance must be found between incentivising innovation (data collection and processing by data holders) and maximising social welfare through large dissemination (data sharing). Therefore, this Chapter will question whether the existing competition law balances pertaining to refusals to share a resource – namely abuses of dominant position (i.e. the essential facilities doctrine) (Section A); abuses of economic dependence (Section B); and input foreclosure in vertical integration (Section C) – remain suitable in light of data's characteristics, or whether they must be adapted for data markets. This question is important because sharing data may potentially entail more benefits and less (incentive) costs than sharing other resources.[1345]

In fact, this fits in a broader discussion pertaining to the adaptation of competition law to the digital environment. Indeed, the European Commission indicated that it is important for competition rules to remain fit for an increasingly digital world, and that this requires to assess the effectiveness of the current rules, and to potentially review them where necessary.[1346]

As the determination of the concrete data sharing remedy to be imposed implies overarching considerations that are equally relevant for the three types of competition law infringements mentioned above, these will be addressed in a specific separate section (Section D).

Finally, the issue of the time-consuming process of competition intervention will be discussed, as, in digital markets where quick reactions are indispensable, the length of the competitive process serves as a key rationale for complementing competition law intervention with *ex ante* legislations imposing B2B data sharing (Section E).

[1344] P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *op. cit.*, p. 616-620. See Part I, Chapter 2, Section B, c), 5. "Need for a balance between the benefits and costs of data sharing".

[1345] See point 90. See M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 31; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", Report for the German Federal Ministry for Economic Affairs and Energy*, 29 August 2018, available at https://ssrn.com/abstract=3250742, p. 10. See also J. Prüfer and C. Schottmüller, "Competing with Big Data", *TILEC Discussion Paper No. 2017-006 and CentER Discussion Paper No. 2017-007*, February 2017, available at https://pure.uvt.nl/ws/portalfiles/portal/15514029/2017_007.pdf.

[1346] Communication from the Commission, "*Shaping Europe's digital future*", *op. cit.*, p. 8.

Section A. Abuse of dominant position: Essential facilities doctrine

227. As data plays a prominent role in the digital economy, timely access to data may turn out to be essential for a firm's competitiveness.[1347] Accordingly, in order to ensure that the competitive advantage of large data holders remains contestable, it might be necessary to safeguard access by competitors to some of their data, in order to (re)create a form of competitive pressure.[1348] This will especially be the case if a large data holder benefits from a dominant position on a specific data market.

A dominant position refers to "a position of economic strength enjoyed by an undertaking, which enables it to prevent effective competition being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers".[1349] This requires the identification of the relevant product market, which comprises "all those products and/or services which are regarded as interchangeable or substitutable by the consumer, by reason of the products' characteristics, their prices and their intended use".[1350] It also requires identifying the relevant geographic market, which comprises "the area in which the undertakings concerned are involved in the supply and demand of products or services, in which the conditions of competition are sufficiently homogeneous and which can be distinguished from neighbouring areas because the conditions of competition are appreciably different in those area".[1351] Combined, these constitute the relevant market.[1352]

228. To preserve its dominant position on a relevant data market, a large data holder may refuse to share (some of) its data with its (potential) competitors, and this raises the question of whether this could amount to an abuse of a dominant position, prohibited by Article 102 of the Treaty on the functioning of the European Union[1353] (hereafter "TFEU").[1354] More specifically, this raises the question of whether refusals to share a resource (or "refusals to deal") can constitute such an abuse. In the European Union, these refusals to deal have been tackled by European Court of Justice, and are traditionally referred to as the "essential

---

[1347] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 73.

[1348] German Federal Ministry for Economic Affairs and Energy, "A New Competition Framework for the Digital Economy: Report by the Commission "Competition Law 4.0" – Executive Summary", 9 September 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competition-framework.pdf?__blob=publicationFile&v=2, p. 1. The full report, in German, is available at https://www.wettbewerbsrecht-40.de/KW40/Redaktion/DE/Downloads/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=3.

[1349] ECJ, *United Brands Company and United Brands Continentaal BV v. Commission*, 14 February 1978, C-27/76, EU:C:1978:22, §65.

[1350] Commission Notice on the definition of relevant market for the purposes of Community competition law, OJ C 372/5, 9 December 1997, § 7. This Notice is currently under review: see https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12325-Evaluation-of-the-Commission-Notice-on-market-definition-in-EU-competition-law.

[1351] *Ibid*., § 8.

[1352] *Ibid*., § 9.

[1353] Treaty on the functioning of the European Union, *OJ C 326/47*, 26 October 2012.

[1354] J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975, p. 44.

facilities doctrine" case law.[1355] This doctrine has been imported from the United States, where it finds its roots in the Supreme Court's *Terminal Railroad* case[1356].[1357] As this thesis focusses on the balancing exercises underlying compulsory B2B data sharing, it will outline the "traditional" balance reached by the essential facilities doctrine in the European Union (a) and will assess whether the result of this balancing exercise needs to be adapted for data markets (b).

a) The "traditional" essential facilities doctrine balance

229. The first relevant case to mention in the context of the essential facilities doctrine, where the European Court of Justice had to address a refusal to deal, is *Commercial Solvents*.[1358] Commercial Solvent was a company manufacturing and selling nitropropane and aminobutanol, which are both necessary for the manufacture of ethambutol that is used in anti-tuberculosis drugs.[1359] For several years, Commercial Solvents sold aminobutanol to Zoya, which used it for the manufacture of ethambutol-based products, but then stopped this supply after having developed its own ethambutol-based products.[1360] Following a complaint by Zoya, the European Court of Justice ruled that "an undertaking which has a dominant position in the market in raw materials and which, with the object of reserving such raw material for manufacturing its own derivatives, refuses to supply a customer, which is itself a manufacturer of these derivatives, and therefore risks eliminating all competition on the part of this customer, is abusing its dominant position".[1361]

230. The second relevant case to mention is *Volvo v. Veng*.[1362] In that case, Volvo, which was the owner of a registered design in respect of body panels for motor vehicles, refused to grant a licence for the import and sale of such panels to Veng, despite the fact that the latter was willing to pay a reasonable royalty.[1363] When asked whether this could amount to an abuse of dominant position, the European Court of Justice outlined that a refusal to grant such a licence could not, in itself, constitute an abuse of dominant position, as otherwise Volvo would be deprived of the substance of its exclusive right on the design.[1364] However, the Court underlined that such a refusal to licence could be subject to a competition law intervention if it involved, on the part of the dominant undertaking, an abusive conduct, such as "the

---

[1355] ECJ, *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18; ECJ, *AB Volvo v Erik Veng (UK) Ltd*, 5 October 1988, C-238/87, EU:C:1988:477; ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98; ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569; ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257; CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289.
[1356] Supreme Court of the United States, *United States v Terminal Railroad Association of St. Louis*, 1912, 224 US 383. See also Supreme Court of the United States, *Verizon Communications v Law Offices of Curtis V. Trinko*, 2004, *LLP*, 540 US 398.
[1357] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *RJTUM*, 2019, Vol. 53, p. 39.
[1358] ECJ, *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18.
[1359] *Ibid*., "I. Statement of the facts".
[1360] *Ibidem*.
[1361] *Ibid*., § 25.
[1362] ECJ, *AB Volvo v Erik Veng (UK) Ltd*, 5 October 1988, C-238/87, EU:C:1988:477.
[1363] *Ibid*., §§ 1 and 4.
[1364] *Ibid*., § 8.

arbitrary refusal to supply spare parts to independent repairers, the fixing of prices for spare parts at an unfair level or a decision no longer to produce spare parts for a particular model even though many cars of that model are still in circulation, provided that such conduct is liable to affect trade between Member States".[1365] Yet, the Court considered that, in the case at hand, there was no such abusive conduct and Volvo was thus entitled to refuse to grant a licence to Veng.[1366]

231. The third relevant case to mention is *Magill*.[1367] In this case, three television stations, namely RTE, ITV and the BBC, which each had their own television guide covering exclusively their own programmes, refused to licence these programme listings to Magill, which aimed at publishing a comprehensive weekly television guide that would combine these different listings.[1368] When asked whether this could amount to an abuse of dominant position by the television stations, that were each deemed to have a monopoly on their programme listings[1369], the European Court of Justice repeated that the refusal by a dominant undertaking to grant a licence cannot in itself constitute an abuse of a dominant position.[1370] However, the Court outlined that, in "exceptional circumstances", the exercise of such an exclusive right could involve an abusive conduct.[1371] In the case at hand, the Court considered that such "exceptional circumstances" were met due to the combination of three elements:

- The dominant undertakings' refusal to provide their programme listings to Magill prevented the appearance of a new product, *in casu* a comprehensive weekly guide for television programmes, that they did not offer and for which there was a potential consumer demand;[1372]
- By denying the access to information that was indispensable in order to compile such a comprehensive weekly guide, the dominant undertakings reserved to themselves the secondary market for comprehensive weekly guides by excluding all competition on that market;[1373] and
- There was no justification for this refusal.[1374]

[1365] *Ibid*., § 9.
[1366] *Ibid*., § 10.
[1367] ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98. For comments of this decision, see, inter alia, T. Vinje, "The final word on Magill: the judgement of the E.C.J.", *E.I.P.R.*, 1995, Volume 17, Issue 6, p. 297-303; P. Crowther, "Compulsory Licensing of Intellectual Property Rights", *European Law Review*, 1995, p. 521-528; A. Robertson, "The Existence and Exercise of Copyright: Can it Bear the Abuse?", *The Law Quarterly Review*, 1995, p. 588-591; S. Taylor, "Copyright versus Right to Compete - The Judgment of the ECJ in Magill", *Computer and Telecommunications Law Review*, 1995, p. 99-102; G. Van der Wal, "Article 86 EC: The Limits of Compulsory Licensing", *European Competition Law Review*, 1994, p. 230-235; H. Calvet et T. Desurmont, "L'arrêt Magill: Une decision d'espèce?", *R.I.D.A.*, 1996, n° 167, p. 3-67.
[1368] ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98, §§ 6-10.
[1369] *Ibid*., § 47.
[1370] *Ibid*., § 49.
[1371] *Ibid*., § 50.
[1372] *Ibid*., § 54.
[1373] *Ibid*., §§ 53 and 56.
[1374] *Ibid*., § 55.

232. The fourth relevant case to mention is *Bronner*.[1375] In that case, Bronner, the publisher of the Austrian daily newspaper "Der Standard", wanted its newspaper to be included in Mediaprint's nationwide home-delivery scheme that it had established for its own newspapers.[1376] Following Mediaprint's refusal to do so, Bronner argued that such a refusal amounted to an abuse of dominant position, as postal delivery did not represent an equivalent alternative to home-delivery, and as, due to its small number of subscribers, it was unable, either alone or in cooperation with other publishers, to operate its own home-delivery scheme in economically reasonable conditions.[1377] Reverting to its decision in Magill, the Court held that such a refusal will only be deemed to be abusive:[1378]

- If the access to the dominant undertaking's resource/service (*in casu* the nationwide home-delivery system) is indispensable to carry a business activity on a secondary market (*in casu* the daily newspaper market), inasmuch as there is no actual or potential substitute;
- If this refusal is likely to eliminate all competition on the secondary market; and
- If it cannot be objectively justified.

In the case at hand, the Court considered that Mediaprint's nationwide home-delivery system was not indispensable. Importantly, the Court indicated that in order for the indispensability of the facility to be established, there must be technical, legal or even economic obstacles capable of making it impossible, or even unreasonably difficult, for any undertaking other than the dominant undertaking to develop an alternative to the facility, whether alone or in cooperation with others.[1379] In this regard, the Court added that it is not enough to argue that it is not economically viable for the access seeker to develop such an alternative, but rather that it is necessary to establish that it is not economically viable "for any undertaking other than the dominant undertaking" to create any alternative facility that is comparable to that of the dominant undertaking.[1380] In this perspective, the access to a facility will not be indispensable if an alternative (even a less advantageous one) can be developed by any undertaking other than the dominant undertaking.[1381] This is because Article 102 TFEU aims at preventing distortions of competition, rather than at protecting specific competitors.[1382] In reaching such a conclusion, the Court seems to have strongly relied on Advocate General Jacobs's opinion:

[1375] ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569. For comments on this decision, see, inter alia, F. Wooldridge, "The Essential Facilities Doctrine and Magill II: The Decision of the ECJ in Oscar Bronner", *Intellectual Property Quarterly*, 1999, p. 256-264; P. Treacy, "Essential Facilities - Is the Tide Turning?", *European Competition Law Review*, 1998, p. 501-505; M. Bergman, "The Bronner Case - A Turning Point for the Essential Facilities Doctrine?", *European Competition Law Review*, 2000, p. 59-63; A. Albors-Llorens, "The "Essential Facilities" Doctrine in EC Competition Law", *The Cambridge Law Journal*, 1999, p. 490-492.
[1376] ECJ, *Bronner*, 26 November 1998, C-7/97, §§ 4-7.
[1377] *Ibid*., §§ 8 and 23.
[1378] *Ibid*., § 41.
[1379] *Ibid*., § 44.
[1380] *Ibid*., §§ 45-46. See also Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 68.
[1381] ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569, § 43.
[1382] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 58.

> "[The imposition of a duty to deal] can be justified in terms of competition policy only in cases in which the dominant undertaking has a genuine stranglehold on the related market. That might be the case for example where duplication of the facility is impossible or extremely difficult owing to physical, geographical or legal constraints or is highly undesirable for reasons of public policy. It is not sufficient that the undertaking's control over a facility should give it a competitive advantage.
>
> I do not rule out the possibility that the cost of duplicating a facility might alone constitute an insuperable barrier to entry. That might be so particularly in cases in which the creation of the facility took place under non-competitive conditions, for example, partly through public funding. However, the test in my view must be an objective one: in other words, in order for refusal of access to amount to an abuse, it must be extremely difficult not merely for the undertaking demanding access but for any other undertaking to compete. Thus, if the cost of duplicating the facility alone is the barrier to entry, it must be such as to deter any prudent undertaking from entering the market. In that regard it seems to me that it will be necessary to consider all the circumstances, including the extent to which the dominant undertaking, having regard to the degree of amortisation of its investment and the cost of upkeep, must pass on investment or maintenance costs in the prices charged on the related market".[1383]

233. The fifth relevant case to mention is *IMS Health*.[1384] In this case, IMS Health refused to provide access, to its competitor NDC Health, to the "1860 bricks structure" it had developed for the presentation of German regional sales data on pharmaceutical products to pharmacies and doctors.[1385] The problem for NDC, which also offered such services, was that it could not develop an alternative brick structure for the presentation of its data and thus had no other choice than to request a licence to use IMS' structure, which was protected by a database right.[1386] This is because the users (pharmacies and doctors) were unfavourable to the use of an alternative brick structure, as the brick structure developed by IMS had become the normal industry standard.[1387] NDC therefore argued that IMS' refusal to licence its brick structure amounted to an abuse of dominant position.[1388] In line with its previous case law, the European Court of Justice held that the refusal, by a dominant undertaking, to licence an

---

[1383] *Ibid*., §§ 65-66.
[1384] ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257. For comments on this case, see, inter alia, E. Derclaye, "The IMS Health decision and the Reconciliation of Copyright and Competition", *European Law Review*, 2004, Volume 29, Issue 5, p. 687-697; H. Meinberg, "From Magill to IMS Health: the new product requirement and the diversity of intellectual property rights", *E.I.P.R.*, 2006, Volume 28, Issue 7, p. 398-403; C. Stothers, "IMS Health and its implications for Compulsory Licensing in Europe", *E.I.P.R.*, 2004, Volume 26, Issue 10, p. 467-472; B. Ong, "Anti-competitive refusals to grant Copyright Licences : reflections on the IMS Saga", *E.I.P.R.*, 2004, Volume 26, Issue 11, p. 505-514; J. Drexl, "IMS Health and Trinko - Antitrust Placebo for Consumers Instead of Sound Economics in Refusal-to-Deal Cases", *International Review of Industrial Property and Copyright Law*, 2004, p. 788-808.
[1385] ECJ, *IMS Health*, 29 April 2004, C-418/01, §§ 2-8.
[1386] *Ibid*., § 21.
[1387] *Ibid*., § 6.
[1388] *Ibid*., § 11.

indispensable resource on which it holds an IP right (*in casu* the brick structure) constitutes an abuse of dominant position if three conditions are fulfilled:[1389]

- The dominant undertakings' refusal to licence prevents the appearance of a new product or service that is not offered by this undertaking and for which there is a potential consumer demand;
- By refusing to licence its indispensable resource, the dominant undertaking reserves to itself a secondary market by excluding all competition on that market; and
- There is no objective justification for this refusal.

The Court considered that these conditions were met in this case. Interestingly, the Court provided some additional explanations about some of these conditions. Regarding the condition of indispensability, and building on the reasoning pertaining to this condition that it had developed in *Bronner*[1390], the Court outlined that the degree of participation by users in the development of IMS' standard brick structure, and the costs linked to it, had to be taken into consideration when determining whether IMS' structure was indispensable for the presentation of regional sales data on pharmaceutical products, as the users had become technically dependent on IMS' structure.[1391] Regarding the condition of the reservation of, and the exclusion of competition on, a secondary market, the Court outlined that it was sufficient to identify a potential or even hypothetical market.[1392] For the Court, "such is the case where the products or services are indispensable in order to carry on a particular business and where there is an actual demand for them on the part of undertakings which seek to carry on the business for which they are indispensable. Accordingly, it is determinative that two different stages of production may be identified and that they are interconnected, inasmuch as the upstream product is indispensable for the supply of the downstream product".[1393]

234. The sixth relevant case to mention is *Microsoft*.[1394] In that case, Sun Microsystems complained that Microsoft's refusal to provide it with the necessary information and technology to allow its work group server operating systems to interoperate with Microsoft's

---

[1389] *Ibid*., § 52.
[1390] See *supra* point 232. See ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569, §§ 43-46. See also Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 68.
[1391] ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, §§ 29-30.
[1392] *Ibid*., § 44.
[1393] *Ibid*., §§ 44-45.
[1394] CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289. For comments on this case, see, inter alia, P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *op. cit.*, p. 933-963; C. Ahlborn and D. Evans, "The Microsoft Judgment and its Implications for Competition Policy Towards Dominant Firms in Europe", *Antitrust Law Journal*, 2009, Volume 75, Issue 3, p. 887-932; I. Graef, "Tailoring the Essential Facilities Doctrine to the IT Sector: Compulsory Licensing of Intellectual Property Rights after Microsoft", *Cambridge Student Law Review*, 2011, Volume 7, Issue 1, p. 1-20; R. Moldén, "Mandatory Supply of Interoperability Information: The Microsoft Judgment", *European Business Organization Law Review*, 2008, p. 305-334; J. Langer, "The Court of First Instance's Microsoft Decision: Just an Orthodox Ruling in an On-Orthodox Case", *Legal Issues of Economic Integration*, 2008, p. 183-195; D. Howarth and K. McMahon, ""Windows has Performed an Illegal Operation": the Court of First Instance's Judgment in Microsoft v Commission", *European Competition Law Review*, 2008, p. 117-134; N. Petit, "L'arrêt Microsoft. Abus de position dominante, refus de licence et vente liée...- l'article 82 sans code source", *Journal de droit européen*, 2008, p. 8-12.

client PC operating system (i.e. Windows) constituted an abuse of dominant position.[1395] Coherently with the previous case law of the European Court of Justice, the Court of First Instance reminded that the refusal, by a dominant undertaking, to licence a product on which it holds an IP right does not, in itself, constitute an abuse of dominant position, but rather that this will only be the case in "exceptional circumstances".[1396] According to the Court, such "exceptional circumstances" are met if:[1397]

- The refusal relates to a product or service indispensable to the exercise of a particular activity on a neighbouring market;
- The refusal is of such a kind as to exclude any effective competition on that neighbouring market; and
- The refusal prevents the appearance of a new product for which there is potential consumer demand.

If such circumstances are present, the dominant undertaking's refusal will be considered as an abuse, unless it can demonstrate an objective justification for the refusal.[1398] In the case at hand, the Court found that these conditions were met and that Microsoft could not rely on an objective justification for its refusal to provide the necessary interoperability information to Sun Microsystems.

235. Importantly, it must be pointed out that, as outlined by Graef, it seems that the Court of First Instance has lowered, in *Microsoft*, the standard for the application of the conditions of the essential facilities doctrine.[1399] Firstly, regarding the indispensability requirement, the Court concluded that access to the interoperability information was indispensable in order for Sun Microsystems to be able to compete "on an equal footing".[1400] Yet, this finding is in stark contrast with the European Court of Justice's decision in *Bronner*, where it held that the access to a facility will not be indispensable if a less advantageous alternative can be developed by any undertaking other than the dominant undertaking.[1401]

Secondly, regarding the condition of the reservation of, and the exclusion of competition on, a secondary market, the Court reminded that "it is necessary to distinguish two markets, namely, a market constituted by that product or service and on which the undertaking refusing to supply holds a dominant position and a neighbouring market on which the product or service is used in the manufacture of another product or for the supply of another service", and that "the fact that the indispensable product or service is not marketed separately does not exclude from the outset the possibility of identifying a separate market".[1402] This echoes the European Court of Justice's reasoning in *IMS Health*.[1403] Yet, the Court of First Instance departed from this decision by holding that it is not necessary to demonstrate that "all

---

[1395] CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, § 7.
[1396] *Ibid*., § 331.
[1397] *Ibid*., § 332.
[1398] *Ibid*., § 333.
[1399] See I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 45-46.
[1400] CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289, § 421.
[1401] ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569, § 43.
[1402] CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289, § 335.
[1403] See *supra* point 233. ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, §§ 43-45.

competition on the market would be eliminated", but rather that it is sufficient to demonstrate that "the refusal at issue is liable to, or is likely to, eliminate all effective competition on the market".[1404] In this regard, the Court added that "the fact that the competitors of the dominant undertaking retain a marginal presence in certain niches on the market cannot suffice to substantiate the existence of such competition".[1405]

Thirdly, regarding the condition of the prevention of the appearance of a "new product", the Court of First Instance made two important adaptations. On the one hand, it noted that this condition is only found in the essential facilities case law dealing with an IP right (namely *Magill* and *IMS Health*).[1406] On the other hand, the Court significantly lowered the threshold to meet this condition, as it provided that a refusal to licence will not only constitute an abuse if this prevents the appearance of a "new product", but also if it prevents the appearance of technical developments.[1407] Once again, such a finding is in stark contrast with the previous case law of the European Court of Justice, in particular its *IMS Health* decision, where the Court held that a refusal to licence will only be abusive if "the undertaking which requested the license does not intend to limit itself essentially to duplicating the goods or services already offered on the secondary market by the owner of the intellectual property right, but intends to produce new goods or services not offered by the owner of the right and for which there is a potential consumer demand".[1408] This has led some authors to question whether the "new product" requirement should still be considered as a condition for the application of the essential facilities doctrine, as virtually anything could be framed as being a "technical development".[1409]

To conclude on this *Microsoft* case, it is fundamental to underline that the judgment of the Court of First Instance has not been appealed by Microsoft, and that, consequently, the European Court of Justice did not have the opportunity to rule on whether it agrees or not with the Court of First Instance's lowering of the standards for the application of the essential facilities doctrine.[1410] It is thus uncertain whether this lowering was a consequence of Microsoft's super-dominant position, and should thus not be translated in other cases, or whether this lowering represents an evolution that should be applied to any subsequent case.[1411]

236. Finally, it is important to mention the recent *Slovak Telekom* case.[1412] The starting point of this case is that Slovak Telekom, which is the incumbent and largest telecommunications operator and broadband provider in Slovakia, has been compelled by the Slovak telecommunications' regularity authority to grant all reasonable and justified access requests

---

[1404] CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289, § 563.
[1405] *Ibidem*.
[1406] *Ibid*., § 334.
[1407] *Ibid*., § 647.
[1408] ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, § 49.
[1409] E. Elhauge and D. Geradin, *Global Antitrust Law and Economics*, Third Edition, St. Paul, Foundation Press, 2018, p. 507-508. See also I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 46.
[1410] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 46.
[1411] *Ibidem*.
[1412] ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239.

to its local loop, as it was considered as an operator having a significant power on the wholesale market for unbundled access to the local loop.[1413] To do so, Slovak Telekom published its reference unbundling offer setting out contractual and technical conditions for the access.[1414] However, the European Commission ruled that the conditions of access set by Slovak Telekom, between 12 August 2005 and 31 December 2010, constituted an abuse of dominant position, notably because it had set unfair terms and conditions in its reference unbundling offer and because it applied unfair tariffs "which did not allow a competitor as efficient as [Slovak Telekom] relying on wholesale access to the unbundled local loops of that operator to replicate the retail broadband services offered by that operator without incurring a loss" (margin squeeze).[1415] This decision was, to a large extent, confirmed by the General Court, although it held that the Commission had failed to prove that Slovak Telekom had engaged in margin squeeze practices between 12 August 2005 and 31 December 2005.[1416]

Slovak Telekom appealed the General Court's decision, arguing that the Commission and the General Court had erred in law by considering that it was not necessary to assess the indispensability of the access to its local loop because it had a regulatory obligation to grant such access.[1417] The Court of Justice ruled that the Commission and the General Court were right to rule that different standards could be applied to outright refusals to deals, such as in the *Bronner* case[1418], than to constructive refusals to deal (imposition of unfair access conditions), such as in the present case.[1419] In substance, the Court held that the demonstration of the indispensable nature of the access to the facility in cases of outright refusals to deal was justified by the fact that forcing the dominant undertaking to provide access, by concluding a contract with a competitor, would be detrimental to its freedom of contract and to conduct a business, and to its right to property.[1420] However, it ruled that, "by contrast, where a dominant undertaking gives access to its infrastructure but makes that access, provision of services or sale of products subject to unfair conditions [constructive refusal to deal], the conditions laid down by the Court of Justice in paragraph 41 of the judgment in Bronner do not apply", and that, accordingly, "the absence of such an indispensability is not in itself decisive for the purposes of the examination of potentially abusive practices on the part of a dominant undertaking".[1421]

The Court justifies this distinction by the fact that, in the latter case, the dominant undertaking already provides the access to its infrastructure, and the competition authority would thus not have to force it to give such access.[1422] Therefore, "the measures that would be taken in such a context will thus be less detrimental to the freedom of contract of the dominant undertaking and to its right to property than forcing it to give access to its infrastructure where it has

[1413] *Ibid*., §§ 9-12.
[1414] *Ibid*., § 12.
[1415] *Ibid*., §§ 14-16. See also European Commission, *Slovak Telekom*, 15 October 2014, case AT.39523.
[1416] *Ibid*., § 20. See also GC, *Slovak Telekom v. Commission*, 13 December 2018, T-851/14, EU:T:2018:929.
[1417] *Ibid*., §§ 21-24 and 31-35.
[1418] See point 232.
[1419] ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239, §§ 38-61.
[1420] *Ibid*., § 46.
[1421] *Ibid*., § 50.
[1422] *Ibid*., § 51.

reserved that infrastructure for the needs of its own business".[1423] Said otherwise, the result of the balancing exercise between the various rights and interests at hand should be different in cases of outright refusals to deal, than in cases of constructive refusals to deal, where the data holder already provides access or is required to provide access by a regulatory obligation (as in the latter case, the legislator will have factored these rights and interests before adopting the obligation).[1424]

It should however be outlined that, according to some authors, such a distinction between outright refusals to deal, where the indispensability criterion is required, and constructive refusals to deal, such as margin squeeze[1425], self-preferencing[1426] and tying[1427] practices, where the condition of indispensability does not appear in the legal test, might be problematic in practice.[1428] For instance, knowing that the standard to find an abuse of dominance is higher for outright refusals to deal than for constructive refusals to deal, a dominant undertaking might opt not to provide access at all, rather than to provide access on restricted conditions, in order to protect its competitive position. As a result, this might potentially reduce the incentives for dominant undertakings to provide access (as they will not want to take the risk to "open the floodgates"), on the one hand, and thus reduce the access possibilities for third parties, on the other hand.

237. To summarise, according to the essential facilities doctrine case law[1429], the outright refusal by a dominant undertaking on a given market to grant access to another undertaking to a facility (a resource or an IP right) of which it is the owner (*de jure* or *de facto*), will constitute an abuse of such dominant position if the following "exceptional circumstances" are met:[1430]

- Access to the facility is indispensable to enable the undertaking requesting access to operate in a secondary market;

[1423] *Ibidem*.
[1424] *Ibid*., §§ 54-56.
[1425] See ECJ, *Konkurrensverket v TeliaSonera Sverige AB*, 17 February 2011, C-52/09, EU:C:2011:83; GC, *Slovak Telekom v. Commission*, 13 December 2018, T-851/14, EU:T:2018:929; ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239.
[1426] European Commission, *Google Search (Shopping)*, 27 June 2017, AT.39740.
[1427] European Commission, *Google Android*, 18 July 2018, AT.40099.
[1428] See, *inter alia*, P. Ibáñez Colomo, "Indispensability and Abuse of Dominance: From Commercial Solvents to Slovak Telekom and Google Shopping", 11 December 2019, available at https://ssrn.com/abstract=3502519; D. Geradin, "Refusal to Supply and Margin Squeeze: A Discussion of Why the "Telefonica Exceptions" are Wrong", *TILEC Discussion Paper No. 2011-009*, 2011, available at https://ssrn.com/abstract=1762687; H. Auf'mkolk, "The "Feedback Effect" of Applying EU Competition Law to Regulated Industries: Doctrinal Contamination in the Case of Margin Squeeze", *Journal of European Competition Law & Practice*, 2012, Vol. 3, Issue 2, p. 149-162; A. Azzopardi, "No abuse is an island: the case of margin squeeze", *European Competition Journal*, 2017, Vol. 13, Issue 2-3, p. 228-248; I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 56-63.
[1429] ECJ, *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18; ECJ, *AB Volvo v Erik Veng (UK) Ltd*, 5 October 1988, C-238/87, EU:C:1988:477; ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98; ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569; ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257; CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289.
[1430] D. Geradin, A. Layne-Farrar and N. Petit, *EU Competition Law and Economics*, Oxford, Oxford University Press, 2012, p. 256.

- By refusing the access, the dominant undertaking reserves to itself a secondary market by excluding all competition on that market;
- The refusal prevents the emergence of a new product or service, or of technological developments, which are not offered by the dominant undertaking and for which there is potential consumer demand; and
- The refusal cannot be justified by objective considerations.

A refusal to share the access to an essential facility is thus not abusive *per se*, as otherwise the dominant undertaking would be deprived of the substance of the exclusive (IP) rights it holds on the facility. It will only be so if the above-mentioned "exceptional circumstances" are met. This is because, as outlined by Advocate General Jacobs in his opinion in *Bronner*[1431], a dominant undertaking's freedom to contract also entails a freedom not to contract, and any competition intervention interfering with such a freedom requires "a careful balancing of conflicting considerations"[1432], namely a balance between the costs and the benefits of providing access to the facility presented as "essential". Indeed, as the finding of an abuse results in the imposition, on the dominant firm, of a duty to deal with another undertaking, any potential benefits deriving from this forced access to the facility has to be balanced with the "principles of freedom to contract[1433], including the right to choose one's trading partners, and freedom to dispose of one's property[1434]".[1435]

This is important because, if the possibility to impose such a duty to deal was not limited to "exceptional circumstances", this could have serious effects on the dominant undertaking's incentives to create and maintain the essential facility. Indeed, from an innovation perspective, "while a duty to deal increases short-term competition and innovation complementary to the facility of the dominant firm, it may diminish incentives for competitors as well as dominant firms to develop substitutes for the existing infrastructure in the long term".[1436] This was also highlighted by the Court of Justice in the *Slovak Telekom* case mentioned above[1437], where it held that "while, in the short term, an undertaking being held liable for having abused its dominant position due to a refusal to conclude a contract with a competitor has the consequence of encouraging competition, by contrast, in the long term, it is generally favourable to the development of competition and in the interest of consumers to allow a company to reserve for its own use the facilities that it has developed for the needs of its business. If access to a production, purchasing or distribution facility were allowed too easily, there would be no incentive for competitors to develop competing facilities. In addition, a dominant undertaking would be less inclined to invest in efficient facilities if it could be bound, at the mere request of its competitors, to share with them the benefits

[1431] ECJ, C-7/97, *Bronner*, 26 November 1998, EU:C:1998:569.
[1432] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 57.
[1433] CFI, *Bayer v Commission*, 26 October 2000, T-41/96, EU:T:2000:242, § 180.
[1434] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 56.
[1435] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 47.
[1436] *Ibidem*.
[1437] See point 236.

deriving from its own investments".[1438] In doing so, the Court confirmed the point that Advocate General Jacobs had made in his opinion on the *Bronner* case, where he indicated that the essential facilities doctrine is the result of a careful balancing between promoting short-term and long-term competition and innovation.[1439]

238. This essential facilities doctrine is also interesting to analyse in the broader perspective of the need to find a balance between competition *in* the market, which favours sustaining innovation (i.e. improvement of an existing product or service that does not affect existing markets), and competition *for* the market, which favours disruptive innovation (i.e. innovation that reshuffles existing markets and leads to the apparition of new markets).[1440] Indeed, the imposition of a duty to deal stimulates competition *in* the market, as competitors will be provided with access to the facility in order to compete on the existing market, while refraining from imposing such access stimulates competition *for* the market, as competitors are rather incentivised to develop alternative products or services that will disrupt the existing market structures from the outside.[1441] Said otherwise, in the former case, competitors are incentivised to develop a similar product/service that is better than the incumbent's, while in latter case, competitors are rather incentivised to create the "next big thing" that will displace the incumbent through the creation of a new type of product/service ("creative destruction").[1442] The latter approach to competition would arguably lead to a succession of highly-dominant (or even monopolistic) positions that would likely persist for a certain period of time, before being displaced by a new highly-dominant (or even monopolistic) undertaking in another market that would reshuffle existing markets.[1443] Examples of Facebook's displacement of MySpace and of Google's displacement of Yahoo are often cited in this regard.

Looking at the essential facilities doctrine case law, the European Court of Justice seems inclined to promote competition *in* the market, rather than competition *for* the market, through the imposition of a duty to deal when the above-mentioned "exceptional circumstances" are met. However, neither the Court nor the European Commission explained why, in such cases, static competition and sustaining innovation should be favoured over dynamic competition

---

[1438] ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239, § 47.
[1439] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 57.
[1440] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 47-51. See also J. Bower and C. Christensen, "Disruptive Technologies: Catching the Wave", *Harvard Business Review*, 1995, Volume 73, Issue 1, p. 43-53; C. Christensen, *The Innovator's Dilemma. When New Technologies Cause Great Firms to Fail*, Boston, Harvard Business School Press, 1997; C. Christensen and M. Raynor, *The Innovator's Solution: Creating and Sustaining Successful Growth*, Boston, Harvard Business School Press, 2003; A. de Streel and P. Larouche, "Disruptive innovation and competition policy enforcement", *OECD Working Paper DAF/COMP/GF(2015)7*, 2015, available at https://ssrn.com/abstract=2678890.
[1441] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 49. See also D. Evans and R. Schmalensee, "Some Economic Aspects of Antitrust Analysis in Dynamically Competitive Industries", *Innovation Policy and the Economy*, Volume 2, A. Jaffe, J. Lerner and S. Stern (eds.), Cambridge, MIT Press, 2002, p. 1.
[1442] See J. Schumpeter, *The Theory of Economic Development: an Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*, Harvard University Press, 1932.
[1443] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 49.

and disruptive innovation.[1444] One potential explanation is that the long-term benefits of incentivising competition *for* the market are, in fact, extremely difficult to assess, as they precisely involve long-term considerations about the development of the market which are, by nature, difficult to predict.[1445] On the other hand, short-term benefits of incentivising competition *in* the market are easier to anticipate and can be observed through increased competition in the downstream markets, leading to more choices and lower prices for consumers.[1446] Therefore, it is understandable that, in the above-mentioned "exceptional circumstances", the competition authorities are willing to impose a duty to deal in order to ensure that a sufficient competitive pressure *in* the market remains in the short-term, as it is unsure that a third party will ever be able to engage, in the long-term, in disruptive innovation that will displace the incumbent by competing *for* the market. In this regard, serious doubts could be casted on whether large digital players such as Google, Facebook, Amazon, Microsoft or Apple will ever be displaced through disruptive innovation by a third party. This is because these actors have entrenched their strong market positions over the years and have used it to continuously expand their ecosystems.[1447]

b) Application of the essential facilities doctrine to data markets: adaptation required?

239. As outlined above, the essential facilities doctrine case law is well established and it seems to have reached an appropriate balance between the costs and the benefits of providing access to the facility presented as "essential", at least when this facility is a "traditional" tangible or intangible resource, in the sense of those that were studied in Part I, Chapter 2, Section A. Yet, this thesis has demonstrated that data has different characteristics than these "traditional" resources.[1448] Indeed, data is a non-rivalrous and general-purpose good[1449], which nevertheless remains technically and contractually excludable.[1450]

This raises the question of whether the balance reached by the essential facilities doctrine case law presented above remains appropriate in light of data's characteristics, or whether the result of this balancing exercise needs to be adapted in order to better fit the characteristics of the data markets. Said otherwise, can data be considered as an essential facility, in light of the existing conditions spelled out in the case law? If not, how could these conditions be adapted to better fit the characteristics of the data markets? In fact, the applicability of the essential facilities doctrine to refusals to grant access to data has been the topic of numerous contributions[1451], and some serious doubts have been casted about its potential application to

---

[1444] *Ibid*., p. 51.
[1445] *Ibidem*.
[1446] *Ibidem*.
[1447] See points 83 to 85.
[1448] See Part I, Chapter 2, Section B, a).
[1449] See point 52.
[1450] See point 53. W. Kerber, "Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 118.
[1451] See, *inter alia*, I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, Alphen aan den Rijn, Kluwer, 2016; J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", op. cit.*, p. 44-55; I. Graef, S. Wahyuningtyas and P. Valcke, "Assessing data access

data markets.[1452] To assess the applicability of this theory to such markets, this thesis will delve further in the suitability of the existing conditions of the essential facilities doctrine for data markets.

1. The "indispensability" condition

240. The first condition for the application of the essential facilities doctrine is that the access to the facility must be indispensable to enable the undertaking requesting access to operate in a secondary market.[1453] In this regard, the European Court of Justice held in *Bronner* that the access to a facility will not be indispensable if a (less advantageous) alternative can be developed by any undertaking other than the dominant undertaking.[1454] To be precise, the "indispensability" condition does not require the demonstration of the absence of "any alternative at all", but rather the absence of "a sufficient alternative for *any* undertaking". Indeed, if one takes the example of a port used as the starting point to cross a narrow see, this infrastructure might be considered as an essential facility for ferry operators even if there is another port 500 kilometre away, as this alternative, though existent, might not be considered as "sufficient for *any* undertaking" in this context.

While this threshold might have been lowered in *Microsoft*, where the Court of First Instance concluded that the access to Microsoft's interoperability information was indispensable in order for Sun Microsystems to be able to compete "on an equal footing"[1455], the European Court of Justice did not have the opportunity to rule on whether it agrees or not with this finding.[1456]

241. When applied to data, the "indispensability" condition requires to demonstrate that "the data owned by the incumbent is truly unique and that there is no possibility for the competitor to obtain the data that it needs to perform its services".[1457] If the access is requested to raw (unstructured) data, this requires a case-by-case assessment of whether any alternative raw dataset is available to the access seeker, or whether the same raw data could be collected by any undertaking having the same size as the dominant undertaking.[1458] If the access is requested to information deriving from such raw data (i.e. structured data)[1459], this will require a case-by-case assessment of whether the same information is available elsewhere (i.e. whether it could be derived from another raw dataset), or whether the same information could

---

issues in online platforms", *Telecommunications Policy*, 2015, Vol. 39, p. 382; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, *op. cit.*; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit.*; J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit.*

[1452] See G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *European Competition Journal*, 2017, Issue 13, Vol. 2-3, p. 249-281.

[1453] See point 237.

[1454] ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569, § 43.

[1455] CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289, § 421.

[1456] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 45-46.

[1457] Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data*"*, 10 May 2016, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf, p. 18.

[1458] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability: Towards a Governance Framework*"*, *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/, p. 36.

[1459] See point 13.

be obtained by any undertaking having the same size as the dominant undertaking (potentially on the basis of a similar raw dataset).[1460]

According to Colangelo and Maggiolino, if applied to data, the *Bronner* case implies that data that is openly accessible online or can be purchased should never be considered as indispensable, as virtually any undertaking can access it or purchase it from data brokers.[1461] Graef is more nuanced. Although she agrees that data that is truly non-rivalrous may not be considered as being indispensable, she underlines that it should be kept in mind that this same data is excludable and can be made exclusive through contractual or technical means.[1462] This could make some types of data indispensable, notably some types of observed personal data that can, in practice, only be collected by dominant undertakings that benefit from strong network effects.[1463] Moreover, the way in which raw data is structured into information could make it indispensable, if this structuring is the consequence of strong network effects leading to a *de facto* industry standard.[1464] Indeed, it should be reminded that, in *IMS Health*, the Court outlined that the users' degree of participation in the development of IMS' standard brick structure, and the costs linked to it, had to be taken into consideration when determining whether IMS' structure was indispensable for the presentation of regional sales data on pharmaceutical products, as the users had become technically dependent on IMS' structure.[1465]

242. Interestingly, data has already been considered as indispensable, when collected in the context of former public monopolies, in a French (*GDF Suez*)[1466] and a Belgian (*Nationale Loterij*)[1467] case. This echoes Advocate General Jacobs' opinion in *Bronner*, where he indicated that the cost of duplicating a facility created under non-competitive conditions, such as through public funding, might constitute an insuperable barrier to entry rendering the access to this facility indispensable.[1468] In both of these cases, a former public monopolist used a customer list that it had developed when it enjoyed a legal monopoly to promote a new service, and this allowed it "to compete unfairly through data cross-subsidisation which "un-levels" the playing field between the former monopolist and the new entrants".[1469] In the French *GDF Suez* case, the French *Autorité de la concurrence* found that the customer list that GDF Suez had developed thanks to its legal monopoly on the gas market was not easily replicable by new entrants and that, by refusing to share this indispensable asset with them,

---

[1460] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 36.
[1461] G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *op. cit.*, p. 270-271.
[1462] I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit*., p. 267. See also J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 28.
[1463] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 36; J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 53.
[1464] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 36.
[1465] ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, §§ 29-30.
[1466] Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, available at https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf.
[1467] Belgian Competition Authority, Decision n°BMA-2015-P/K-27-AUD, 22 September 2015, available at https://www.abc-bma.be/sites/default/files/content/download/files/2015pk27-aud-bma-pub.pdf.
[1468] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, §§ 66-67.
[1469] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 35.

GDZ Suez had abused its dominant position in the market for natural gas.[1470] In the Belgian *Nationale Loterij* case, the Belgian Competition Authority found that the access to the customer list that the Nationale Lottery had developed thanks to its legal monopoly on the Belgian lottery market was indispensable to compete with the Nationale Lottery on the sports betting market, as this customer list "could not have been reproduced by competitors in the market under reasonable financial conditions and within a reasonable period of time".[1471]

243. In spite of these two examples, it is important to outline that, even if some data are not accessible to all firms on an equal basis and are not sold by data brokers, this does not necessarily imply that these data are indispensable, as long as it is possible to find substitutes.[1472] This was notably affirmed by the European Commission in the *Facebook/WhatsApp* merger, where it indicated that a wide number of undertakings collect user data for advertising purposes (Google, Facebook, Amazon, eBay…).[1473] In sum, while there might be cases in which a specific dataset will be considered as being indispensable, these will likely be exceptional.

In itself, this is not too problematic because the essential facilities doctrine entails a strong interference with the data holder's business interests, which justifies why it should only apply in exceptional circumstances. These circumstances could notably result from the fact that a data holder is the sole source of a specific type of data, the access to which is indispensable for another undertaking evolving on a downstream market.[1474] This could derive from historic national monopolies, as in the *GDF Suez* and *Nationale Loterij* cases presented above[1475], or from the fact that the collection/production of a certain type of data is the result of a specific type of activity that only a very limited number of actors are able to pursue. Indeed, as outlined by Rubinfeld and Gal, "unique access points to unique data may lead to situations in which the data cannot be easily replicated", as this would require a two-level entry, which might be unrealistic for a large number of undertakings.[1476] This could notably be the case for data created as the result of interactions on a social network (e.g. data collected by Facebook about how people's emotion affect their conduct), for data collected based on a specific standard (e.g. IMS Health's standard brick structure)[1477], or for data generated as a by-product of a specific production activity (e.g. geological data collected as a by-product of an oil deep-drilling activity).[1478] This could also derive from hypotheses where the incumbent data holder

---

[1470] *Ibidem*; I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit.*, p. 271-272.
[1471] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 35.
[1472] G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *op. cit.*, p. 273.
[1473] European Commission, *Facebook/WhatsApp*, 3 October 2014, case M.7217, §§ 188-189; G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *op. cit.*, p. 271.
[1474] See J. Drexl, "Data Access and Control in the Era of Connected Devices", *Study on Behalf of the European Consumer Organisation (BEUC)*, 2019, available at https://www.beuc.eu/publications/beuc-x-2018 121 data access and control in the area of connected devices.pdf, p. 68.
[1475] See point 242.
[1476] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 351.
[1477] See point 241.
[1478] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 351 and 357.

has technically or contractually excluded the access to a sole source of data[1479], or where the access to this sole source of data is subject to a very high access price and/or to very strict conditions.[1480] In such cases, the essential facilities doctrine could prove useful to compel the data holder to share the data at hand with several undertakings, provided that the other conditions of the doctrine are met as well.

244. Finally, it is important to remind here that, in light of the European Court of Justice's decision in *Slovak Telekom*, it seems that this indispensability condition would only apply in cases of outright refusals to provide access to the data, and not to constructive refusals to provide access to the data, namely situations in which the data holder already provides (or is compelled by regulation to provide) access to the data, but does so at unfair conditions.[1481] This distinction is important to keep in mind, as arguably this would imply that if a dominant undertaking is compelled by regulation to provide access to some data (see the sectoral examples in the banking[1482], energy[1483] and automotive sector[1484] and the recent proposal for a Digital Markets Act[1485]) but does so at unfair conditions, this could not only constitute an infringement of that regulation, but also potentially a constructive refusal to share data that might be considered as an abuse of dominant position, the proof of which will not require the demonstration of the indispensability of the data at hand.

2. The condition of the reservation of, and the exclusion of competition on, a secondary market

245. The second condition for the application of the essential facilities doctrine is that, by refusing to provide access to the facility, the dominant undertaking reserves to itself a secondary market by excluding all competition on that market.[1486] In this regard, the European Court of Justice held in *IMS Health* that it was sufficient to identify a potential or even hypothetical market.[1487]

246. The key factor to take into consideration when assessing whether this second condition is fulfilled is thus if "the dominant firm reserves the downstream market to itself by denying a competitor access to an input".[1488] This implies that such a condition will only be fulfilled in

---

[1479] See I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit.*, p. 267. See also J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*", op. cit.*, p. 28.

[1480] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit*., p. 362. See also B. Lundqvist, "Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law", *Stockholm Faculty of Law Research Paper Series n° 54*, 2018, available at https://ssrn.com/abstract=3103870, p. 4.

[1481] See point 236. ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239, §§ 38-61.

[1482] See Part II, Chapter 1, Section B, b).

[1483] See Part II, Chapter 1, Section B, c).

[1484] See Part III, Chapter 3, Section A, a).

[1485] See point 382.

[1486] See point 237.

[1487] See point 233. ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, §§ 44-45.

[1488] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *Yearbook of European Law*, 2019, p. 25. See also ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98, § 56; ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, § 52.

hypothesis where the dominant undertaking is itself already active on the downstream market, and not in hypotheses where it is not (yet) active on the downstream market. Indeed, in the latter case, a refusal to provide access to an input to third parties wishing to conduct a business on a downstream market would not amount to a reservation, by the dominant undertaking, of that market to itself as it is not active on it.[1489] In the context of the application of the essential facilities doctrine to "traditional" resources, this is justified by the fact that, in principle, the dominant firm does not have any incentive to refuse the access to an input to third parties wishing to conduct a business on a downstream market on which it is not active, as it does not have to protect its position on that market and as charging third parties for the access will in fact provide it with additional revenues.[1490]

247. Yet, if applied to digital markets, this requirement might be highly problematic. This is because "data advantages" may be leveraged by undertakings active on one market to expand and strengthen their position in *connected markets*, i.e. distinct markets in which the data gathered in the first market turns out to be a valuable input to improve the goods or services offered.[1491]. Indeed, as outlined by Drexl, *"*a typical feature of the data economy is that data is collected for one purpose but may turn out to be interesting for very different purposes pursued by other firms of very different sectors".[1492] These connections between markets make the digital economy much more dynamic than the "brick-and-mortar" economy.[1493]

Therefore, as the dynamic connection between markets is greater in data markets than in traditional markets, a dominant undertaking may, in fact, refuse to share data with third parties wishing to conduct a business on a downstream market on which it is not (yet) active "either because it plans to enter in the downstream market (future offensive leverage) or because it fears that the data seeker will disrupt its business (defensive leverage)".[1494] Indeed, due to the complex data markets' dynamics, complements to the dominant undertaking's product/service on the upstream market, developed on a downstream market, may, in time, become substitutes to the dominant undertaking's product/service on the upstream market (disruptive innovation).[1495]

[1489] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 25.
[1490] *Ibid*., p. 26.
[1491] J. Prüfer and C. Schottmüller, "Competing with Big Data", *TILEC Discussion Paper No. 2017-006 and CentER Discussion Paper No. 2017-007*, February 2017, available at https://pure.uvt.nl/ws/portalfiles/portal/15514029/2017_007.pdf, p. 2-3; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 56; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 19.
[1492] J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*"*, *op. cit.*, p. 49.
[1493] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 26.
[1494] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 28. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 36-37; I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 67-68.
[1495] See L. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. Valletti and M. Van Alstyne, "The EU Digital Markets Act: A Report from a Panel of Economic Experts", *EU Science Hub*, 2021, available at https://ec.europa.eu/jrc/en/publication/eu-digital-markets-act, p. 26.

248. There is thus a strong argument to be made that this second condition of the essential facilities doctrine should be adapted for digital markets.[1496] More specifically, some authors argue that, since a dominant firm might engage in future offensive or defensive leveraging tactics, "the fact that it is not active in the downstream market itself should not stand in the way of holding the refusal to deal abusive".[1497] Accordingly, when applied to refusals to provide access to data, the second condition of the essential facilities doctrine should arguably be adapted and should arguably also apply to hypothesis in which the refusal prevents a third party from operating a business on a downstream market on which the dominant undertaking is not (yet) active.[1498] In this perspective, it should be added that "the fact that the requested data have not already been traded, which is very often the case in practice, should not be an obstacle to imposing sharing as it suffices that there is demand and that such demand can legally and practically be met".[1499] This echoes the European Court of Justice finding in *IMS Health* that it is sufficient to identify a potential or even hypothetical market.[1500]

3. The "new product" condition

249. The third condition for the application of the essential facilities doctrine is that the refusal to provide access to the facility must prevent the emergence of a new product or service, or of technological developments, which are not offered by the dominant undertaking and for which there is potential consumer demand.[1501] Following the *Microsoft* judgment, this condition has become more difficult to interpret.[1502]

250. If applied to refusals to share data, this "new product" condition implies that the access seeker will have to demonstrate that the data would allow him to create a sufficiently new product/service – or at least an improved product/service if the reduction of the threshold in *Microsoft* became the norm – compared to that of the dominant undertaking.[1503] In this regard, Drexl outlines that while it can be doubted that the mere generation of new information by the access seeker deriving from the data will be sufficiently innovative to meet this requirement, such information could be used to offer new products/services, or at least technical improvements of an existing product/service, on a secondary market.[1504]

However, as for the second condition of the essential facilities doctrine analysed above[1505], this third condition requires, in the context of "traditional" resources, that the dominant

---

[1496] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 26.
[1497] *Ibidem*. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 36.
[1498] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 68.
[1499] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 36.
[1500] ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, § 44.
[1501] See point 237.
[1502] See point 235. R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1503] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 29. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1504] J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access", *op. cit.*, p. 52.
[1505] See points 245 to 248.

undertaking should also be active on the secondary market.[1506] Indeed, the European Court of Justice held in *IMS Health*, that the access seeker should not "limit itself essentially to duplicating the goods or services *already offered on the secondary market* by the [dominant undertaking]" (emphasis added).[1507] Yet, as outlined above, in data markets, the dominant undertaking may in fact not (yet) be active, and may thus not (yet) offer products/services, in the downstream market.[1508] Therefore, some authors have suggested to adapt this "new product" requirement in the context of the application of the essential facilities doctrine to refusals to share data, and to adopt a more general consumer harm approach, that would amount to conducting a balance between the negative consequences that the refusal to share would entail for consumers and the negative consequences that the imposition of a data sharing remedy could entail.[1509]

251. To some extent, adopting such a general consumer harm approach is the aim of Graef's proposal to make the application of the "new product" condition dependent on whether the upstream market is characterised by external market failures, such as strong network effects.[1510] For her, such an adaptation of the "new product" requirement "would bring the essential facilities doctrine more in line with the underlying economic interests and the balance between competition *for* and *in* the market" (emphasis in the text).[1511]

Applying this "new product" condition strictly in situations where the upstream market is not characterised by external market failures would promote competition *for* the market in such situations, by encouraging investments in innovation by the access seekers.[1512] This would incentivise these access seekers to create disruptive products/services that would displace the dominant undertaking, as they know that the creation of the "next big thing"[1513] will provide them with a (temporary) monopoly position on the newly created market.[1514] Indeed, as outlined by the Supreme Court of the United States in *Trinko*, "the opportunity to charge monopoly prices – at least for a short period – is what attracts 'business acumen' in the first place; it induces risk taking that produces innovation and economic growth".[1515]

[1506] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 29. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 37.
[1507] ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257, § 49.
[1508] See point 247.
[1509] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 29. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 37.
[1510] I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit*., p. 275. See also I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 69-72.
[1511] See point 238. I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 71.
[1512] *Ibid*., p. 70.
[1513] See J. Schumpeter, *The Theory of Economic Development: an Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*, Harvard University Press, 1932.
[1514] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 52.
[1515] Supreme Court of the United States, *Verizon Communications v Law Offices of Curtis V. Trinko,* 2004, *LLP*, 540 US 398, p. 407.

On the other hand, external market failures, such as strong network effects, lock-in situations and high switching costs[1516], "may make it commercially unviable for competitors to introduce a new product".[1517] In such cases, long-term competitive advantages may be established, and this could endanger the contestability of these data driven markets.[1518] Indeed, as the market power of these dominant undertakings entrenches over time, this could delay, or even prevent, the occurrence of new waves of competition *for* the market by new entrants.[1519] In such cases where external market failures shield the dominant undertakings from sufficient competitive pressure and market contestability, the standard for competition law intervention should be lowered in order to re-establish some level of competition *in* the market.[1520] Accordingly, Graef argues that in the presence of such external market failures, "the new product condition should be dropped to ensure that access seekers who intend to introduce sustaining innovations or products similar to that of the dominant undertaking are able to gain access to the necessary input so that the process of competition in the market can be (re)launched".[1521] In turn, this would benefit consumers who would be offered lower prices and more choices/variety.[1522]

In fact, Graef argues that her proposal could find some support in the existing essential facilities doctrine case law. For her, the fact that important external market failures prevented market entry by potential competitors in the *Microsoft* case might explain why the Court of First Instance lowered the standards for the fulfilment of the doctrine's conditions.[1523] In contrast, the higher standards imposed by the European Court of Justice in the other cases presented above[1524] would remain applicable in cases where there are no external market failures preventing entry by potential competitors.[1525]

4. Adaptation to the characteristics of data

252. In light of the above, there are strong arguments to support the adaptation of the essential facilities doctrine when it is applied to refusals to share data, as the result of the balancing exercise reached by this doctrine when applied to "traditional" resources may need to be reconsidered in order to better fit the characteristics of the data markets.[1526]

[1516] See Part I, Chapter 2, Section B, c), 1. "Data collection and production incentives" and Part I, Chapter 2, Section B, c), 2. "Entry barriers to data markets". See M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*.; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 339-381; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit*., p. 24.

[1517] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 69.

[1518] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 55.

[1519] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 54-55.

[1520] *Ibidem*.

[1521] *Ibid*., p. 69-70.

[1522] *Ibid*., p. 70.

[1523] See point 234. *Ibid*., p. 55 and 70.

[1524] See especially points 231 to 233.

[1525] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 55.

[1526] *Ibid*., p. 40; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 37-38.

Indeed, any competition intervention interfering with a dominant undertaking's freedom (not) to contract requires "a careful balancing of conflicting considerations"[1527], namely a balance between the costs and the benefits of providing access to the facility presented as "essential". A balance must thus be found between the "need to protect the dominant firm's investment incentives and the need to ensure that strongly entrenched positions of market power, protected by high barriers of entry, remain contestable".[1528] Said otherwise, a careful balancing between promoting short-term and long-term competition and innovation must be operated.[1529]

253. If applied to refusals to share data, this means that compulsory data sharing, through the means of a competition law intervention, should only be imposed if the benefits outweigh the costs.[1530] Indeed, data collection and processing, and consequently data sharing, entail costs, and data sharing obligations might create disincentives for data collection and processing by both the dominant undertaking (fear of free-riding) and the access seekers (expectation to free-ride).[1531] On the other hand, compulsory data sharing could allow access seekers to enter (or create) a secondary market, which could lead to more diversity, choice, innovation and competition.[1532] A balance must thus be found. In this regard, it must be reminded that, due to data's characteristics, the benefits of data sharing may arguably be greater than the benefits of sharing other resources.[1533] Moreover, the costs of data sharing may arguably be smaller than the costs of sharing rival resources, as the impact on the dominant undertaking's incentives will be lower in the former than in the latter situation, since the sharing does not prevent the dominant undertaking from keeping to use the data.[1534] This is even more so if the data to be shared has been generated as a by-product of another business activity[1535], or if it has been collected in the context of a legal monopoly[1536].[1537]

[1527] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 57.
[1528] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit.*, p. 98.
[1529] Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264, § 57.
[1530] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5; W. Kerber, "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *JIPITEC*, 2018, Issue 9, p. 330; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1531] See point 89. J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit.*, p. 76-77; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 374; M. Madison, "Tools for Data Governance", *Technology and Regulation*, 2020, p. 31 and 34; M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 44-45; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1532] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1533] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 31; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*"*, *Report for the German Federal Ministry for Economic Affairs and Energy*, 29 August 2018, available at https://ssrn.com/abstract=3250742, p. 10. See also J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1534] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.
[1535] See the *Magill* case at point 231.
[1536] See the *GDF Suez* and *Nationale Loterij* cases at point 242.
[1537] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 37.

254. Accordingly, some authors argue that the threshold for imposing the access to data as a remedy to an abuse of a dominant position should be lower than the threshold to impose the access to more "traditional" resources.[1538] In this regard, several policy reports on the adaptation of competition law to the digital environment have also outlined that "the threshold for finding that a refusal to supply data constitutes an abuse may be somewhat lower than the threshold for finding an abuse in cases of a refusal to grant access to infrastructures or to intellectual property rights.[1539] This is true in particular if and to the extent that the refusal to grant access relates to data which is generated virtually incidentally and without special investment".[1540] Importantly, this does not mean that there should be no threshold at all, as the benefits of the sharing still need to be balanced with the costs that it entails for the dominant undertaking, but rather that the threshold for imposing the sharing should be lower for data than for more "traditional" resources.[1541]

255. More concretely, the threshold for the application of the essential facilities doctrine could be reduced, when applied to refusals to share data, through the adaptation of the second (reservation of, and the exclusion of competition on, a secondary market) and third (prevention of the appearance of a "new product") conditions of the doctrine. As outlined above[1542], the second condition of the essential facilities doctrine could be adapted in order to also apply to hypotheses in which the refusal prevents a third party from operating a business on a downstream market on which the dominant undertaking is not (yet) active[1543], while the third condition could be made dependent on whether the upstream market is characterised by external market failures, in which case it could arguably be dropped.[1544]

256. Regarding the first condition of the doctrine (the "indispensability" condition), it is argued that it should apply to outright refusals to share data, as the imposition of a data sharing remedy in such a scenario would strongly interfere with the data holder's business interests.[1545] On the other hand, it is argued that this condition should not be applied to constructive refusals to share data.[1546] Indeed, as the imposition of a data sharing remedy would require a form of monitoring[1547], which could be extremely burdensome for

---

[1538] *Ibid*., p. 38.

[1539] In this perspective, the threshold for finding an abuse could thus be higher for data protected by a *sui generis* right than for data that are not protected by such a right, for instance because there has been no substancial investment in their obtention, verification or presentation. On this *sui generis* right, see points 58 to 60.

[1540] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 10. See also J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit*., p. 74-77; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit*., p. 98-108.

[1541] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 38.

[1542] See points 245 to 251.

[1543] I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 68; I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit*., p. 26; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 36.

[1544] I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit*., p. 275. See also I. Graef, "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *op. cit.*, p. 69-72.

[1545] See points 240 to 243.

[1546] See point 244.

[1547] P. Ibáñez Colomo, "Indispensability and Abuse of Dominance: From Commercial Solvents to Slovak Telekom and Google Shopping", 11 December 2019, available at https://ssrn.com/abstract=3502519, p. 35. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 38.

competition authorities, this should be limited to exceptional cases, especially because competition authorities may be ill-suited to deal with such issues.[1548] In this regard, opting for more systemic solutions in order to ensure contestability and innovation on the data markets, rather than resorting to case-by-case competition interventions, might be preferable, notably through the creation of potential *ex ante* legislations imposing B2B data sharing.[1549]

257. The fourth condition of the doctrine (the absence of an objective justification for the refusal) should also be briefly pointed out. Indeed, as some (most) of the data that the access seekers wish to obtain may be personal data, dominant undertakings could be tempted to use personal data protection considerations as an objective justification for refusals to share it[1550], and it might be difficult for competition authorities to evaluate whether such a claim is legitimate, or whether it is a disguise for an anti-competitive conduct.[1551] In this regard, competition authorities should require these dominant undertakings to lay down and substantiate the data protection concerns they raise in order to refuse data sharing with third parties, and they should cooperate with data protection authorities in order to assess whether the data protection standards imposed on third parties by these dominant undertakings are (suspiciously) high.[1552] As this articulation between personal data protection law and competition law requires an extensive analysis, this will be tackled below in a separate Chapter of this thesis.[1553]

258. To conclude, it should be mentioned here that, as the questions pertaining to the type of data sharing remedy to be imposed are equally relevant for the other types of competition law infringements that will be analysed in the following sections, namely abuses of economic dependence (Section B) and input foreclosure in vertical integration (Section C), they will be addressed in a specific section dedicated to overarching considerations pertaining to compulsory B2B data sharing as a competition law remedy (Section D).

Moreover, it is important to underline that, in any case, the essential facilities doctrine might not often be called upon in practice because the threshold, even if it is lowered in the way suggested above, would remain difficult to reach[1554], as the doctrine should only apply in "exceptional circumstances".[1555] Moreover, it only allows targeting a limited number of undertakings, namely those holding a dominant position in a well-defined market.

[1548] See V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *Max Planck Institute for Innovation and Competition Research Paper No. 19-04*, 2019, available at https://ssrn.com/abstract=3337524, p. 18-19; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit*., p. 10.

[1549] See Part III, Chapter 3. See also Communication from the Commission, "*Shaping Europe's digital future*", *op. cit*., p. 9; Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 5 and 14.

[1550] See for instance E. Egan, "Data Portability and Privacy", *Facebook White Paper*, September 2019, available at https://iapp.org/media/pdf/fb_whitepaper_sep_2019.pdf.

[1551] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech", *TILEC Discussion Paper DP 2020-012*, May 2020, available at https://ssrn.com/abstract=3598130, p. 36-37.

[1552] *Ibidem*.

[1553] See Part III, Chapter 2. "Articulation between data protection and competition law".

[1554] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 8.

[1555] See point 237.

Yet, market definition is a complex task in the digital environment, as digital markets are often two-sided and characterised by network externalities that each side imposes on the other.[1556] Moreover, they often imply "zero" price products/services on one side of the market, generally the consumer side (these products/services are however not "free", as consumers "pay" with their personal data to use them[1557]), which are subsidised by the other side of the market.[1558] As a result, the classic "small but significant non-transitory increase in price" (SSNIP) test is difficult to apply in such markets, and the alternative proposition of resorting to a "small but significant non-transitory decrease in quality" (SSNDQ) test faces the same difficulties of balancing between the two sides of the market than the SSNIP test.[1559] Therefore, there are growing calls to reconsider the way in which digital markets are defined in the digital environment. Traditionally, as outlined by Bourreau and de Streel:

> "The determination of market power is done in two steps which are closely related. First, the product market is defined mainly on the basis of demand substitution between existing products and, in a subsidiary way, on the basis of supply substitution when new suppliers can enter in the short term without entailing a significant adjustment of existing tangible and intangible assets.[1560] Then, the market power is determined mainly on the basis of the current market position of the firms and the barriers to entry and expansion and, when relevant, the countervailing buyer power[1561]".[1562]

When determining market power on digital multi-sided markets, the European Commission's expert report on "Competition Policy for the digital era" suggests, instead, to focus on product/service functionalities as the starting point for determining substitutability relationships, even if this test is not as rigorous as the SSNIP test.[1563] In this perspective, it is suggested that competition policy should analyse all the sides of the market and should consider the way in which they interact.[1564] Indeed, the interdependence between these different sides/markets is crucial in digital markets, and this contrasts with classic market definition which traditionally aims at isolating markets from one another.[1565] Pushing this logic further, some have suggested to take this interdependence into account by focussing on

---

[1556] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 42-43. For a broader analysis of the complexity of market definition in the digital environment, see p. 42-50; I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition Law and Economics Review*, 2015, Vol. 38, Issue 4, p. 473–506.

[1557] See point 131.

[1558] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 44.

[1559] *Ibid*., p. 44-45.

[1560] Commission Notice on the definition of relevant market for the purposes of Community competition law, OJ C 372/5, 9 December 1997, §§ 13-23. This Notice is currently under review: see https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12325-Evaluation-of-the-Commission-Notice-on-market-definition-in-EU-competition-law.

[1561] Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, *OJ C 45/7*, 24 February 2009, §§ 12-18.

[1562] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 25.

[1563] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 45.

[1564] *Ibidem*.

[1565] *Ibid*., p. 46.

"ecosystems of products/services"[1566], and to complement this with "a novel analysis based on capabilities/input markets in order to better reflect the importance, the rate and the uncertainty of innovation and the key role played by innovation capabilities [such as data]".[1567] In any case, the dynamic nature of the digital environment might entail that it will always be complicated to identify well-defined markets because, as outlined by Crémer *et al.*:

> "Dynamic market environment leads to fluid, quickly-changing relationships of substitutability and possibly partial overlaps of varying significance between different services, sometimes combined with practices of multihoming and/or changing perceptions of consumer needs. (…) In such settings, the determination of substitutability relationships based on the present patterns of choice may turn out to be too narrow in hindsight and lead to "false positives". At the same time, inaction in the light of a mere possibility of changing market boundaries may lead to "false negatives"".[1568]

259. As a result, establishing dominance of large digital firms on such markets will likely remain a complex task.[1569] Accordingly, some have argued that there could be more flexibility in applying the abuse of dominance rules, as "instead of first defining the relevant market, competition authorities and courts could be allowed to find relevant market power by implication when anti-competitive behaviour is not sufficiently controlled by competition and a subsequent foreclosure effect can be proven".[1570] In the same vein, others have held that, in digital markets, "less emphasis should be put on the market definition part of the analysis, and [that] more importance [should be] attributed to the theories of harm and identification of anti-competitive strategies".[1571]

In this perspective, it is interesting to note that the German experts' report for the modernisation of competition law suggested the introduction, in German competition law, of the possibility for competition authorities to intervene below the threshold of market dominance, in cases where the unilateral behaviour of an undertaking that is not (yet) dominant, but that is active on a market characterised by strong positive network effects, aims at inducing market "tipping" in its favour, notably through targeted obstruction of multi-homing or switching.[1572] Yet, as outlined above[1573], such "tipping" could be particularly

---

[1566] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 26; see also J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 47-48.
[1567] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 27.
[1568] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 47.
[1569] W. Kerber, "Updating Competition Policy for the Digital Economy?", *op. cit.*, p. 5.
[1570] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 1.
[1571] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 46.
[1572] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 2; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, *op. cit.*, p. 59-64. See also the Governmental draft bill (GWB-Digitalisierungsgesetz) for the 10th amendment to the Competition Act of 9 September 2020: Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen, available at https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/gwb-digitalisierungsgesetz.html.

harmful for competition due to its potential irreversibility.[1574] Accordingly, the report suggested the introduction of a new provision in the GWB[1575], "which prohibits platform operators in tight oligopolies, or platform operators with superior market power, to obstruct multi-homing or the changing of platforms, insofar as this strategic obstruction is suitable to promote a "tipping" of the market".[1576] Such a provision has eventually been included in the tenth amendment to the German Competition Act, namely the GWB Digitalisation Act ("GWB-Digitalisierungsgesetz".[1577]

Moreover, the same report also suggested the inclusion of a third form of market power in the GWB, distinct from supplier and buyer power, namely "intermediation power"[1578], which some large digital actors benefit from due to increasing returns to scale, network externalities and their control on large amounts of data, and which they can leverage in adjacent markets.[1579] Such a provision has also been included in the GWB Digitalisation Act.[1580] As summarised by Kerber, "the basic idea is that many platforms do not only have market power due to large direct and indirect network effects, and can therefore be gatekeepers to large groups of customers, but that they are at the same time also information intermediaries, e.g. by offering search functions, rankings and ratings, which implies information asymmetries between the platforms and the users".[1581] As a result, the German report outlines that "providers of goods and services may depend for their economic survival on being present on each and any of those platforms, or at least on the majority of them if the same customers cannot be served in a similarly effective way otherwise and if it is essential to reach a large proportion of potential customers. A provider of goods or services may therefore be dependent on a digital platform under similar conditions as – conventionally – on a reseller,

---

[1573] See point 79. See also J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf, p. 6-9; J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2.

[1574] W. Kerber, "Updating Competition Policy for the Digital Economy?", *op. cit.*, p. 6; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 3.

[1575] "*Gesetz gegen Wettbewerbsbeschränkungen*" (Act against Restraints of Competition, adopted on 26 August 1998 and lastly amended on 19 January 2021). The official English translation of the GWB is available at http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0066.

[1576] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 3.

[1577] See Bundeskartellamt, "Amendment of the German Act against Restraints of Competition (Press release)", 19 January 2021, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html. The full text, in German, of the GWB-Digitalisierungsgesetz is available at https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s0002.pdf%27%5D__1612262835179.

[1578] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 3-4. For more information on this concept, see H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, *op. cit.*, p. 66 *et seq*. See also the Governmental draft bill (GWB-Digitalisierungsgesetz) for the 10th amendment to the Competition Act of 9 September 2020, *op. cit*.

[1579] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 49.

[1580] See Bundeskartellamt, "Amendment of the German Act against Restraints of Competition (Press release)", *op. cit*.

[1581] W. Kerber, "Updating Competition Policy for the Digital Economy?", *op. cit.*, p. 6.

such as a food retailer".[1582] In fact, it should be outlined that the GWB already contains a provision forbidding the abuses of such economic dependence[1583], which also allows competition authorities to intervene below the threshold of market dominance. This thesis will now turn to the analysis of such provisions forbidding the abuse of economic dependence.

[1582] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 3-4.

[1583] See §20 GWB "*Gesetz gegen Wettbewerbsbeschränkungen*" (Act against Restraints of Competition, adopted on 26 August 1998 and lastly amended on 19 January 2021). The official English translation of the GWB is available at http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0066.

Section B. Abuse of economic dependence[1584]

260. While Article 102 TFEU only allows targeting dominant undertakings, powerful data holders that do not benefit from such a dominant position could also start refusing to share their data with undertakings having a limited bargaining power. For instance, in the USA, Twitter suddenly decided to stop providing access to its "Firehose" data to PeopleBrowsr, a data analytics company, while this access had been provided freely for years and while PeopleBrowsr had built its business model on this access.[1585] Similarly, after having allowed hiQ's access and use of its data for several years, LinkedIn requested hiQ to stop accessing its data, and used blocking techniques preventing hiQ from doing so, while this access was at the core of hiQ's business model.[1586] In these two cases, while neither Twitter nor LinkedIn were considered as being dominant, both PeopleBrowsr and hiQ were arguably dependent on these platforms to operate their business. Indeed, as outlined by the Expert Group for the Observatory on the Online Platform Economy, "platforms generate value for businesses by providing them with access to demand for their products, or to factors of production such as labour or capital. A business can become to varying extents dependent on (or even "locked in" to) such a platform. This makes the business vulnerable to possible unfair and distortive practices by the platform".[1587]

These two cases, which will be discussed more extensively further[1588], raise the question of whether the concept of abuse of economic dependence could prove to be a valuable alternative in order to deal with refusals, by non-dominant undertakings, to share data with undertakings having a weaker bargaining power (b). In order to be able to answer this question, the "traditional" balance reached by the application of the concept of abuse of economic dependence to "traditional" resources must first be analysed (a).

a) The "traditional" abuse of economic dependence balance

261. Given that there is no harmonisation of the provisions pertaining to the abuse of economic dependence in the EU, each Member State is free to adopt the rules that it sees fit.[1589] For the purpose of this thesis, it has been chosen to focus on Belgium, which has

---

[1584] This Section is based on T. Tombal, "Economic dependence and data access", *IIC*, 2020, Volume 51, Issue 1, p. 70-98.

[1585] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013; I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, Alphen aan den Rijn, Kluwer, 2016, p. 257.

[1586] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

[1587] Expert Group for the Observatory on the Online Platform Economy, "Measurement & Economic Indicators: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports, p. 17.

[1588] See point 268.

[1589] See Article 3.2 of the Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty Regulation, *OJ L 1*, 4 January 2003. This Article allows Member States to adopt and apply on their territory stricter national laws which prohibit or sanction unilateral conduct engaged in by undertakings.

adopted such a law on the 4th of April 2019[1590], and on Germany and France, which provided inspiration to the Belgian legislator.[1591] In Belgium, the law of 4 April 2019 has added a new Article IV.2/1 in the "Code de droit économique" (hereafter "CDE"), which provides that:

> *"*The abusive exploitation, by one or more undertaking(s), of the state of economic dependence of one or more dependent undertaking(s) is prohibited, if competition is likely to be affected on the relevant Belgian market or a substantial part of it*"*.[1592]

In Germany, §20 GWB[1593] provides that:

> "(1) § 19(1)[1594] in conjunction with paragraph 2 no. 1 shall also apply to undertakings and associations of undertakings insofar as other undertakings are dependent on them as suppliers or purchasers of a certain type of goods or commercial services, in such a way that there aren't sufficient and reasonable possibilities to switch to third undertakings, and that there is a clear imbalance to the countervailing power of the other undertakings (relative market power)".[1595]

While the previous version of §20 GWB only benefitted small or medium-sized enterprises, this limitation was abolished by the tenth amendment to the German Competition Act, namely the GWB Digitalisation Act ("GWB-Digitalisierungsgesetz")[1596], as the situation of dependence covered by this provision could also arise for large firms.[1597]

In France, Article L. 420-2, al. 2 of the French "Code de Commerce" provides that:

> *"*The abuse of the state of economic dependence of a client or supplier by an undertaking or group of undertakings is also prohibited, if it is likely to affect the functioning or structure of competition".[1598]

[1590] Loi du 4 avril 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *M.B.*, 24 mai 2019.

[1591] For an overview of all of the EU Member States that have such provisions against the abuse of economic dependence see: College of Europe, "Study on the impact of national rules on unilateral conduct that diverge from Article 102 of the Treaty on the Functioning of the European Union (TFEU) – Final Report", 21 November 2012, available at https://ec.europa.eu/competition/calls/tenders_closed.html.

[1592] Author's translation of: "Est interdit le fait pour une ou plusieurs entreprises d'exploiter de façon abusive une position de dépendance économique dans laquelle se trouvent une ou plusieurs entreprises à son ou à leur égard, dès lors que la concurrence est susceptible d'en être affectée sur le marché belge concerné ou une partie substantielle de celui-ci*"*.

[1593] "*Gesetz gegen Wettbewerbsbeschränkungen*" (Act against Restraints of Competition, adopted on 26 August 1998 and lastly amended on 19 January 2021). The official English translation of the GWB is available at http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0066.

[1594] §19 GWB targets the prohibited conduct of dominant undertakings.

[1595] Author's own translation.

[1596] See Bundeskartellamt, "Amendment of the German Act against Restraints of Competition (Press release)", *op. cit*.

[1597] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*"*, *op. cit.*, p. 7. For a more extensive discussion of this point, see H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, *op. cit*., p. 56-57.

[1598] Official English translation: https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

From these provisions, it appears that two main conditions of application are common to the three Member States, namely the need to show a state of economic dependence and the need to show an abuse of this state of economic dependence.

1. State of economic dependence

262. The notion of economic dependence can be defined as the absence of "sufficient and reasonable possibilities" of switching to other undertakings. According to Feteira, "[it] is usually understood that the *sufficiency* of existing alternatives can be assessed on *objective* grounds, whilst the *reasonableness* of resorting to such alternatives necessarily entails a more *subjective* assessment which relies more heavily on the possibilities available to the plaintiff" (emphasis in the original text).[1599]

Although this is the specific wording used in Germany, the test is substantially the same in France and Belgium. Indeed, French law requires to show the absence of an equivalent solution (objective assessment of the sufficiency of alternatives) making it impossible for the plaintiff to resort, within a reasonable time frame[1600], to another undertaking due to technical or economic reasons[1601] (subjective assessment of the reasonableness to resort to these alternatives). Similarly, Belgian law requires to show the absence of an equivalent alternative (objective assessment of the sufficiency of alternatives) for the dependent undertaking to switch towards another undertaking within a reasonable time frame, on reasonable terms and at reasonable cost[1602] (subjective assessment of the reasonableness to resort to these alternatives).

263. Contrary to the assessment of a position of dominance, which takes place in the context of a given relevant market involving multiple actors, the assessment of a state of economic dependence focusses on a concrete bilateral relationship. This bilateral perspective is at the core of these provisions, as the concern is not whether a dominant undertaking has the market power to behave independently of the other actors on the market, but rather whether an undertaking is dependent on its bilateral relationship with a (non-dominant) undertaking in order to operate.[1603] This is apparent from the four classical case groups of economic dependence, namely: assortment-based dependence[1604] (the other party's good is considered

---

[1599] L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, Alphen aan den Rijn, Kluwer, 2016, p. 150.
[1600] Autorité de la concurrence, Decision n°15-A-06, 31 March 2015, §269.
[1601] *Ibid*., p. 167-168. See also French Cour de Cassation, case n° 02-14529, 3 March 2004.
[1602] Article I.6, 4° CDE. Belgian law requires to show that, due to this lack of reasonably equivalent alternative, the stronger undertaking can impose services or conditions which could not be obtained under normal market circumstances, but this condition is redundant with the definition of the abuse provided for in Belgian law: "any behaviour that an undertaking can adopt because it holds the dependent undertaking in a situation of economic dependence" (Proposition de loi du 22 février 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *Doc*., Ch., 2018-2019, n° 3595/001, p. 15).
[1603] See, for instance, Autorité de la concurrence, Decision n°10-D-08, 3 March 2010, § 165. See also Autorité de la concurrence, Decision n°20-MC-01 (*Syndicat des éditeurs de presse v. Google*), 9 April 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-04/20mc01.pdf, § 179. This latter case is briefly evoked at point 270.
[1604] See for example BGH, *Designer Polstermöbel*, 9 May 2000, WuW/DE-R 481; *Depotkosmetik*, 15 May 1998, WuW/DE-R 206; *Reparaturbetrieb*, 23 February 1988, WuW/E BGH 2479; *Cartier*, 10 November 1987,

as a must-stock good due to its notoriety or popularity); scarcity-based dependence[1605] (the other party is one of the rare sources where the good can be found); dependence arising from a long-lasting business relationship[1606]; and demand-based dependence[1607] (due to the other party's importance in the undertaking's turnover).[1608]

Yet, despite the clear identification of these case groups, situations of economic dependence have rarely been acknowledged by the courts in practice, because the requirement of the demonstration of the absence of reasonable alternatives has been restrictively interpreted by the courts.[1609] Indeed, courts require the (allegedly) dependent undertakings to provide in-depth economic and financial evidence to support their claim, and these undertakings truly struggle to bring such a proof.[1610] Therefore, in light of this high burden of proof, many (allegedly) dependent undertakings refrain from formulating such complaints, as they fear reprisals if they were to be unsuccessful.[1611]

2. Abuse of the economic dependence

264. Showing a state of economic dependence is not enough, as it must also be shown that there has been an abuse of this state. This calls for two types of considerations. On the one hand, it is first necessary to discuss the types of conduct that may constitute a potential abuse. On the other hand, the anticompetitive harm deriving from this abuse must be questioned, and there is a need to find a balance between the benefits and the costs of competition law intervention.

WuW/E BGH 2451; *Adidas*, 30 June 1981, WuW/E BGH 1885; *Rossignol*, 20 November 1975, WuW/E BGH 1391. See also French Cour de Cassation, cases n° 91-16988 and 91-17090, 12 October 1993; Autorité de la concurrence, Decisions n^{os} 87-MC-02, 25 March 1987; 89-D-39, 13 December 1989; 93-D-48, 9 November 1993; 98-D-32, 26 May 1998; and 01-D-49, 31 August 2001.

[1605] See for example Berlin Court of Appeal, *Agip II*, 7 June 1974 and 4 July 1974, WuW/E OLG 1497 and 1499. See also French Cour de Cassation, cases n° 91-16988 and 91-17090, 12 October 1993.

[1606] See for example BGH, *Kfz-Vertragshändler*, 21 February 1995, WuW/E BGH 2983; *Herstellerleasing*, 19 January 1993, WuW/E BGH 2875; *Opel Blitz*, 23 February 1988, WuW/E BGH 2491; *Kraftwagenleasing*, 30 September 1971, WuW/E BGH 1211. See also Autorité de la concurrence, Decisions n^{os} 89-D-16, 30 May 1989; 90-D-42, 6 November 1990; 99-D-54, 29 September 1999; and 20-D-04, 16 March 2020.

[1607] See for example BGH, *Konditionenanpassung*, 24 September 2002, WuW/DE-R 948; *Sehhilfen*, 12 May 1976, WuW/E BGH 1423. See also French Cour de Cassation, cases n° 91-16988 and 91-17090, 12 October 1993; Autorité de la concurrence, Decisions n^{os} 91-D-51, 19 November 1991; 94-D-60, 13 December 1994; 96-D-44, 18 June 1996; 03-D-11, 23 February 2003; and 20-D-04, 16 March 2020; Comm. Gand (réf.), 28 octobre 2020, inéd., R.G. n°A/20/02490, commented in B. Gielen and C. Verdonck, "First Belgian ruling on abuse of economic dependence", 3 December 2020, available at https://www.lexology.com.

[1608] L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, *op. cit.*, p. 151-158 and 170-171.

[1609] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *Yearbook of European Law*, 2019, p. 43. See also College of Europe, "Study on the impact of national rules on unilateral conduct that diverge from Article 102 of the Treaty on the Functioning of the European Union (TFEU) – Final Report", *op. cit.*, p. 51-57. For rare cases where this situation of economic dependence was acknowledged, see Comm. Gand (réf.), 28 octobre 2020, inéd., R.G. n°A/20/02490, commented in B. Gielen and C. Verdonck, "First Belgian ruling on abuse of economic dependence", 3 December 2020, available at https://www.lexology.com; and Autorité de la concurrence, Decision n° 20-D-04, 16 March 2020, p. 205-209.

[1610] See College of Europe, "Study on the impact of national rules on unilateral conduct that diverge from Article 102 of the Treaty on the Functioning of the European Union (TFEU) – Final Report", *op. cit.*, p. 51.

[1611] *Ibid*., p. 52.

i. Types of conduct that may constitute a potential abuse

265. Any behaviour that an undertaking can adopt because it holds the dependent undertaking in a situation of economic dependence may constitute a potential abuse. Therefore, it will be necessary to show that the undertaking has exceeded the reasonable exercise of its economic freedom and that it could not have adopted this behaviour "but for" the state of economic dependence.[1612] In this regard, Belgian law proves particularly useful as Article IV.2/1 CDE identifies five practices that can be considered as abusive:

> *"*1° the unlawful refusal of a sale, purchase or other transaction conditions[1613]; 2° the direct or indirect imposition of purchase or sale prices or other unfair trading conditions; 3° the limitation of production, markets or technical development to the detriment of consumers; 4° the application of unequal conditions to equivalent services to economic partners, thereby placing them at a competitive disadvantage[1614]; 5° the subjection of the conclusion of contracts to the acceptance, by the economic partners, of additional services which, by their nature or according to commercial usage, are not related to the subject matter of those contracts".[1615]

This list provides some clarity regarding practices that could potentially be considered as abusive, as it is presumed that an undertaking has only been able to adopt them because it holds the dependent undertaking in a situation of economic dependence.

ii. Anticompetitive effects

266. As these provisions on the abuse of economic dependence are situated in the realm of competition law, it seems natural that a form of anticompetitive effect must also be demonstrated. Yet, this might seem counter-intuitive as, at first sight, these provisions focus on bilateral relationships and not on a given market. To clarify this, the *ratio legis* of these abuse of economic dependence provisions must be outlined.

[1612] L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, *op. cit*., p. 171; Proposition de loi du 22 février 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *Doc*., Ch., 2018-2019, n° 3595/001, p. 15.

[1613] For an example, see Comm. Gand (réf.), 28 octobre 2020, inéd., R.G. n°A/20/02490, commented in B. Gielen and C. Verdonck, "First Belgian ruling on abuse of economic dependence", 3 December 2020, available at https://www.lexology.com.

[1614] See Autorité de la concurrence, Decision n° 20-D-04, 16 March 2020, p. 209-219, where the *Autorité* ruled that Apple subjected its premium distributors to unfair and unfavourable commercial conditions in comparison with those it imposed to its network of integrated distributors, and that this differential treatment was not objectively justified. According to the *Autorité*, this constituted an abuse as these premium distributors (mostly SMEs) were discriminated, as they were often deprived of sufficient stock during the launch of new goods and were thus unable to fulfil client orders, while its network of integrated distributors was regularly supplied and thus did not have these problems.

[1615] Author's translation of: "1° le refus illicite d'une vente, d'un achat ou d'autres conditions de transaction ; 2° l'imposition de façon directe ou indirecte des prix d'achat ou de vente ou d'autres conditions de transaction non équitables ; 3° la limitation de la production, des débouchés ou du développement technique au préjudice des consommateurs ; 4° le fait d'appliquer à l'égard de partenaires économiques des conditions inégales à des prestations équivalentes, en leur infligeant de ce fait un désavantage dans la concurrence ; 5° le fait de subordonner la conclusion de contrats à l'acceptation, par les partenaires économiques, de prestations supplémentaires, qui, par leur nature ou selon les usages commerciaux, n'ont pas de lien avec l'objet de ces contrats*"*.

In Belgian law, the stated objective is to protect weaker parties against stronger undertakings who act unfairly, by limiting marginally, and in the public interest, their entrepreneurial freedom by sanctioning abusive conducts resulting from positions of economic dependence.[1616] Similarly, abuse of economic dependence provisions were introduced in French law in order to counter the economic power of distribution groups that the rules of abuse of dominance were allegedly not able to address, and in German law in order to tackle concerns over market conditions in the retail market.[1617] This tends to show that the goal of such provisions is two-fold, namely protecting weaker parties against stronger undertakings, and countering the economic power of some non-dominant undertakings.

This illustrates the core issue at hand when applying legal provisions relating to economic dependence, as they require to reach a careful balancing between "safeguarding competition in the market, respecting freedom of contract and protecting the freedom of competition of the weaker parties against powerful business partners".[1618] Indeed, while the non-dominant undertaking has the freedom not to contract (or to bring an end to an existing contract) with the dependent undertaking, this might create anticompetitive effects by restricting the latter's freedom to compete, and more broadly by restricting market access and contestability. On the other hand, protecting smaller competitors could potentially harm consumers if this leads to market inefficiencies resulting in higher prices.[1619] A balance of interest thus has to be conducted, whose aim is to protect the ability of the parties to take part in the process of competition and to ensure that all benefit from an equal opportunity to enter and operate in the market, which illustrates the core underlying balance between the parties' individual interests and the broader institutional interest of protecting the competitive process and market efficiency.[1620]

267. More fundamentally, this illustrates the debate between the different approaches of the economic role of competition law, namely whether competition law's focus should be the efficiency of the market or the protection of the freedom to compete.[1621] Incidentally, this debate is especially important for the effectivity of the French and Belgian provisions, which

---

[1616] Proposition de loi du 22 février 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *Doc*., Ch., 2018-2019, n° 3595/001, p. 4-5.

[1617] L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, *op. cit.*, p. 144-145 and 165.

[1618] L. Boy, "Abuse of market power: controlling dominance or protecting competition?", *The Evolution of European Competition Law: whose Regulation, which Competition?*, H. Ullrich (ed.), Cheltenham and Northampton, Edward Elgar, 2006, p. 218, cited in M. Bakhoum, "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *Max Planck Institute for Innovation & Competition Research Paper No. 15-15*, 2015, available at https://ssrn.com/abstract=2703809, p. 14.

[1619] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 44; College of Europe, "Study on the impact of national rules on unilateral conduct that diverge from Article 102 of the Treaty on the Functioning of the European Union (TFEU) – Final Report", *op. cit.*, p. 13-15.

[1620] L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, *op. cit.*, p. 161-162; I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 44.

[1621] M. Bakhoum, "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *op. cit.*, p. 14.

explicitly state that the abuse has to be likely to affect the functioning or the structure of competition.[1622]

Under the "efficiency approach", the possibility to protect against abuses of economic dependence through competition law is questionable because, as pointed out by Bougette *et al.*, "at first sight, an abuse of economic dependence involves only a vertical relationship between two partners along a supply chain. It may not affect any relevant markets and inflict harm only on a given undertaking".[1623] Indeed, given that this issue of economic dependence is assessed in a bilateral relationship and that the stronger undertaking is not required to have a dominant position, but merely a relative market power towards the weaker undertaking, the exclusion, by a non-dominant undertaking's behaviour, of a small dependent undertaking may arguably rarely be likely to affect the functioning or structure of competition under the "efficiency approach". This is because showing that the dependent undertaking's mere exclusion from the market is likely to have such an effect is a major hurdle.[1624] For instance, if an aftermarket service provider is dependent on a car manufacturer having a 20% market share, due to a long-lasting business relationship, and that the latter terminates this relationship in an abusive way, the small undertaking may not be able to show that this is likely to affect the efficiency of this aftermarket. Moreover, the competition authorities' reluctance to deal with issues that appear to be more linked to contract law than to competition law explains that cases of abuse of economic dependence have been neglected in their decisional practice.[1625]

However, under the "freedom to compete approach", protecting against abuses of economic dependence may be justified in order to protect the market against structural restrictions.[1626] As pointed out by Bougette *et al.*, "economic dependence related abuses can have significant effects on overall welfare. Ignoring such abuses as potential anticompetitive behaviour per se, violates the fundamental idea of the effects-based approach, namely that actual effects should

---

[1622] Article L. 420-2, al. 2 of the French Code de Commerce; Article IV.2/1 of the Belgian Code de droit économique. Interestingly, this condition was completely omitted by the President of the Ghent Commercial Court, in one of the rare cases where an abuse of economic dependence was established. See Comm. Gand (réf.), 28 octobre 2020, inéd., R.G. n°A/20/02490, commented in B. Gielen and C. Verdonck, "First Belgian ruling on abuse of economic dependence", 3 December 2020, available at https://www.lexology.com. This condition was however analysed in the French *Apple* case, which is one of the rare French cases where an abuse of economic dependence was established (see Autorité de la concurrence, Decision nº 20-D-04, 16 March 2020). In that case, the *Autorité* ruled that Apple subjected its premium distributors to unfair and unfavourable commercial conditions in comparison with those it imposed to its network of integrated distributors, and that this differential treatment was not objectively justified (see footnote 1614). For the *Autorité*, this had anticompetitive effects as these practices limited the competitive emulation on, and thus the functioning and the structure of, intra-brand competition for Apple products, which could have led to the emergence of new proximity services for consumers; and as these practices led to the weakening of these premium distributors, and in some cases to their eviction from the market (see p. 219-224).

[1623] P. Bougette, O. Budzinski and F. Marty, "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *Ilmenau Economics Discussion Papers No. 119*, 2018, available at http://hdl.handle.net/10419/191022, p. 6.

[1624] F. De Boüard, *La dépendance économique née d'un contrat*, Paris, LGDJ, 2007, p. 298-299; L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, *op. cit.*, p. 171.

[1625] P. Bougette, O. Budzinski and F. Marty, "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *op. cit.*, p. 6.

[1626] M. Bakhoum, "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *op. cit.*, p. 17.

trump formalistic assertions. Depending on the case in question, consumer welfare and the competition process may be negatively affected by (…) economic dependence abuses in several ways".[1627] Notably, the competitive process could be harmed if these abuses of economic dependence undermine the undertakings' possibilities to access the market. Accordingly, such abuses should be sanctioned on the basis of competition law in order to protect the freedom to compete.[1628] In this second perspective, the standard for establishing that there is a likely effect on the functioning or the structure of competition is lower as "intervention is required in order to protect freedom, as an institution, and as an individual economic right".[1629]

This second approach fits more with the two-fold objective of the provisions pertaining to the abuse of economic dependence, as the weaker party is not only protected because it is in a situation of unequal bargaining power, but also because this "protects the competitive process as a whole"[1630] by countering the economic power of some non-dominant undertakings. Indeed, "preserving market access cannot be seen as a non-economic goal of antitrust legislation which can be criticized for an induced trade-off with economic efficiency. Instead, freedom to access the market (contestability) is considered a necessary condition for efficiency and long-run welfare".[1631] Therefore, in light of this potential effect on the competitive process and of the potential negative welfare it might entail, abuses of economic dependence should fall within the scope of competition law.[1632] Of course, the standard should not be so low as to protect free-riding firms.[1633]

b) Application of abuses of economic dependence to data markets?

268. This thesis raises the question of whether the concept of abuse of economic dependence, classically applied to "traditional" resources, could be translated in data markets. Indeed, this could prove to be a valuable alternative in order to deal with refusals, by non-dominant undertakings, to share data with undertakings having a weaker bargaining power.[1634] To illustrate this, two USA cases can be presented.

The first case is *PeopleBrowsr v. Twitter*.[1635] PeopleBrowsr's business model was to analyse Twitter data in order to resell information to clients about consumer's feedback towards products/services and to identify "influencers", via its access to the Twitter "firehose" (all the tweets passing through Twitter on a real-time basis). At one point, Twitter informed

---

[1627] P. Bougette, O. Budzinski and F. Marty, "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *op. cit.*, p. 7.
[1628] *Ibid*., p. 8.
[1629] M. Bakhoum, "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *op. cit.*, p. 17.
[1630] W. Kerber, "Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars", 26 August 2019, available at https://ssrn.com/abstract=3445422, p. 29.
[1631] P. Bougette, O. Budzinski and F. Marty, "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *op. cit.*, p. 8.
[1632] *Ibid*., p. 10.
[1633] M. Bakhoum, "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *op. cit.*, p. 17.
[1634] See *supra* point 260.
[1635] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013.

PeopleBrowsr, and other third party developers, that as of 30 November 2012, it would cut the "firehose" tap and that PeopleBrowsr would have to conclude a contract with one of Twitter's certified data resellers in order to get access to the "firehose" data.[1636] PeopleBrowsr argued that it was "dependent*"* on this access in order to deliver the service it had built, and a San Francisco court issued a temporary restraining order mandating Twitter to temporarily keep providing access to the "firehose" to PeopleBrowsr. Unfortunately, no decision on the merits of the case followed this preliminary injunction as the parties settled the case in 2013, by agreeing that PeopleBrowsr would retain its access to the "firehose" until the end of 2013, and would then have to transition towards access via a certified data reseller in 2014.[1637]

The second case is *hiQ v. LinkedIn*.[1638] hiQ's business model was to provide information to businesses about their workforces based on statistical analysis of publicly available LinkedIn data.[1639] Their "Keeper" product told employers which of their employees presented the greatest risk of being recruited by another company, while their "Skill Mapper" product provided a summary of the workers' skills. After having allowed hiQ's access and use of its data for several years (from 2012 to 2017), LinkedIn sent, on 23 May 2017, a cease and desist letter requesting hiQ to stop accessing its data, and used blocking techniques preventing hiQ from doing so. hiQ complained and argued that its data analytics business was wholly "dependent*"* on the access to that data, and that LinkedIn's decision to block its access to its data had an anticompetitive purpose – namely to monetise this data itself with a competing product – and thus had to be considered as an unfair competition practice. LinkedIn argued that its decision was only motivated by the aim to protect its users' privacy and to preserve their trust, to which hiQ replied that it was only accessing data that users had willingly made public to all. The District Court concluded that hiQ had raised serious questions about whether LinkedIn had unfairly leveraged its power in the professional networking market in order to develop a competing product ("Talent Insights"), and therefore issued a preliminary injunction ordering LinkedIn to stop preventing hiQ's access to the data. This preliminary ruling was confirmed by the Ninth Circuit Court of Appeals, which concluded that hiQ had successfully established that the survival of its business was threatened by LinkedIn's suspension of the access to its data, and that hiQ had thus demonstrated a likelihood of irreparable harm.[1640] However, when ruling on the merits[1641], the District Court ruled that hiQ had failed to properly define the product market and to adequately allege anticompetitive

---

[1636] I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit*., p. 257.
[1637] *Ibidem*.
[1638] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf.
[1639] LinkedIn users can choose to keep their profiles entirely private, or to make them viewable by their direct connections on the site, a broader network of connections, all other LinkedIn members or the entire public (including internet users not registered on LinkedIn). In the case at hand, *hiQ* conducted its business by automatically collecting, harvesting or "scraping" the data from the latter categories of profiles (publicly available LinkedIn profiles).
[1640] United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html.
[1641] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

conduct, but granted hiQ leave to amend its market definition and its anticompetitive claims.[1642]

269. In fact, these two cases present some striking similarities with the *Commercial Solvents*[1643] case presented above.[1644] Indeed, the underlying justification for a competition law intervention is similar, as in all three cases an undertaking active in an upstream market suddenly stopped to supply undertakings active on a downstream market, following the development of its own product/service on that downstream market.[1645] Naturally, the biggest difference is that Commercial Solvents was a dominant undertaking and that the case was thus assessed on the basis of Article 102 TFEU.

PeopleBrowsr v. Twitter and *hiQ v. LinkedIn*, on the other hand, raise the question of whether the refusal, by a non-dominant undertaking benefiting from a "relative or superior market power", to share data with another undertaking, whose commercial activity "depends" on this access, could amount to an abuse of economic dependence. The above overview of the Belgian, German and French law showed that two main conditions for the application of these provisions are common to the three Member States, namely the need to show a state of economic dependence and the need to show an abuse of this state of economic dependence.

1. Assessment of the state of economic dependence

270. The assessment of a state of economic dependence focusses on whether an undertaking is dependent on its bilateral relationship with a non-dominant undertaking in order to operate.[1646] Interestingly, such questions of economic dependence have been evoked in two cases that did not imply questions of data sharing, but which nevertheless involved digital platforms.[1647] Indeed, several French publishers and news agencies complained to the *Autorité de la Concurrence* that Google's implementation of the French Law n° 2019-775 of 24 July 2019, creating a neighbouring right for the benefit of several news agencies and publishers, constituted an abuse of dominant position, as well as an abuse of economic dependence.[1648] Unfortunately, as the French Competition Authority ruled that Google was dominant on the French market for generalised search services, it did not assess the existence of such an

---

[1642] C. Brennan, M. Mantine, G. Stegmaier and G. Vose, "hiQ Labs, Inc. v. LinkedIn Corp.: federal judge dismisses antitrust claims regarding access to data", 1 October 2020, available at https://www.reedsmith.com/en/perspectives/2020/10/hiq-labs-inc-v-linkedin-corp-federal-judge-dismisses-antitrust-claims.

[1643] ECJ, *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18.

[1644] See point 229.

[1645] See *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18, § 25.

[1646] See, for instance, Autorité de la concurrence, Decision n°10-D-08, 3 March 2010, § 165. See also Autorité de la concurrence, Decision n°20-MC-01 (*Syndicat des éditeurs de presse v. Google*), 9 April 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-04/20mc01.pdf, § 179.

[1647] For reflections pertaining to potential cases of "platform dependence", see S. Lee and J. Schißler, "Platform Dependence and Exploitation", *Paper presented at the 14th ASCOLA Conference*, June 2019, available at https://ssrn.com/abstract=3403002.

[1648] Autorité de la concurrence, Decision n°20-MC-01 (*Syndicat des éditeurs de presse v. Google*), 9 April 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-04/20mc01.pdf, § 2.

economic dependence *in casu*.[1649] Similarly, in the context of its investigation against Amazon, the *Bundeskartellamt* considered that it could be relevant to assess small seller's dependence on Amazon's relative market power in order to have access to final consumers, but nevertheless did not investigate this question *in casu*.[1650]

Coming back to the topic of data sharing, on which this thesis focusses, a two-step assessment must be conducted in order to determine whether an access seeker is dependent, in order to conduct its business, on the access to the data of a non-dominant undertaking having a superior market power. First, an objective assessment of the sufficiency of alternatives for any undertaking is necessary. Second, a subjective assessment of the reasonableness to resort to these alternatives for the access seeker must be conducted.

i. Objective assessment of the sufficiency of alternatives for any undertaking

271. The first question is thus whether sufficient alternatives to the data held by the undertaking having superior market power are available to any other undertaking. Said otherwise, it must be questioned whether the access seeker could, in theory, collect that data itself or access it via another undertaking. This first objective assessment is rather similar to the "indispensability" condition of the essential facilities doctrine, which applies to dominant undertakings.[1651] Indeed, according to the French *Autorité de la concurrence* and the German *Bundeskartellamt*, this "indispensability" condition requires to show that "the data owned by the incumbent is truly unique and that there is no [other] possibility for the competitor to obtain the data that it needs to perform its services".[1652]

As a reminder, the "indispensability" condition does not require the demonstration of the absence of "any alternative at all", but rather the absence of "a sufficient alternative for *any* undertaking".[1653] This finding can be derived from the *Bronner* case, where the European Court of Justice held that the access to a facility will not be indispensable if an alternative (even a less advantageous one) can be developed by *any* undertaking other than the dominant undertaking.[1654]. In order for the indispensability of the facility (*in casu* a newspapers' nationwide home-delivery system) to be established, the Court ruled that there must be "obstacles capable of making it impossible, or even unreasonably difficult, for *any* other publisher [to develop a substitute]".[1655]

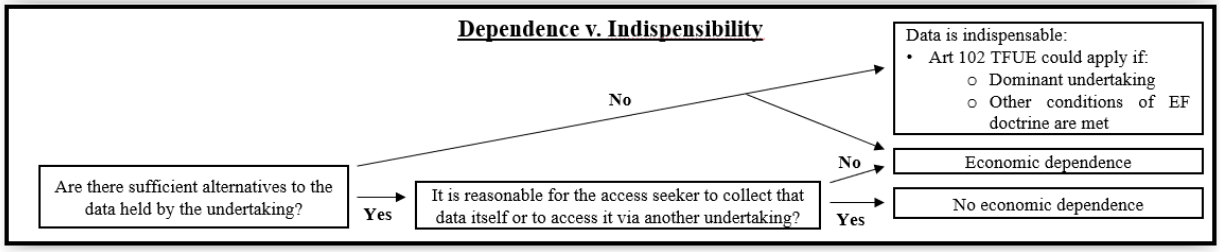
[1649] *Ibid*., § 181.
[1650] I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 45; Bundeskartellamt, *Amazon – Online sales*, 17 July 2019, B2 – 88/18 (case summary available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B2-88-18.pdf?__blob=publicationFile&v=4).
[1651] See points 240 to 244.
[1652] Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data*"*, 10 May 2016, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf, p. 18.
[1653] See point 240.
[1654] ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569, § 43.
[1655] *Ibid*., §44.

272. If it appears from this objective assessment that no sufficient alternatives to the data held by a non-dominant undertaking having superior market power exist for *any* undertaking, it will *de facto* not be reasonable *for the access seeker* to collect that data itself or to access it via another undertaking (subjective assessment of the reasonableness to resort to these alternatives). Therefore, the state of economic dependence will be established. However, if this objective assessment leads to the finding that the data is not indispensable and that there are, in fact, sufficient alternatives to the data, then it is necessary to move on to the second step and to assess, from a subjective point of view, whether it is reasonable *for the access seeker* to collect that data itself or to access it via another undertaking.

ii. Subjective assessment of the reasonableness to resort to these alternatives for the access seeker

273. This subjective assessment is one of the key differences between resorting to provisions of abuse of economic dependence and resorting to Article 102 TFEU, as the latter does not provide such a second step. This is because Article 102 TFEU requires an absolute indispensability, while the provisions forbidding the abuse of economic dependence only require a relative dependence (e.g. the access to the dataset is necessary in order *for the access seeker* to conduct its business, but it might not be necessary for other undertakings).

Figure 11: Comparison between Dependence and Indispensability



Source: T. Tombal, Economic dependence and data access[1656]

If it is reasonable to require the access seeker to collect the data itself or to access it via another undertaking, then it is not in a state of economic dependence. On the contrary, if it is not reasonable, then it should be deemed to be in a state of economic dependence. To assess whether this is reasonable, the technical and economic barriers to this alternative should be considered. This means questioning whether this could be done within a reasonable time frame, on reasonable terms and at reasonable cost.

274. Considering such barriers is not new in the realm of competition law. As indicated earlier, the European Court of Justice held in *Bronner* that, in the context of Article 102 TFEU, there must be "*obstacles* capable of making it impossible, or even unreasonably difficult, for *any other publisher* [to develop a substitute]" (emphasis added).[1657] The Court added that "it is not enough to argue that it is not economically viable by reason of the small circulation of the daily newspaper or newspapers to be distributed. For such access to be

[1656] T. Tombal, "Economic dependence and data access", *IIC*, 2020, Volume 51, Issue 1, p. 83.
[1657] ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569, §44.

capable of being regarded as indispensable, it would be necessary (…) to establish (…) that it is not economically viable to create a second home-delivery scheme (…) with a circulation comparable to (…) the existing scheme".[1658] This finding could be used to assess the existence of economic barriers creating a situation of economic dependence. Naturally, given that the provisions prohibiting the abuse of economic dependence only require a relative dependence, while Article 102 TFEU requires an absolute indispensability, the standard for recognising such an economic barrier should be lower. Thus, the test could be reformulated as follows: Are there economic and technical barriers making it unreasonably difficult for the access seeker (and not for *any* undertaking) to collect the data itself or to access that data via another undertaking? Considering that the assessment of dependence is relative and not absolute, it will be enough to argue that it is not economically viable for the access seeker to do so due to its own limited capacities, rather than having to show that it would not be economically viable for *any* undertaking having the same capacities as the data holder.

275. In the digital economy, such economic and technical barriers could stem from the fact that the undertaking faces high costs to switch away from the non-dominant undertaking towards a substitute.[1659] Such high switching costs can notably derive from the fact that the undertaking has made significant investments to build its technology in a way that complies with the non-dominant undertakings' specifications, and that these investments would be lost ("sunk costs"), implying a need for new investments, if the undertaking wanted to switch to a substitute.[1660] Alternatively, high switching costs can also arise from the fact that any substitute would be far inferior, such as when a non-dominant undertaking is a "gatekeeper" to a specific market segment, because there are few other means of reaching that segment.[1661]

More specifically for data, it should be outlined that access to data relevant for competition is considered as one of the five factors to assess an undertaking's power in a multi-sided market and network.[1662] Therefore, "consumer lock-in"[1663] and "network effects"[1664] could constitute such economic and technical barriers that make an access seeker dependent on another undertaking having relative or superior market power. Indeed, if the users are locked-in the latter's product or service – because no alternative having reached a critical mass of users is available (network effects) – the access seeker will be dependent on this undertaking as it is the only viable connexion to these users. The undertaking having superior market power

---

[1658] *Ibid*., §§ 45-46.

[1659] Expert Group for the Observatory on the Online Platform Economy, "Measurement & Economic Indicators: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports, p. 17.

[1660] *Ibidem*.

[1661] *Ibidem*.

[1662] §18, n°3a of the Gesetz gegen Wettbewerbsbeschränkungen (Act against Restraints of Competition); J. Haucap, "A German approach to antitrust for digital platforms", in *Digital Platforms and Concentration - Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (ed.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 10.

[1663] Consumers are "locked into" a service because no other reasonable alternative, having reached a minimum scale (e.g. having a sufficient minimum number of users), exists.

[1664] Having more costumers provides more data, which allows to improve the product/service. In turn, improving the product/service attracts more consumers that provide additional data, which again allows to improve the product/service, etc.

could thus be a "gatekeeper" of that user data, as the access seeker would not be able to collect the data itself, or to access that data via another undertaking, within a reasonable time frame, on reasonable terms and at reasonable cost.

276. This "gatekeeper" situation was arguably present in the *PeopleBrowsr v. Twitter*[1665] and *hiQ v. LinkedIn*[1666] cases. Indeed, PeopleBrowsr argued that its business-model was dependent on the access to the Twitter "firehose" in order to deliver the service it had built. Indeed, it argued that Twitter's data was unique and essential as tweets provide unique insight about which members of communities are influential and provide unique feedback regarding consumers' reactions to products and brands, and as other social networking sites, such as Facebook, do not provide the same rich set of public data regarding users' sentiments and influence.[1667] The Superior Court of the State of California validated this argument. Similarly, hiQ argued that its data analytics business was wholly dependent on the access to LinkedIn's data, as no viable alternative to LinkedIn's data was available.[1668] Ruling on the preliminary injunction, both the District Court[1669] and the Court of Appeal concurred with hiQ, by holding that there was no equivalent alternative source of data (not even Facebook) and that it would not be reasonable to require hiQ to collect the data itself either, as this would imply a considerable amount of time and expenses for hiQ to fundamentally change the nature of its business.[1670] In light of these examples, it can be argued that, like several other digital platforms, Twitter and LinkedIn might benefit from a form of "gatekeeper power" as they effectively serve as an infrastructure for their specific market segments, because they are in fact "the only real option", which could allow them to extort and extract better terms from undertakings that depend on their infrastructure.[1671]

[1665] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013.

[1666] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

[1667] Declaration of John David Rich in support of plaintiff's application for a temporary restraining order in the case *PeopleBrowsr v. Twitter* in the Superior Court of the State of California, County of San Francisco, November 2012, paras 4-5, available at http://www.scribd.com/doc/114846303/Rich-Declaration-PB-v-TW-Restraining-Order-28-Nov-12, cited in I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition Law and Economics Review*, 2015, Vol. 38, Issue 4, p. 499.

[1668] United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html, p. 13.

[1669] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf.

[1670] United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html, p. 13-14.

[1671] L. Khan, "What makes tech platforms so powerful?", *Digital Platforms and Concentration, Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (ed.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 13-14. See also P. Bougette, O. Budzinski and F. Marty, "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *op. cit.*, p. 14.

277. An additional key factor for this "assessment of reasonableness" test lies in the access seeker's burden of proof, as it has to convince the competition authorities that it is truly dependent on the access because it cannot reasonably collect the data itself or access that data via another mean. To do so, the access seeker has to provide clear explanations about the product/service that it offers (or intends to offer) and the reasons why that data is necessary for its (current or future) business-model.[1672] Indeed, requiring these additional explanations would avoid that these provisions on the abuse of economic dependence are used as proxies for free-riding tactics, which would deter innovation. This implies that access should not be granted to undertakings that simply want to copy the data holder's business model. Rather, access to data through the provisions on the abuse of economic dependence should only be granted if the access seeker offers (or wishes to offer) a different product/service than the one offered by the data holder, or at least a technical improvement of that product/service.[1673]

Arguably, this requirement was satisfied in the *PeopleBrowsr v. Twitter*[1674] and *hiQ v. LinkedIn*[1675] cases. Indeed, PeopleBrowsr's business model was to analyse Twitter data in order to resell information to clients about consumer's feedback towards products/services and to identify "influencers". It therefore did not access Twitter's data in order to copy its business model and to create a similar social network, but rather to provide new added-value services on the basis this data. Similarly, hiQ's business model was to provide information to businesses about their workforces based on statistical analysis of publicly available LinkedIn data, by telling employers which of their employees presented the greatest risk of being recruited by another company and by providing a summary of the workers' skills. Once again, this access to LinkedIn's data was not made to copy its business model and to create a similar professional social network, but rather to provide new added-value services.

2. Assessment of the abuse

278. After having established that the access seeker is in a state of economic dependence towards the data holder, it will be necessary to determine whether the refusal, by the latter, to provide access to the data constitutes an abuse of such economic dependence. This second condition calls for two types of considerations. On the one hand, it is first necessary to demonstrate a conduct that constitutes a potential abuse. On the other hand, the anticompetitive harm deriving from this abuse must be proven.

[1672] Naturally, the access seeker should be careful not to provide too much information, in order to avoid the application of Article 101 TFEU because of a risk of tacit collusion. However, this latter issue could be solved by preventing the data holder's department dealing with the data access request from sharing this specific information with other departments. Moreover, if some of the data to which the access is requested is personal data, providing explanations about the product/service that it intends to offer will also be necessary to comply with the core processing principles of Article 5 of the GDPR, and notably the principle of purpose limitation.

[1673] See, by analogy, the "new product" condition of the essential facilities doctrine: points 249 to 251.

[1674] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013.

[1675] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

i. Demonstrating a conduct that constitutes a potential abuse

279. In Belgian law, Article IV.2/1, 1° CDE explicitly identifies the unlawful refusal to supply as a practice that can be considered as abusive. Similarly, in French law, Article L.420-2, al. 2 of the Code de Commerce provides that a refusal to sell may be abusive. An unlawful refusal to supply/provide access to data to an undertaking which has demonstrated that it is dependent on this access could thus, in certain circumstances, be abusive. The key issue is to determine when such a refusal to share data is "unlawful*"*. Two possible sets of cases should be outlined.

280. In the first set of cases, the access seeker has already developed its product/service on the basis of the access to the data holder's data, and the latter decides to "close the tap" and to no longer share this data (termination of an existing business relationship). The question is whether this refusal to keep sharing the data for the future, while access had been provided in the past which allowed the dependent undertaking to build its product/service, constitutes an unlawful restriction of the latter's possibility to compete in the market, amounting to an abuse. In this regard, it should be noted that the European Commission indicates, in its guidance on abusive exclusionary conducts by dominant undertakings, that terminating an existing business relationship is more likely to be abusive than a *de novo* refusal to supply because of the relationship-specific investments that have already been made.[1676]

Once again, the *PeopleBrowsr v. Twitter*[1677] and *hiQ v. LinkedIn*[1678] cases could arguably be considered as conducts that constitute a potential abuse. Indeed, in both these cases, the data holders let another undertaking develop an added-value service on the basis of the free access to its data, creating the impression that they could create a perennial business-model via this free access. Yet, once Twitter and LinkedIn realised that these services had added-value and that they were dependent on this access, they decided to terminate the existing business relationship. This conduct could potentially be abusive if it generates anti-competitive effects.[1679]

[1676] Communication from the Commission – Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, *OJ C 45*, 24 February 2009, §84.

[1677] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013.

[1678] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

[1679] On this point, see United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html, p. 22-23. However, when ruling on the merits, the District Court ruled that hiQ had failed to substanciate this claim, but granted hiQ leave to amend it (United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020; C. Brennan, M. Mantine, G. Stegmaier and G. Vose, "hiQ Labs, Inc. v. LinkedIn Corp.: federal judge dismisses antitrust claims regarding access to data", *op. cit.*).

281. In the second set of cases, the access seeker has no pre-existing business relation with the data holder, and alleges that it is dependent on the data holder's data to launch a new product/service, which is not a simple copy of the data holder's business model, but rather aims at creating added-value (refusal to supply). Here, there could potentially be an abuse if the undertaking has exceeded the reasonable exercise of its economic freedom and that it could not have refused the access absent the state of economic dependence. To do so, the conduct, *in casu*, of the undertaking having a superior market power towards the dependent undertaking should be compared with the conduct of a similar undertaking operating in a similar market (e.g. in other countries or in markets for similar products/services) where there is no dependence.

For instance, Kerber raises the question of whether the refusal, by car manufacturers, to share vehicle data with independent repairers and providers of complementary services (e.g. on-board applications), while it is shared with official distributors or "certified" service providers, could amount to an abuse of economic dependence.[1680] He points out, in this regard, that "it can be argued that under certain conditions firms on aftermarkets and in IOT-contexts with several stakeholders that need access to the same data for offering valuable services might claim access to the data that one stakeholder holds exclusively".[1681] Moreover, and because refusal to share data might not fit perfectly within the four traditional case groups of abuse of economic dependence identified earlier[1682], Kerber suggests to develop a new case group for situations where data holders have a *de facto* exclusive control on the access to certain data sources and where they might abuse from the state of economic dependence of other firms who need this access in order to offer products or services to the users.[1683] To support this, Kerber relies on a report for the German Federal Ministry for Economic Affairs and Energy, which indicated that:

> *"*It may be useful to clarify in § 20 para. 1 GWB that a relevant form of dependence may also result from an undertaking being dependent, in order to achieve a substantial value creation within a value creation network, on access to automatically generated machine or service usage data that is exclusively controlled by another company; and *denial of access to data can constitute an unreasonable exclusionary conduct, even if markets for such data do not yet exist"* (emphasis added).[1684]

[1680] W. Kerber, "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *JIPITEC*, 2018, Issue 9, p. 329.
[1681] *Ibidem*.
[1682] See point 263.
[1683] W. Kerber, "Data-sharing in IoT Ecosystems from a Competition Law Perspective", *op. cit*., p. 32. For a more thorough analysis of how this could be applied to the automotive sector, where the car manufacturers might have such a *de facto* exclusive control, see p. 28-35.
[1684] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 6. For a more extensive discussion of this point, see H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, *op. cit*., p. 47-57 and 156. See also the Governmental draft bill (GWB-Digitalisierungsgesetz) for the 10th amendment to the Competition Act of 9 September 2020: Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen, available at https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/gwb-digitalisierungsgesetz.html.

Indeed, the benefit of the protection of §20 GWB is not limited to undertakings engaged in existing agreements or business relations, but may extend to undertakings willing to enter into such agreements or relations.[1685] Accordingly, the authors of the report saw great potential in a broader application of §20 GWB, which "can become an effective instrument for closing persisting gaps in controlling abusive behaviour in view of the special challenges facing the digital economy".[1686] As a result of these arguments, the tenth amendment to the German Competition Act, namely the GWB Digitalisation Act ("GWB-Digitalisierungsgesetz")[1687], included a new paragraph (1a) in §20 GWB, which provides that:

> "A dependency pursuant to paragraph 1 may also result from the fact that a company is dependent on access to data controlled by another company for its own activities. The denial of access to such data for a reasonable fee may constitute an unreasonable impediment under paragraph 1 in conjunction with § 19(2)(1). This shall also apply if a business transaction has not yet been opened for this data".[1688]

Once again, the importance of the access seeker's explanations about the product/service that it intends to offer, and about the reasons why that data is necessary to offer that product/service, will be paramount in order to avoid free-riding tactics that would deter innovation.

ii. Demonstrating the anticompetitive harm deriving from this abuse

282. Additionally, the anticompetitive harm deriving from this abuse must be proven. As discussed above[1689], the "freedom to compete approach" of the economic role of competition law fits more with the two-fold objective of the provisions pertaining to the abuse of economic dependence, as the weaker party is not only protected because it is in a situation of unequal bargaining power, but also because this "protects the competitive process as a whole"[1690] by countering the economic power of some non-dominant undertakings. Indeed, "freedom to access the market (contestability) is considered a necessary condition for efficiency and long-run welfare".[1691] Abuses of economic dependence might thus be

---

[1685] L. Feteira, *The Interplay between European and National Competition Law after Regulation 1/2003*, *op. cit.*, p. 152.

[1686] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 1.

[1687] See Bundeskartellamt, "Amendment of the German Act against Restraints of Competition (Press release)", 19 January 2021, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html. The full text, in German, of the GWB-Digitalisierungsgesetz is available at https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s0002.pdf%27%5D__1612262835179.

[1688] Author's own translation.

[1689] See *supra* points 266 and 267.

[1690] W. Kerber, "Data-sharing in IoT Ecosystems from a Competition Law Perspective", *op. cit.*, p. 29.

[1691] P. Bougette, O. Budzinski and F. Marty, "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *op. cit.*, p. 8.

sanctioned in order to protect the freedom to compete, as an institution, and as an individual economic right.[1692]

The first set of conducts outlined above (termination of an existing business relationship), can indeed have anticompetitive effects. To illustrate this, the *PeopleBrowsr v. Twitter*[1693] and *hiQ v. LinkedIn*[1694] cases should once again be outlined. In *PeopleBrowsr*, Twitter's conduct might have been considered as anticompetitive, as it can arguably be defined as a "leveraging" behaviour by which Twitter intended to foreclose competition in this downstream analysis market to the benefit of its certified resellers.[1695] Additionally, it could also be argued that Twitter's conduct was anticompetitive as it waited for a data recipient, *in casu* PeopleBrowsr, to show the lucrative nature of a market based on the "firehose" data analysis before reserving that market to its certified data resellers.[1696] Similarly, LinkedIn's conduct does tend to indicate an anticompetitive "leveraging" behaviour by which it intended to foreclose competition in the downstream analysis market by developing a competing product after having waited for a data recipient, *in casu* hiQ, to show the lucrative nature of a such a data analysis market.[1697] In both of these cases, it seemed necessary to protect the access seekers' freedom to compete.

Similarly, the second set of conducts outlined above (refusal to supply), might also have anticompetitive effects as there might be cases where the refusal to share data unlawfully restricts the access seeker's possibility to compete in the market. In this regard, the European Commission's expert report on "Competition Policy for the digital era" outlined that:

> "[W]here a machine producer enjoys some degree of market power, or even just bilateral power, the bargaining power of a machine user may not suffice. A number of experts and industry participants argue that exclusive control over machine usage data then leads to the foreclosure of secondary markets and *may significantly reduce the*

[1692] M. Bakhoum, "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *op. cit.*, p. 17.

[1693] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013.

[1694] United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

[1695] I. Graef, S. Wahyuningtyas and P. Valcke, "Assessing data access issues in online platforms", *Telecommunications Policy*, 2015, Vol. 39, p. 384–385; I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit*., p. 257.

[1696] Z. Abrahamson, "Essential Data", *The Yale Law Journal*, 2014, vol. 124, n° 3, p. 874, cited in I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit.*, p. 257.

[1697] See United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html, p. 22-23. However, when ruling on the merits, the District Court ruled that hiQ had failed to substantiate this claim, but granted hiQ leave to amend it (United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020; C. Brennan, M. Mantine, G. Stegmaier and G. Vose, "hiQ Labs, Inc. v. LinkedIn Corp.: federal judge dismisses antitrust claims regarding access to data", *op. cit*.).

contestability of a machine producer's position on the primary market, *due to a data-driven lock-in of machine users*" (emphasis added).[1698]

3. Potential remedy and potential adaptation of EU competition law

283. If the conditions identified above are fulfilled, the provisions prohibiting the abuse of economic dependence could theoretically be applied to the refusal to share data. Quite logically, a potential remedy would then be to impose on the non-dominant undertaking an obligation to share (some of) its data with the access seeker. This requires to determine the categories of data potentially covered by the sharing remedy. Indeed, depending on this scope, the consequences for the non-dominant data holder, and for the data subjects in case personal data are involved, could vary greatly. As the determination of the categories of data that should be covered by such a compulsory B2B data sharing remedy implies overarching considerations equally applicable to the different types of competition law infringements analysed in this thesis, these will be addressed in a specific section (Section D).

284. Finally, it is fundamental to underline that the above analysis has been conducted on the basis of the national law of three Member States, as there is no harmonisation of the provisions pertaining to the abuse of economic dependence in the EU.[1699] In order to avoid national law discrepancies on how these issues are handled in the internal market, the European Commission could consider the adoption of an abuse of economic dependence provision at the EU level, that would allow to deal, in specific cases, with refusals by non-dominant undertakings to share data. Together with a lowered threshold of application of the essential facilities doctrine for refusals, by dominant undertakings, to share data[1700], this could constitute a welcome evolution of the European competition framework in order to tackle one of the two core data market failures presented above, namely data concentration.[1701]

Indeed, adopting an abuse of economic dependence provision at the EU level, and lowering the threshold of the essential facilities doctrine, should not be seen as mutually exclusive evolutions, but rather as complementary initiatives to remedy this data concentration market failure. A competition intervention based on the essential facilities doctrine allows to tackle, through a single action, more systemic market failures in order to benefit a broad number of downstream competitors. On the other hand, competition interventions based on abuse of economic dependence considerations take, by nature, place in more bilateral scenarios, and thus do not enable to remedy a systemic market failure through a single action. Moreover, the threshold for finding an abuse of economic dependence is easier to meet than the threshold of the essential facilities doctrine, and this provision could potentially be applied to a broader number of undertakings, as the demonstration of a dominant position of the data holder is not required. Accordingly, these two courses of action are complementary, as an adapted essential

---

[1698] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 88.
[1699] For an overview of all of the EU Member States that have such provisions against the abuse of economic dependence see: College of Europe, "Study on the impact of national rules on unilateral conduct that diverge from Article 102 of the Treaty on the Functioning of the European Union (TFEU) – Final Report", 21 November 2012, available at https://ec.europa.eu/competition/calls/tenders_closed.html.
[1700] See points 252 to 258.
[1701] See points 78 to 83.

facilities doctrine could be used to remedy systemic market failures that result from the conduct of a circumscribed number of dominant actors, while competition interventions based on abuse of economic dependence considerations could be used against a broader amount of non-dominant undertakings, in order to remedy more specific market failures deriving from the dependence of certain undertakings on another one. They would thus both contribute to tackling data concentration market failures, but would be resorted to in different scenarios. The other core data market failure, namely data conglomeration and domino effects[1702], on the other hand, could be addressed through merger regulation, to which this thesis now turns.

[1702] See points 84 and 85.

Section C. Input foreclosure in vertical mergers

285. As outlined above[1703], network effects and economies of scope, scale and speed in data may not only protect large data holders in their core data driven markets, but they may also be leveraged by these undertakings to expand and strengthen their position in a *connected market*.[1704] If these connected markets' dynamics are combined with the first mover advantage outlined above[1705], this could lead to a *domino effect*, i.e. "a first mover in market A can leverage its dominant position, which comes with an advantage on user information, to let connected market B tip, too, even if market B is already served by traditional incumbent firms".[1706] In turn, this could lead to successive market tipping in several connected markets[1707], and to the establishment of digital conglomerates.[1708]

286. Although these conglomerates could be pro-competitive, they could also generate market failures (e.g. raise entry barriers for innovative entrants) and long-term competitive advantages, which could have a negative impact on the contestability of these markets.[1709] Moreover, the conglomerate could also foreclose competition on some of the markets where it is active if these markets depend on the access to a key resource, such as specific types of data, produced on a primary market where the conglomerate is also active and dominant, and if the conglomerate refuses to share this resource with its competitors and reserves its use for itself.[1710] This is where the "input foreclosure" theory could potentially come into play, in order to prevent vertical mergers from leading to such a situation. The application of this theory to "traditional" markets will first be briefly presented (a), before questioning whether it could be applied to "data foreclosure" (b). Then, the complex issue of the acquisition of "nascent innovative players"[1711] will be briefly presented (c).

[1703] See points 84 and 85.

[1704] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2-3; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 56; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 19.

[1705] See points 79 and 80.

[1706] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2-3.

[1707] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 71.

[1708] See *supra* point 84. See also T. Eisenmann, G. Parker and M. Van Alstyne, "Platform Envelopment", *Strategic Management Journal*, 2011, Vol. 32(12), p. 1270–1285; D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", December 2019, available at https://ssrn.com/abstract=3504025; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *CERRE Report*, March 2019, available at http://www.crid.be/pdf/public/8377.pdf, p. 4 and 11. For a discussion of the "killer acquisitions" issue, see p. 21-23.

[1709] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit..*, p. 14; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 55.

[1710] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit..*, p. 18-19.

[1711] This expression is preferred to the more broadly used expression "killer acquisition" as, in fact, large data holders rarely simply acquire a potential competitor in order to "kill" its activities (like in the pharma sector), but rather often develop it in order to reinforce their position on the market or on a neighbouring market, as illustrated by Google's acquisition of YouTube, or by Facebook's acquisitions of Instagram and WhatsApp (see Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 10).

a) The traditional "input foreclosure" theory

287. While vertical mergers do not lead to the elimination of direct competitors, and might even lead to an improvement of competition in cases where the merged entity's competitors are already vertically integrated, these mergers can nevertheless create foreclosure risks.[1712] One of these risks is downstream foreclosure, namely a situation in which the merged entity decides to no longer supply an important input[1713] to its competitors in the downstream market (or decides to raise the price or reduce the quality of this input for these competitors) – while this input was supplied to them by the merging party operating on the upstream market prior to the merger –, in order to advantage its own downstream operations after the merger.[1714] For instance, in the *TomTom/TeleAtlas* merger[1715], the Commission expressed concerns that the merged entity would deny supplying downstream competitors in the portable navigation system market with digital maps.[1716]

According to the Commission's guidelines on non-horizontal mergers[1717], in order to establish such an input foreclosure, it is not needed to demonstrate that any competitor would be forced to leave the market, but rather solely to demonstrate that this would entail higher prices for consumers.[1718] In order to do so, the merged entity's ability to foreclose access to the input (significant degree of market power)[1719], its incentive to foreclose (the foreclosure would be profitable)[1720], and the overall likely impact on effective competition (increased rivals' costs or entry barriers)[1721] must be assessed.[1722] Naturally, likely efficiencies deriving from the merger will also have to be assessed.[1723] A balance will thus have to be found between the market efficiencies and deficiencies that may result from the vertical merger.

For instance, the Commission cleared the *TomTom/TeleAtlas* merger[1724] after concluding that the merged entity would not have been able to limit its competitors' access to the input (the digital maps) nor to increase the costs of the access to the input, due to the presence of an upstream competitor, and that it would have had no incentive to foreclose the access to the

---

[1712] D. Geradin, A. Layne-Farrar and N. Petit, *EU Competition Law and Economics*, Oxford, Oxford University Press, 2012, p. 514.
[1713] An input will be important if, for example, it "represents a significant cost factor relative to the price of the downstream product (…) [or if it is] a critical component without which the downstream product could not be manufactured or effectively sold on the market, or [if it represents] a significant source of product differentiation for the downstream product, [or if] the cost of switching to alternative inputs is relatively high" (European Commission, Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings, *OJ C 265/6*, 18 October 2008, § 34).
[1714] D. Geradin, A. Layne-Farrar and N. Petit, *EU Competition Law and Economics*, *op. cit.*, p. 514.
[1715] European Commission, *TomTom/TeleAtlas*, 14 May 2008, case M.4854.
[1716] D. Geradin, A. Layne-Farrar and N. Petit, *EU Competition Law and Economics*, *op. cit.*, p. 500.
[1717] European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit*.
[1718] *Ibid*., § 31; R. Whish and D. Bailey, *Competition Law*, 7th ed., Oxford, Oxford University Press, 2012, p. 878.
[1719] European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit*., §§ 33-39.
[1720] *Ibid*., §§ 40-46.
[1721] *Ibid*., §§ 47-51.
[1722] R. Whish and D. Bailey, *Competition Law*, *op. cit*., p. 878.
[1723] *Ibidem*; European Commission, European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit*., §§ 52-57.
[1724] European Commission, *TomTom/TeleAtlas*, 14 May 2008, case M.4854.

input because the additional sales of portable navigation systems would not have compensated the loss of revenue from the sales of digital maps to competitors.[1725]

b) Application to "data foreclosure"?

288. It is worth questioning whether this input foreclosure theory could be applied to data, in situations where a merged entity might have the possibility to decide to no longer provide access to (or to raise the price or reduce the quality of) important data to its competitors in the downstream market after the merger.

289. In order to do so, the merged entity's ability to foreclose access to the data would first have to be demonstrated, in light of the merged entity's "significant degree of market power" on the upstream market.[1726] In this regard, it must be reminded that the economic characteristics of data benefit large incumbent data holders who have access to more (recent) data than their competitors[1727], and lead to market concentration.[1728] Indeed, data driven markets have a natural tendency to tip towards monopolisation.[1729] Moreover, because such situation is persistent once the market has tipped, even in dynamic high-tech markets, there is a strong *first-mover advantage*.[1730] Therefore, if the merged entity has benefited from such first-mover advantage and market tipping dynamics in order to gain a stronghold on the upstream market, it could be considered as benefitting from a "significant degree of market power".

Such a finding will, however, be function of the determination of the scope of the data market at hand. Yet, market definition is a complex task in the digital environment.[1731] A key consideration, in this regard, will be to determine whether there are substitutes to the merged entity's data on the upstream market, which could be used by its competitors on the downstream market in case of a foreclosure of access to the upstream data.[1732] Indeed, as outlined by the European Commission in the *TomTom/TeleAtlas* merger[1733], the merged entity will not be able to limit its competitors' access to the input, nor to increase the costs of the

---

[1725] A. Jones and B. Sufrin, *EU Competition Law. Text, Cases, and Materials*, 4th ed., Oxford, Oxford University Press, 2011, p. 951.

[1726] European Commission, European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit.*, §§ 33-39.

[1727] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 3 and 19-24.

[1728] See Part I, Chapter 2, Section B, c), 1. "Data collection and production incentives". M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*, p. 336.

[1729] See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf, p. 6-9; J. Prüfer and C. Schottmüller, "Competing with Big Data", *TILEC Discussion Paper No. 2017-006 and CentER Discussion Paper No. 2017-007*, February 2017, available at https://pure.uvt.nl/ws/portalfiles/portal/15514029/2017_007.pdf, p. 2.

[1730] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2.

[1731] See point 258. On the complexity of market definition in the digital environment, see also I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition Law and Economics Review*, 2015, Vol. 38, Issue 4, p. 473–506; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 42-50.

[1732] See, by analogy, G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *European Competition Journal*, 2017, Issue 13, Vol. 2-3, p. 273.

[1733] European Commission, *TomTom/TeleAtlas*, 14 May 2008, case M.4854.

access to the input, if there are sufficiently strong upstream competitors that offer a substitutable input.[1734]

Demonstrating the absence of such viable substitute data sources could be a significant hurdle to overcome. For instance, the European Commission has affirmed, in its *Google/DoubleClick* merger decision, that Google and DoubleClicks' competitors could purchase data on users' search and web-browsing behaviour from third parties such as other major web publishers, internet service providers or portals.[1735] Similarly, in its *Facebook/WhatsApp* merger decision, it held that a wide number of undertakings, which are not controlled by Facebook (Google, Apple, Amazon, eBay, Microsoft, Twitter…), collected sizeable amounts of user data that could be used by competitors as alternatives to Facebook's data for targeted advertising purposes.[1736]

Nevertheless, it is interesting to point out that, in its *Microsoft/LinkedIn* decision, the European Commission outlined that, in theory, refusals, by the merged entity, to share data with competitors on the downstream market may "increase barriers to entry/expansion in the market for actual or potential competitors, which may need this data to operate on this market".[1737] Yet, when assessing whether this concern was established *in casu*, the European Commission concluded, like in the *Facebook/Whatsapp* case, that several other undertakings collected sizeable amounts of user data that could be used by competitors as alternatives to the merged entity's data for targeted advertising purposes.[1738] The European Commission also reached a similar conclusion in its *Apple/Shazam* merger decision, where it held that "it would be unlikely that the merged entity would have the ability to foreclose competing providers of digital music streaming apps even if Shazam's data would be integrated into Apple's dataset".[1739]

On the contrary, in the *Thomson/Reuters* merger case, the European Commission did express concrete concerns that the merging entities' competitors would not have sufficient alternatives to access necessary financial information products after the merger, and that this could significantly reduce competition "in the markets for the distribution of aftermarket broker research reports, of earning estimates, of fundamental financial data of enterprises and of time series of economic data".[1740] To alleviate these concerns, the merging parties committed to share copies of the databases containing such financial information products with competitors

---

[1734] A. Jones and B. Sufrin, *EU Competition Law. Text, Cases, and Materials*, *op. cit*., p. 951.
[1735] European Commission, *Google/DoubleClick*, 11 March 2018, case M.4731, §§ 269-272 and 365; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 38.
[1736] European Commission, *Facebook/WhatsApp*, 3 October 2014, case M.7217, §§ 187-190; G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *op. cit.*, p. 271; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 39.
[1737] European Commission, *Microsoft/LinkedIn*, 6 December 2016, case M.8124, § 179; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 39.
[1738] European Commission, *Microsoft/LinkedIn*, 6 December 2016, case M.8124, § 180; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 40.
[1739] European Commission, *Apple/Shazam*, 6 September 2018, case M.8788, § 340; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 40.
[1740] European Commission, *Thomson Corporation/Reuters Group*, 19 February 2008, case M.4726, §§ 151-156; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 39.

that would request it.[1741] Similarly, in the *Google/Fitbit* merger, the merging parties committed to maintain the access, for software applications, to the users' health and fitness data through the Fitbit Web API, without charges and provided that the users have consented to this.[1742]

According to Hoffmann and Johannsen, the European Commission's decisional practice analysing the merged entity's ability to foreclose access to the data has been too short-sighted, as it has been centred on the overall availability of data post-merger (absolute foreclosure theory of harm), and this explains why, in light of data's non-rivalrous and ubiquitous nature, it rarely expressed competition concerns.[1743] Yet, because data is a general-purpose good[1744], and because the competitive advantages that the merged entity could derive from the data will not necessarily be limited to one market[1745], the European Commission should consider the fact that "additional competition concerns may arise when the accumulation of large piles of data from a huge multitude of sources by digital conglomerates leads to such an advantage that competitors will not be able to match anymore, increasing the likelihood of further anti-competitive strategies (relative foreclosure theory of harm)".[1746] If the Commission were to adopt such a relative foreclosure theory of harm instead, this could increase the cases in which the merged entity's ability to foreclose access to the data could be established, as it could also encompass cases in which "the accumulation of data generated by a merger gives the merged entity such a large advantage that regardless of having access to specific information no one will have sufficient incentives to challenge the market(s) in which the merged entity is active".[1747] For Hoffmann and Johannsen, the justification of the need, for the European Commission, to adopt such a "relative foreclosure theory of harm" in digital markets could be based "on the assumption that data-induced economic power can generate a greater advantage than it would have generated in a pre-digital era. This advantage is not related to a specific relevant market, but to the whole conglomerate's digital ecosystem".[1748]

290. Secondly, the merged entity's incentive to foreclose the access to the data for competitors in the downstream market, as this would be profitable for it, will have to be assessed.[1749] In this regard, it must be reminded that network effects and economies of scope, scale and speed in data, which the merged entity benefits from on the upstream market, may be leveraged by the merged entity to expand and strengthen its position in the downstream

---

[1741] European Commission, *Thomson Corporation/Reuters Group*, 19 February 2008, case M.4726, § 480; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 39.
[1742] European Commission, *Google/Fitbit*, 17 December 2020, case M.9660; European Commission, "Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions", *Press release n° IP/20/2484*, 17 December 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2484.
[1743] J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data: On Data-specific Theories of Harm and Remedies", *Max Planck Institute for Innovation and Competition Research Paper No. 19-05*, 31 May 2019, available at https://ssrn.com/abstract=3364792, p. 1 and 7.
[1744] See point 52.
[1745] See points 285 and 286.
[1746] J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*, p. 1.
[1747] *Ibid*., p. 7. For more details, see p. 7-32.
[1748] J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*, p. 22.
[1749] European Commission, European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit.*, §§ 40-46.

market, if such data turns out to be a valuable input to improve the goods or services offered on that downstream market (*connected markets* dynamic).[1750] In fact, this could even reinforce the merged entity's position in the upstream market, if the data gathered on the downstream market is a valuable input to improve the goods or services offered on the upstream market.[1751] As this would be profitable for the merged entity, it could be argued that it has an incentive to foreclose the access to the data for competitors in the downstream market.

291. Thirdly, the overall likely impact of the foreclosure on effective competition must be assessed.[1752] This will require to find an appropriate balance between the pro-competitive effects of the merger (notably in terms of the efficiencies that it might entail), and its potential anti-competitive effects. Regarding the latter, it should be reminded that the first-mover advantage, market tipping and connected markets dynamics mentioned above could lead to a *domino effect*. Any efficiencies deriving from the merger will thus have to be balanced with the risks that this could entail. [1753]

292. In light of the above, this thesis argues that the "input foreclosure" theory could potentially have been applied to Twitter and LinkedIn in the two cases mentioned above in the analysis of the abuse of economic dependence[1754], had the circumstances of these cases been slightly different. Indeed, had Twitter/LinkedIn merged with a downstream data analytics company, the issue could have been raised of whether this merger could have led to an input foreclosure if Twitter/LinkedIn had decided to no longer provide access (or to raise the price or reduce the quality of) to its important data[1755] to its competitors in the downstream data analysis market after the merger. In light of the merged entity's ability to foreclose access to the input (significant degree of market power of Twitter/LinkedIn as no viable alternative to Twitter/LinkedIn's data was available)[1756], of its incentive to foreclose (the foreclosure would be profitable as PeopleBrowsr/hiQ had demonstrated the lucrative nature of this downstream

---

[1750] See point 285. J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2-3; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 56; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 19.

[1751] J. Prüfer and C. Schottmüller, "Competing with Big Data", *op. cit.*, p. 2-3.

[1752] European Commission, European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit.*, §§ 47-51.

[1753] R. Whish and D. Bailey, *Competition Law*, 7th ed., Oxford, Oxford University Press, 2012, p. 878; European Commission, European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit.*, §§ 52-57.

[1754] Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020. See *supra* point 268.

[1755] An input will be important if, for example, it "represents a significant cost factor relative to the price of the downstream product (…) [or if it is] a critical component without which the downstream product could not be manufactured or effectively sold on the market, or [if it represents] a significant source of product differentiation for the downstream product, [or if] the cost of switching to alternative inputs is relatively high" (European Commission, European Commission, Guidelines on the assessment of non-horizontal mergers, *op. cit.*, § 34).

[1756] See point 276.

market)[1757], and of the overall likely impact on effective competition (increased costs for PeopleBrowsr/hiQ to access the data)[1758], this might have been a potential case of application of the theory.

293. If the conditions of the "input foreclosure" theory are fulfilled, a potential remedy would then be to subject the validation of the merger to the merging entity's commitment to guarantee that it will share (some of) its important data with competitors in the downstream market at a reasonable price, as in the *Thomson/Reuters* case mentioned above.[1759] Indeed, sharing specific types of data could attenuate the anti-competitive effects of conglomerates by allowing competition to emerge and ensuring market contestability, as "compulsory access will allow entrants, on the one hand, to enjoy the same economies of scope in product development than the [merged] firm and, on the other hand, to generate demand-side synergies of similar magnitude when integrating the key [data] in their product ecosystems".[1760] Due to overarching considerations with the two previous Sections, the delineation of the categories of data that should fall within such a commitment to share data will be addressed in Section D.

Nevertheless, it must be kept in mind that, in light of the dynamic nature of data markets, which makes their evolution somewhat unpredictable, it could be difficult for the European Commission to assess whether the proposed data sharing commitment will comprehensively eliminate the competition concerns.[1761] To alleviate this predictability issue, the use of "conditional remedies" could be envisaged, which are "remedies which only apply under certain circumstances, i.e. certain events or a certain timeframe[1762]".[1763] Indeed, this would ease the complex balancing between under- and over-enforcement in dynamic markets. Obviously, in light of the principle of legal certainty, the conditions in which the (data sharing) remedy would have to be "activated" will have to be clearly defined from the outset and will have to be as operable as possible.[1764]

Naturally, commitments to share data are not the only available remedies, and other avenues are suggested in the legal doctrine, such as the imposition of non-discrimination obligations, structural breakups or preventing the merged entity from combining the datasets produced on the upstream and downstream markets (data siloing[1765]).[1766] Finally, the competition authority

---

[1757] See point 282.
[1758] See point 268.
[1759] See point 289. European Commission, *Thomson Corporation/Reuters Group*, 19 February 2008, case M.4726, § 480; R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 39. See also J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*, p. 56-62.
[1760] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*., p. 30.
[1761] J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*, p. 53.
[1762] F. De Bure and L. Bary, "Disruptive Innovation and Merger Remedies: How to Predict the Unpredictable?", *Concurrence*, September 2017, N° 3-2017, Art. N° 84407, p. 7.
[1763] J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*, p. 53.
[1764] *Ibid*., p. 55.
[1765] See, in this regard, the commitments proposed by Google in the *Google/Fitbit* merger: European Commission, *Google/Fitbit*, 17 December 2020, case M.9660; European Commission, "Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions", *Press release n° IP/20/2484*, 17 December 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2484.

could also decide to block the merger due to the competition concerns that a data combination would entail, but this has never been done so far, at the European level, by the European Commission.[1767] As this thesis focusses on compulsory B2B data sharing, these alternatives will not be further detailed here.

c) The particular issue of the acquisition of "nascent innovative players"

294. Finally, to conclude this Section pertaining to mergers, the complex issue of the acquisition of "nascent innovative players"[1768] will be briefly presented. Indeed, in the digital economy, large data holders often acquire such "nascent innovative players". For instance, since 2008, Google has acquired 168 undertakings (notably Waze, YouTube or DoubleClick that were potential competitors), Facebook has acquired 71 undertakings (including Instagram and WhatsApp that were also arguably potential competitors), and Amazon has acquired 60 undertakings, which is a respective average of around 15, 6 and 5 acquisitions per year.[1769]

The effects on competition of such acquisitions are challenging to assess.[1770] On the one hand, such acquisitions could pursue legitimate goals, such as acquiring specific human or technical competences that are precious and rare, or acquiring an extensive potential user-base.[1771] Moreover, they might be efficient and beneficial for both parties, as these "nascent innovative players" might lack the sufficient (human and technical) skills and resources to develop their innovative ideas themselves.[1772] Indeed, an innovative idea created by a "nascent innovative

---

[1766] On these alternative remedies, see *inter alia*, J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*; United States House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets – Majority Staff Report and Recommendations", 2020, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf; J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*; OECD, "Lines of Business Restrictions – Background note", 8 June 2020, DAF/COMP/WP2(2020)1, available at https://one.oecd.org/document/DAF/COMP/WP2(2020)1/en/pdf; S. Besen and P. Verveer, "Competition and data: Potential remedies", *Wake Forest Journal of Business and Intellectual Property Law*, 2021, Volume 21, Number 2, p. 103-143. See also Articles 3.8, 5 and 6 of the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final.

[1767] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 38. For such cases of merger blockings in the United States, see S. Besen and P. Verveer, "Competition and data: Potential remedies", *op. cit.*, p. 116-126.

[1768] This expression is preferred to the more broadly used expression "killer acquisition" as, in fact, large data holders rarely simply acquire a potential competitor in order to "kill" its activities (like in the pharma sector), but rather often develop it in order to reinforce their position on the market or on a neighbouring market, as illustrated by Google's acquisition of YouTube, or by Facebook's acquisitions of Instagram and WhatsApp (see Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 10).

[1769] Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 9; Lear, "Ex-post Assessment of Merger Control Decisions in Digital Markets – Final Report", 9 May 2019, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803576/CMA_past_digital_mergers_GOV.UK_version.pdf, p. ii.

[1770] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 4.

[1771] Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 9; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 4.

[1772] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 21.

player" might be dependent on the mobilisation of a large data holder's skills and resources in order to blossom into a product/service that is picked-up by a large user-base, and it is possible that the "nascent innovative player" would have never reached this result on its own. In this regard, some "nascent innovative players" might even never really intend to bring a new/disruptive product/service on the market themselves, which would compete with the large data holder's product/service, but rather simply aim at being acquired by the said large data holder.[1773]

On the other hand, acquisitions of "nascent innovative players" could also entail anti-competitive effects, if large data holders systematically identify and acquire smaller innovative players, which could become potential rivals in the future.[1774] In fact, it is extremely complex for competition authorities to identify such practices, as such potential rivals will often emerge in niche markets that may not necessarily clearly overlap with the markets on which the acquiring large data holder is active.[1775] Conversely, the troves of data that these large data holders control across several markets in their ecosystem allow them to identify early on potential threats that might emerge on niche markets.[1776]

295. That being said, such acquisitions will, in practice, only be subject to a competition assessment (for instance in order to determine whether they could lead to an "input foreclosure") if they have been notified to a competition authority, which will only occur if certain thresholds are met. As this thesis analyses compulsory B2B data sharing initiatives in the European legal framework, it will focus on the European Union mergers' thresholds enshrined in the "Merger Regulation".[1777] In this regard, Article 1.2 of the Merger Regulation provides that a merger has an EU dimension if:

> "(a) the combined aggregate worldwide turnover of all the undertakings concerned is more than EUR 5 000 million; and
>
> (b) the aggregate Community-wide turnover of each of at least two of the undertakings concerned is more than EUR 250 million,
>
> unless each of the undertakings concerned achieves more than two-thirds of its aggregate Community-wide turnover within one and the same Member State".

Article 1.3 of the Merger Regulation adds that a merger that does not meet the thresholds contained in Article 1.2 will nevertheless have an EU dimension if:

> "(a) the combined aggregate worldwide turnover of all the undertakings concerned is more than EUR 2 500 million;

[1773] *Ibidem*.
[1774] Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 10; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 4
[1775] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*", op. cit.*, p. 5.
[1776] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 21.
[1777] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings, *OJ L 24/1*, 29 January 2004.

(b) in each of at least three Member States, the combined aggregate turnover of all the undertakings concerned is more than EUR 100 million;

(c) in each of at least three Member States included for the purpose of point (b), the aggregate turnover of each of at least two of the undertakings concerned is more than EUR 25 million; and

(d) the aggregate Community-wide turnover of each of at least two of the undertakings concerned is more than EUR 100 million,

unless each of the undertakings concerned achieves more than two-thirds of its aggregate Community-wide turnover within one and the same Member State".

296. Therefore, only the acquisitions that meet these "EU dimension" thresholds will have to be notified to the European Commission prior to their implementation.[1778] Yet, quite often, the "nascent innovative players" that are acquired by large data holders have not yet monetised their innovation, and, in such cases, the value of the target company is not reflected by the turnover it achieves and the notification thresholds are usually not reached.[1779] This is because, in such digital markets, "nascent innovative players" often prioritise the growth of their user-base, in order to be the first to reap network effects and to attempt to make the (niche) market tip in their favour, rather than the growth of their turnover and profit.[1780]

As a result, only a handful of these acquisitions have been substantially scrutinised by competition authorities[1781], while some others, which might have a significant impact on competition, have escaped review by competition authorities, in particular in the digital sector.[1782] For instance, Facebook's 19 billion dollars acquisition of Whatsapp was only notified to the European Commission[1783] because market share thresholds were met in several Member States (Spain, Cyprus, United Kingdom), in which the transaction was notifiable and for which the competition authorities accepted to refer the case to the European Commission.[1784]

297. Accordingly, growing calls for the adaptation of these notification thresholds have been made, and several alternatives have been suggested. For instance, the French *Autorité de la Concurrence* has suggested "the introduction of an obligation to inform the Commission

---

[1778] Article 4 of Council Regulation 139/2004.
[1779] Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 9.
[1780] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*., p. 32.
[1781] J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel, p. 12.
[1782] Communication from the Commission, Guidance on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases, Brussels, 26 March 2021, C(2021) 1959 final, p. 3.
[1783] European Commission, *Facebook/WhatsApp*, 3 October 2014, case M.7217.
[1784] Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 12.

and/or the competition authorities concerned of *all concentrations* implemented on European territory *by "structuring" undertakings*" (emphasis added).[1785] These are defined as undertakings "which hold considerable market power on the market in which they are mainly active but also on neighbouring markets, due to their "gatekeeper" status".[1786] The European Commission and/or national competition authorities could then require the structuring undertaking to formally notify the acquisition for merger control review if they consider that it might present competitive risks (such as risks of input foreclosure).[1787] A similar suggestion has been made in the Furman Report, which recommended that the UK Competition and Markets Authority should be informed of all intended acquisitions by an undertaking having "strategic market status".[1788] These are the undertakings that are "in a position to exercise market power over a gateway or bottleneck in a digital market, where they control others' market access".[1789] While starting from the same perspective, the Stigler Committee report went a step further, as it not only recommended that the Federal Trade Commission (FTC) should be informed of every acquisition made by an undertaking having "bottleneck power"[1790], but rather suggested that all of these acquisitions should be formally notified to the FTC and receive a pre-clearance.[1791]

Another potential adaptation that has been suggested would be to include the value of the acquisition as an alternative threshold in the Merger Regulation, as is currently done in Austria and Germany.[1792] This would allow the European Commission "to determine whether the high transaction price reflects the important future revenues expected from the innovative target (which is welfare enhancing) or reflects the insurance premium for market stability and monopoly rent when the acquired innovation will be killed (which is welfare detrimental)".[1793]

Alternatively, the German experts' report for the modernisation of competition law suggested the inclusion of a broader provision in German competition law which would aim at keeping markets open and contestable, independently of the meeting of a particular threshold, and

---

[1785] *Ibid*., p. 13. Author's own translation.
[1786] *Ibid*., p. 5. Author's own translation.
[1787] *Ibid*., p. 13.
[1788] J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit*., p. 95; S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", 31 March 2020, available at https://ssrn.com/abstract=3565491, p. 4.
[1789] J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit*., p. 55.
[1790] Bottleneck power "describes a situation where consumers primarily single-home and rely upon a single service provider, which makes obtaining access to those consumers for the relevant activity by other service providers prohibitively costly" (Stigler Committee on Digital Platforms, "Final Report", September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report, p. 32).
[1791] Stigler Committee on Digital Platforms, "Final Report", *op. cit*., p. 111; S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", *op. cit*., p. 4.
[1792] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 32. See Bundeskartellamt and Bundeswettbewerbsbehörde, "Guidance on Transaction Value Thresholds for Mandatory Pre-Merger Notification (Section 35 (1a) GWB and Section 9 (4) KartG)", July 2018, available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitfaden/Leitfaden_Transaktionsschwelle.pdf?__blob=publicationFile&v=2.
[1793] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 32.

which would allow "the competition authority to consider, when assessing the existence of a significant impediment to effective competition, the existence of an overall strategy of a dominant company to systematically acquire fast-growing companies with a recognizable and considerable potential to become competitors in the dominated market in the future".[1794] In the same perspective, the European Commission's expert report on "Competition Policy for the digital era" outlined that "where an acquisition plausibly is part of such a strategy, the burden of proof [should be] on the notifying parties to show that the adverse effects on competition are offset by merger-specific efficiencies".[1795]

In any case, the implementation of any of these alternatives would require a modification of the existing European legal framework applicable to mergers.[1796] In this regard, it is worth mentioning that the European Commission's proposal for a Digital Markets Act[1797] provides that "gatekeepers"[1798] offering "core platform services"[1799] will have to "inform the Commission of any intended concentration within the meaning of Article 3 of Regulation (EC) No 139/2004 involving another provider of core platform services or of any other services provided in the digital sector irrespective of whether it is notifiable to a Union competition authority under Regulation (EC) No 139/2004 or to a competent national competition authority under national merger rules".[1800] This notification will notably have to specify the number of yearly active business users and of monthly active end users of the acquisition target, and the rationale for the merger.[1801]

Finally, it must be underlined that the European Commission has indicated in its guidance on the application of the referral mechanism (by national competition authorities to the Commission), set out in Article 22 of the Merger Regulation, that this mechanism could be used for "transactions where the turnover of at least one of the undertakings concerned does not reflect its actual or future competitive potential. This would include, for example, cases where the undertaking: (1) is a start-up or recent entrant with significant competitive potential that has yet to develop or implement a business model generating significant revenues (or is still in the initial phase of implementing such business model); (2) is an important innovator

---

[1794] H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary", *op. cit.*, p. 5. See also Bundeskartellamt, "Amendment of the German Act against Restraints of Competition (Press release)", 19 January 2021, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html. The full text, in German, of the GWB-Digitalisierungsgesetz is available at https://www.bgbl.de/xaver/bgbl/start.xav#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl121s0002.pdf%27%5D_1612262835179.

[1795] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 124. On this point, see also Stigler Committee on Digital Platforms, "Final Report", *op. cit.*, p. 98; and S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", *op. cit.*, p. 3.

[1796] On the broader discussion pertaining to the potential need to adapt competition law in order to better fit the digital environment, see the references mentionned in footnote 63.

[1797] Proposal for a Digital Markets Act. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.

[1798] See Articles 2.1 and 3 of the Proposal for a Digital Markets Act. For more details on the designation of these gatekeepers, see points 397 and 398.

[1799] See Article 1.2 of the Proposal for a Digital Markets Act. For a definition of these services, see Articles 2.2 and 2.5 to 2.11 of the Proposal.

[1800] Article 12.1 of the Proposal for a Digital Markets Act.

[1801] Article 12.2 of the Proposal for a Digital Markets Act.

or is conducting potentially important research; (3) is an actual or potential important competitive force; (4) has access to competitively significant assets (such as for instance raw materials, infrastructure, data or intellectual property rights); and/or (5) provides products or services that are key inputs/components for other industries. In its assessment, the Commission may also take into account whether the value of the consideration received by the seller is particularly high compared to the current turnover of the target".[1802] According to the Commission, such referrals could even be made for transactions that have already been closed, although the referral of mergers that have been implemented for more than six months would only be considered as appropriate in exceptional circumstances, for instance due to "the magnitude of the potential competition concerns and of the potential detrimental effect on consumers".[1803] It should however be outlined that both the national competition authorities and the Commission respectively retain a considerable margin of discretion in deciding whether to refer cases or to accept such referrals.[1804] While this guidance introduces some flexibility in an attempt to address the phenomenon of the acquisition of "nascent innovative players", its application could generate legal uncertainties, notably in terms of the possibility to refer transactions that have already been completed.

[1802] Communication from the Commission, Guidance on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases, *op. cit*., p. 5.
[1803] *Ibidem*.
[1804] *Ibid*., p. 1.

Section D. Overarching considerations pertaining to compulsory B2B data sharing as a competition law remedy

298. Through Sections A to C, this thesis has demonstrated that refusals to share data could lead to three types of competition law infringements, namely abuses of a dominant position, abuses of economic dependence and input foreclosure in vertical mergers, if the conditions of application of these theories are met. For each of these infringements, a potential remedy could be to impose on the large data holder[1805] an obligation to share (some of) its data with several third parties. Naturally, other remedies (data siloing, structural breakups, non-discrimination obligations, etc.) could also be envisaged.[1806] However, as this thesis focusses on compulsory B2B data sharing, these alternatives will not be further detailed here.

In order to impose such a compulsory B2B data sharing remedy on a large data holder, it is necessary to identify the third parties that will be entitled to benefit from the access to the data (a), to determine the categories of data that should be shared (b), and to consider a potential remuneration for the large data holder (c). Finally, the potential anti-competitive effects of such a data sharing remedy will need to be considered (d).

a) Identification of the third parties that will be entitled to benefit from the data sharing remedy

299. Imposing a compulsory B2B data sharing remedy on a large data holder first requires to identify the third parties that should benefit from the access to such data. Indeed, as the aim of the remedy is to restore competition on the markets at hand, the remedy should not create *erga omnes* rights of access, but should only grant access rights to certain well-identified undertakings. In this regard, and as outlined respectively in Sections A to C, in the case of a refusal to share data leading to an abuse of dominant position, the data sharing remedy should only benefit to third parties for whom the access to the dominant undertaking's data is indispensable to operate a business on a downstream market.[1807] In the case of a refusal to share data leading to an abuse of economic dependence, the data sharing remedy should only benefit to third parties that are dependent on the non-dominant undertaking' data in order to operate a business on a downstream market.[1808] Finally, in the case of input foreclosure by a merged entity, the shared data should only benefit third parties that would be unable to

---

[1805] In the context of this Section, this expression relates to a "dominant undertaking" in cases of an abuse of a dominant position, to a "non-dominant undertaking with relative market power" in cases of an abuse of economic dependence, and to a "merged entity having significant market power" in cases of input foreclosure in vertical mergers.

[1806] On these alternative remedies, see *inter alia*, J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*; United States House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets", *op. cit.*; J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data", *op. cit.*; OECD, "Lines of Business Restrictions – Background note", *op. cit.* See also Articles 3.8, 5 and 6 of the Proposal for a Digital Markets Act.

[1807] See points 240 to 244. However, this indispensability condition should arguably not apply to constructive refusals to share data (See point 236; ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239, §§ 38-61).

[1808] See points 270 to 277.

operate on the downstream market if they were foreclosed from accessing the merged entity's data.[1809]

What is thus common, in all three cases, is that an access seeker will have to demonstrate that it cannot collect the data itself, nor access it via another undertaking, and that it needs it to operate on a downstream market. However, the threshold for demonstrating such an absence of alternative is different in the three cases, as, for instance, the threshold for demonstrating the indispensability of a dataset implies an objective assessment and is much higher than the threshold for demonstrating the dependence on the access to a dataset, which requires both an objective and a subjective assessment.[1810]

In light of the above, it is thus apparent that this requirement of the identification of the third parties benefitting from the data sharing remedy is inextricably linked with the requirement to determine the categories of data that should be shared by the large data holder, to which this thesis now turns.

b) Determination of the categories of data that should be shared

300. Imposing a compulsory B2B data sharing remedy on a large data holder also requires to determine the categories of data that should be shared. As the primary purpose of such a data sharing remedy is to tackle market failures[1811] deriving from a lack of data sharing[1812], this thesis argues that the remedy should cover larger amounts of (aggregated) personal data pertaining to multiple individuals and/or non-personal data, rather than smaller quantities of data linked to a specific individual.[1813] It should be outlined from the outset that this will require a careful articulation between personal data protection law and competition law, which will be tackled below in a separate Section of this thesis.[1814]

In order to determine the concrete categories of data that should be covered by the remedy, this thesis suggests to consider the data typology that has been proposed in Part I, Chapter 1, Section C. As a reminder, this thesis suggests a common holistic approach for both personal and non-personal data, which is composed of four categories of data, namely actively provided data, observed data, inferred/derived data and acquired data.

301. The third category of data ("acquired data") should arguably be excluded from the scope of the remedy as, in principle, if the large data holder has been able to acquire the said data from a third party, the access seeker should normally also be able to acquire the same data from such third party. In such a scenario, there would be no reason to compel the large data holder to share such data with the access seeker.

[1809] See points 289 to 291.
[1810] See points 240 to 244, 270 to 277 and 289 to 291.
[1811] On these market failures see Part I, Chapter 2, Section B, c), 3. "Data market failures".
[1812] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", 19 February 2020, COM(2020) 66, p. 3, 5, 8 and 14. See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Shaping Europe's digital future*", Brussels, 19 February 2020, COM(2020) 67, p. 8.
[1813] See Part I, Chapter 3, Section B.
[1814] See Part III, Chapter 2, Section B.

302. Instead, the key question is to determine whether the data sharing remedy should only cover the large data holder's actively provided and observed data, or whether it should also extend to its inferred/derived data. When answering this question, it should be kept in mind that while a data sharing remedy would entail benefits for the access seeker, this could also entail potential negative effects on the data holder's business interests. Indeed, data sharing generates costs for the data holder, which must be balanced with the potential benefits deriving from the sharing.[1815]

303. In this perspective, there are strong arguments to be made that the large data holder's actively provided and observed data should fall within the scope of the data sharing remedy. Indeed, the true value of data does not generally stem from its mere collection, but rather from the information and knowledge that can be derived and inferred from this primary data.[1816] These actively provided and observed data are thus "a valuable input for data-intensive business models in the digital economy".[1817] Yet, in markets which are highly concentrated and where only a handful of undertakings can observe the individuals' activity, "observed data is not ubiquitously available, and it is also usually neither feasible nor socially desirable to duplicate the collection of the same observed data".[1818] This explains why, in practice, access requests are frequently targeted at "observed data, which often cannot be replicated, and at [actively provided] data that would take a significant amount of effort to volunteer again".[1819]

304. The justification for the inclusion of these actively provided and observed data in the scope of the data sharing remedy will arguably even be stronger if these have been collected as a by-product of the large data holder's core economic activity, rather than as the object of its core economic activity.[1820] This is notably due to the fact that data that are collected as a by-product of a core economic activity are difficult to replicate by another firm that is interested in this data rather than in the core economic activity (drilling oil, selling grocery goods, providing health services…).[1821] This might create "a two-level entry problem that may erect high entry barriers in the data-collection market".[1822] Moreover, the (incentive)

[1815] See Part I, Chapter 2, Section B, c), 5.
[1816] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 342. See also C. Argenton and J. Prüfer, "Search engine competition with network externalities", *Journal of Competition Law and Economics*, 2012, Vol. 8(1), p. 73; V. Mayer-Schönberger and Y. Padova, "Regime change? Enabling Big Data through Europe's new Data Protection Regulation", *Columbia Science & Technology Law Review*, Vol. XVII, 2016, p. 320.
[1817] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *CERRE Report*, 2020, available at https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy, p. 55. See also R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 16.
[1818] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy*"*, *op. cit.*, p. 53.
[1819] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit.*, p. 101.
[1820] On this distinction, see point 12. See also M. Gal and D. Rubinfeld, "Data Standardization", *New York University Law Review*, 2019, Vol. 94, Number 4, p. 746; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 357; OECD, *Consumer Data Rights and Competition - Background note*, June 2020, DAF/COMP(2020)1, available at http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm, p. 15.
[1821] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 357.
[1822] *Ibid*., p. 377.

costs of sharing this data in both scenarios are arguably different. Indeed, requiring the sharing of data collected as a by-product will arguably generate lower incentives costs for the large data holder than requiring the sharing of data collected as the object of its core economic activity because, in the former case, data are not collected for the sake of a data-centric business, but rather in order to facilitate the pursuit of the undertaking's core economic activity for which data are a mean and not a goal. Therefore, the large data holder has to collect these data in any case for the pursuit of its core economic activity, and its incentive to collect the data will thus only be marginally affected by a data sharing obligation.

To be sure, this does not mean that requiring the sharing does not entail any costs at all in terms of innovation and incentives to collect the data, but rather that these costs will be lower. This has to be balanced with the fact that these data generated as a by-product could be re-used for other purposes, potentially not linked to the undertaking's core activity, thus generating additional value for society. To give an example, one could think of data collected by sensors on machines in an assembly line, which could be used for other purposes. Indeed, these data are not collected and structured as a goal in itself, but as a by-product of the core economic activity, e.g. assembling cars in a factory, as a mean to increase the efficiency of production.

Additionally, taking this factor into consideration is in line with the analogous discussions pertaining to the "spin-off effect" for the *sui generis* database right, according to which it is questioned whether databases that are by-products ("spin-offs") of a main or other activity of the data producer should also be protected by the *sui generis* database right.[1823] Indeed, in some cases, protecting these spin-off databases could give rise to absolute or unwanted natural monopolies.[1824]

305. Nevertheless, while this distinction could have merit when assessing the balance between the benefits and the costs of imposing the data sharing remedy, it must be underlined that, in practice, it might be extremely difficult to determine whether a specific dataset has been collected as a by-product or as the object of the large data holder's core economic activity. Indeed, this notion of "core economic activity" is evolutive.[1825] In many cases, firms will first start to collect data passively, as a by-product of their core economic activity, but once they realise the value that such data can have, they will tend to move towards more active data collection approaches.[1826]

[1823] On this "spin-off effect" theory, see *inter alia*, E. Derclaye, "Databases sui generis right: should I adopt the spin off theory?", *E.I.P.R.*, 2004, Issue 26(9), p. 402-413; B. Hugenholtz, "Program Schedules, Event Data and Telephone Subscriber Listings under the Database Directive--The 'Spin-Off' Doctrine in the Netherlands and elsewhere in Europe", *Paper presented at 11th Annual Conference on International Intellectual Property Law and Policy, Fordham University School of Law, New York, April 14-25*, 2003, available at https://www.ivir.nl/publicaties/download/spinofffordham.pdf.

[1824] E. Derclaye, "Databases sui generis right: should I adopt the spin off theory?", *op. cit.*, p. 412; B. Hugenholtz, "Program Schedules, Event Data and Telephone Subscriber Listings under the Database Directive--The 'Spin-Off' Doctrine in the Netherlands and elsewhere in Europe", *op. cit.*, p. 7.

[1825] See point 12.

[1826] OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 15-16. For an example in the retail business, see J. Turow, *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, New Haven, Yale University Press, 2017.

306. On the other hand, this thesis argues that, in order to preserve the business interests of the data holder, its inferred/derived data should not be covered by the data sharing remedy. This is because these types of data will often be the most valuable for data holders, as this is where the real added value of their product/service must be found.[1827] Indeed, as outlined by Krämer *et al.*, "such data is the result of innovation efforts (e.g. in data analytics) with the intent to derive actionable insights that are then the basis for competition in digital markets".[1828] Accordingly, excluding such categories of data from the scope of the remedy would prevent potential competitors of the data holders from benefiting from these actionable insights in which the data holders have heavily invested, and would incentivise them to derive such actionable insights themselves on the basis of the actively provided/observed data that they would obtain through the remedy. Indeed, inferred/derived data should arguably be seen as "the basis for competition between data-intensive firms, whereas [actively provided] data and observed data are the 'raw data' inputs".[1829] As the focus of competition is shifted from collection to analysis considerations, this is also likely to stimulate innovation.[1830]

307. To conclude on the determination of the categories of data that should be shared, two additional remarks must be formulated. Firstly, this thesis argues that the concrete categories of personal and non-personal data covered by the remedy should not be *all of* the large data holder's actively provided and observed data, but rather only a *specific subset* of these actively provided and observed data, which will need to be determined on a case-by-case basis. This is because the requirement to identify the scope of the data covered by the remedy is inextricably linked with the above-mentioned requirement of the identification of the third parties benefitting from the data sharing remedy. More specifically, the remedy should be limited to the actively provided and observed data that are considered as indispensable to operate a business on a downstream market, in the case of an abuse of dominant position[1831]; to the non-dominant undertaking's actively provided and observed data on which the access seeker is dependent in order to operate a business on a downstream market, in the case of an abuse of economic dependence;[1832] or to the merged entity's important actively provided and observed data, without which the access seeker would be unable to operate on a downstream market, in the case of input foreclosures in vertical mergers.[1833]

Secondly, in order to ensure that its data sharing remedy will efficiently tackle the anti-competitive practice that it aims to address, the competition authority will also have to determine whether the data sharing remedy should be static or dynamic. Indeed, in certain situations, it might not be sufficient to impose the static sharing of data through a one-shot (or periodic) bulk data transfer(s). Rather, due to the digital economy's dynamic nature, it might be necessary to consider the imposition of a more dynamic data sharing remedy, that would

---

[1827] See point 17.
[1828] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 93.
[1829] *Ibid*., p. 17.
[1830] J. Krämer, P. Senellart and A. de Streel, "Making data portability more effective for the digital economy", *op. cit.*, p. 9.
[1831] See points 240 to 244.
[1832] See points 270 to 277.
[1833] See points 289 to 291.

guarantee that the access seeker has access to the large data holder's relevant actively provided and observed data, via application programming interfaces ("APIs")[1834], on a constant basis and in (near) real-time. As the latter type of remedy will entail higher implementation costs for the large data holder, it should however only be imposed when the benefits of such dynamic real-time access trump its costs. This will thus require a case-by-case assessment by the competition authority.

c) Remuneration of the large data holder

308. One way to attenuate the costs of the sharing for the large data holder would be to provide for a potential remuneration. Indeed, this would counter-balance the possible stifling effects that such a duty to share (aggregated) personal data pertaining to multiple individuals and/or non-personal data could have on these data holder's business incentives.

As, due to the Arrow information paradox[1835], the value of data is difficult to assess, it is advisable for the competition authority not to impose a specific price for the sharing, but rather to "rely on more open terms provided they are sufficiently precise for the data owner to determine with enough legal certainty the price to charge".[1836] In this perspective, the competition authority could require the large data holder to propose a FRAND (Fair Reasonable And Non-Discriminatory) price for the sharing, by analogy with the licensing-fee requirements used in the context of the Standard Essential Patents (SEPs).[1837] While this would be more comfortable for competition authorities than setting the concrete price themselves, it is important to outline that there are also a significant number of uncertainties in determining what constitutes a FRAND price, as illustrated by the numerous discussions around this term in the realm of SEPs.[1838]

In this regard, Drexl points out that the *Huawei*[1839] judgment of the European Court of Justice, where the Court created a negotiation framework for the licensing of SEPs[1840], could provide inspiration to deal with data sharing cases and could assist the parties to reach an agreement

---

[1834] "An application programming interface (API) is an interface or communication protocol between a client and a server intended to simplify the building of client-side software. It has been described as a "contract" between the client and the server, such that if the client makes a request in a specific format, it will always get a response in a specific format or initiate a defined action" (https://en.wikipedia.org/wiki/Application_programming_interface).

[1835] See point 111. K. Arrow, "Economic Welfare and the Allocation of Resources for Invention", *The Rate and Direction of Inventive Activity: Economic and Social Factors*, National Bureau of Economic Research (ed.), 1962, p. 609-626.

[1836] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 38.

[1837] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *op. cit.*, p. 373.

[1838] See, for instance, D. Geradin, A. Layne-Farrar and N. Petit, *EU Competition Law and Economics*, Oxford, Oxford University Press, 2012, p. 457; D. Geradin, "Ten Years of DG Competition Effort to Provide Guidance on the Application of Competition Rules to the Licensing of Standard-Essential Patents: Where Do We Stand?", 21 January 2013, available at https://ssrn.com/abstract=2204359, p. 7-8; C. Graham and J. Morton, "Latest Developments in Standards, Patents and FRAND licensing", *E.I.P.R.*, 2014, Vol. 36, Issue 11, p. 700-706; R. Stern, "What are Reasonable and Non-discriminatory Terms for licensing a Standard-essential Patent?", *E.I.P.R.*, 2015, Vol. 37, Issue 9, p. 549-557; J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975, p. 55; ECJ, *Huawei,* 16 July 2015, C-170/13, EU:C:2015:477.

[1839] ECJ, *Huawei,* 16 July 2015, C-170/13, EU:C:2015:477.

[1840] *Ibid*., §§ 60-69.

on the data sharing price.[1841] This negotiation framework, applied to data, could be the following:

- Once the access seeker has expressed its willingness to pay a FRAND remuneration for the data, the data holder must present a specific written offer specifying the price and the way in which it is to be calculated;
- It is then for the access seeker to respond diligently to that offer in good faith and without delaying tactics;
- Should the access seeker not accept the offer made to it, it has to submit to the data holder, promptly and in writing, a specific counter-offer that corresponds to FRAND remuneration; and
- Where no agreement is reached on the details of the FRAND remuneration following the counter-offer, the parties should, by common agreement, request that the price be determined by an independent third party. To set this price, this thesis argues that the independent third party could, for instance, rely on the "baseball arbitration" mechanism, originally used in the USA for baseball salary negotiations.[1842] According to this mechanism, each party proposes a price to the third party, who is tasked with choosing the price that appears to be the most "reasonable" under the circumstances of the cases. This forces each party to restrain themselves from proposing unreasonable prices, as they know that if they suggest an extravagant price, while the other party suggests a more "reasonable" one, the independent third party will pick the other party's price. A variant form is the "night baseball arbitration", where the independent third party first decides itself what could be a reasonable price and then looks at the party's proposals and choses whichever is the closest to the price it first considered.

309. The independent third party mentioned above could be one of the national authorities that the European Commission's proposal for a Data Governance Act suggests to appoint in order to supervise *voluntary* B2B data sharing with trusted data intermediaries.[1843] Indeed, these national authorities will arguably be in a good position to assess the appropriateness of the proposed price for the data sharing, due to their expertise with *voluntary* data sharing. It could thus also be resorted to them in the context of *compulsory* data sharing imposed by a competition law remedy. Moreover, if technical experts are appointed within these authorities, they will arguably also be in a better position to determine the technical means of the sharing (one shot data transfer; daily/weekly/monthly transfers of bulks of data; real-time access[1844] via APIs, etc.) if the parties do not find an agreement in this regard. This would relieve the

---

[1841] J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", op. cit.*, p. 55. See also H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *op. cit.*, p. 4-29.

[1842] See http://www.arbitration.com/articles/what-is-baseball-arbitration.aspx.

[1843] See Recitals 22 to 34 and Articles 13 and 23 to 25 of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final.

[1844] The "freshness" and "up-to-dateness" of the data can indeed be of the utmost importance for certain business models. See V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *Max Planck Institute for Innovation and Competition Research Paper No. 19-04*, 2019, available at https://ssrn.com/abstract=3337524, p. 18-19.

competition authorities from assuming this role for which they are ill-suited.[1845] This is especially so in cases where the sharing needs to be continuous, for instance in order to ensure interoperability, as the competition authorities are not well-equipped to deal with these issues.[1846] To fulfil these tasks, these national authorities could be assisted by the Support Centre for Data Sharing, created in 2019, which has been tasked with collecting the best practices and existing model contract terms for *voluntary* data sharing agreements[1847], and which could thus provide valuable insights.[1848] Moreover, they could be assisted by the future European Data Innovation Board, which is a formal expert group that the European Commission suggests to create in order to implement the future horizontal governance framework for *voluntary* data sharing, and which should support the European Commission's work on technical standardisation and interoperability to facilitate data sharing.[1849]

310. Independently of the determination of the body that should monitor this negotiation process, this thesis argues that several factors should, in any case, be taken into consideration when determining the price of the sharing remedy. On the one hand, in cases where a refusal to share data leads to the termination of an existing business relation, the price of the sharing should arguably remain the same as the one that existed prior to the termination, for a reasonable period of time to be determined on a case-by-case basis. For instance, this reasonable period of time could correspond to the above-mentioned negotiation period. Indeed, although there might be an objective justification for a price increase, "freezing" the price during this reasonable period should ensure that the access seeker will be put in a more comfortable bargaining position during this negotiation period. Accordingly, if the data was shared for free prior to the refusal to keep sharing the data in the future, like in the *PeopleBrowsr v. Twitter* and *hiQ v. LinkedIn* cases mentioned above[1850], the sharing should arguably remain free during this negotiation period.

On the other hand, and provided that such a difference can be established in practice[1851], the sharing price for data generated as a by-product of a core economic activity should, arguably,

---

[1845] *Ibid*., p. 17.
[1846] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit*., p. 10.
[1847] Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication "*Towards a common European data space*", Brussels, 25 April 2018, SWD(2018) 125 final, p. 6.
[1848] See Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final, p. 55.
[1849] See Recitals 40 and 41 and Articles 26 and 27 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit*., p. 54.
[1850] See point 268. Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf; United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html; United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.
[1851] See points 12 and 305.

be lower than the sharing price for data whose collection, structuration and analysis is the core economic activity of the large data holder. This is because sharing data collected as a by-product will arguably generate lower incentives costs for the large data holder than sharing data collected as part of the data holder's core economic activity.[1852]

d) Factoring the potential anti-competitive effects of the data sharing remedy

311. Last but not least, the data sharing remedy will have to be carefully designed in order to avoid the creation of potential anti-competitive effects. This would notably be the case if the large data holder and the specific third parties receiving the data (i.e. the data recipients) decided to use the shared data in order to enter into anti-competitive agreements, prohibited by Article 101 of the TFEU.[1853] Indeed, "Article 101 TFEU can stand in the way of data sharing in situations where the exchange of information among competitors gives rise to collusion under Article 101(1) TFEU[1854] and the resulting restriction of competition cannot be justified under Article 101(3) TFEU[1855] by showing that the procompetitive effects outweigh the anticompetitive effects".[1856]

Arguably, this collusion risk might not materialise if the competition authority solely compels the large data holder to share the data with specific data recipients, but does not provide for a reciprocal data flow from the recipients towards the data holder, nor for data sharing between the various recipients. This is especially so because, in order to preserve the business interests of the data holder, only actively provided and observed data will be shared with the data

---

[1852] See point 304.

[1853] On this issue, see B. Lundqvist, "Competition and Data Pools", *Journal of European Consumer and Market Law*, 2018, p. 146-154; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 92-98; I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper DP 2019-005*, November 2019, available at https://ssrn.com/abstract=2956308, p. 7-8; H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *IIC*, 2019, Volume 50, Issue 1, p. 22-23; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 24.

[1854] "The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:
(a) directly or indirectly fix purchase or selling prices or any other trading conditions;
(b) limit or control production, markets, technical development, or investment;
(c) share markets or sources of supply;
(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".

[1855] "The provisions of paragraph 1 may, however, be declared inapplicable in the case of:
- any agreement or category of agreements between undertakings,
- any decision or category of decisions by associations of undertakings,
- any concerted practice or category of concerted practices,

which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:
(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;
(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question".

[1856] I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing", *op. cit.*, p. 7.

recipients, and not the large data holder's inferred/derived data, which are the most commercially sensitive.[1857]

On the other hand, this collusion risk must be factored if the competition authority envisages to impose to the large data holder the obligation to pool some of its data with other data held by the specific third parties "receiving" the data. Indeed, in such a scenario, there is a risk that the procompetitive goal of the data sharing remedy could be misused by the participants to the data pooling agreement, for instance to fix prices, limit production or share markets or sources of supply.[1858] Therefore, if the competition authority wishes to impose such a data pooling remedy, it will need to ensure that the procompetitive effects of the data pool outweigh its potential anticompetitive effects.

However, at this point in time, this might be difficult to assess for the competition authority, as there is some uncertainty on the way in which Article 101 TFEU should be applied to data pooling arrangements.[1859] Indeed, while the Commission's Guidelines on Horizontal Agreements outline several factors that must be taken into consideration in order to weigh these anticompetitive risks – such as "the strategic nature of the information, the market coverage of the firms involved, the individualised or aggregated nature of the company information exchanged, the age of the data, the frequency of the information exchange, the public or non-public nature of the information, and whether the exchange of information is public or non-public"[1860]–, competition issues entailed by data pooling are still relatively new and under-researched, and several voices have been raised regarding the need for more legal clarity on these issues.[1861] In fact, this is one of the goals of the current revision process of these Guidelines, which will likely be concluded in the beginning of 2022. In the meantime, it can be recommended to competition authorities to exercise caution and restraint regarding the imposition of data pooling as a remedy, until more clarity is provided on the matter.

312. However, if, despite this existing uncertainty, a competition authority wants to impose a data pooling remedy, it will, at the very least, have to ensure that the pool will not lead to the foreclosing of competitors from the market, due to a denial of access to the pool, or to the granting of the access to the pool on less favourable terms.[1862] In this regard, the competition authority could take inspiration from past cases. For instance, in the *Asnef-Equifax* case, the European Court of Justice assessed the compatibility with Article 101 TFEU of a register that allowed Spanish financial institutions to share solvency and credit information data about

---

[1857] See Part III, Chapter 1, Section D, b).
[1858] Article 101.1, a) to c) of the TFEU.
[1859] I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing", *op. cit.*, p. 7.
[1860] *Ibidem*; Communication from the Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 14 January 2011, 2011/C 11/01, §§ 86-94.
[1861] See, inter alia, Commission Staff Working Document, Evaluation of the Horizontal Block Exemption Regulation, Brussels, 6 May 2021, SWD(2021) 103 final, p. 29, 43, 57 and 68; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 9 and 92-98; B. Lundqvist, "Competition and Data Pools", *op. cit.*, p. 153.
[1862] Commission Staff Working Document, Evaluation of the Horizontal Block Exemption Regulation, *op. cit.*, p. 29; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 9 and 92-93 and 97-98.

their clients in order to evaluate the risks of non-repayment of loans.[1863] In that case, the Court held that such an information sharing practice would be less likely to restrict competition if the relevant market is not highly concentrated and if the access to the information sharing tool is accessible in a non-discriminatory manner to all the actors active in the relevant market.[1864] Similarly, it should be highlighted that the European Commission has recently sent a Statement of Objections to Insurance Ireland, which is an association of companies active in the insurance sector in Ireland covering over 90% of the Irish motor vehicle insurance market.[1865] This is because the Commission considers that Insurance Ireland has infringed competition law by denying the access to its "Insurance Link" data sharing platform (which comprises a non-life insurance claims data pool) to certain insurers and their agents, as this puts the latter at a competitive disadvantage.

Moreover, the competition authority will need to ensure that the pooling remedy will not discourage the participants in the pool from differentiating and improving their own data collection and analytics processes (which would hamper innovation), and that it will not lead to an anti-competitive information exchange of competitively sensitive information (although, as outlined above, this risk should be quite limited as only actively provided and observed data will be shared, and not inferred/derived data, which are the most sensitive and valuable).[1866] Regarding the latter concern, competition authorities could build on the valuable insights provided by Lundqvist:

> "[A]s a rule of thumb, pools where the parties share relevant strategic and competitive information, such as pricelists, future output prediction and new innovations, should be considered at risk of being anticompetitive, according to Article 101(1) TFEU, while still possibly being available for an exemption under Article 101(3) TFEU. On the other end of the spectrum, data pools containing technical information for the development of new products and services could be regarded as benign research or technical developments cooperations, and should be judged in analogy with R&D collaborations, standard-setting efforts or, to some extent, patent pools. We could add to this latter group also the data pools facilitating interoperability between devices and products, such as connected cars.
>
> The difficult data pools would be the pools containing a large amount of customers, i.e., firms or consumer information. (…) Such pools may contain much necessary information for the development of new and better products and services. They are platforms for creating efficiencies and innovation. These data pools do not imply collusion between firms providing data regarding price or output. (…) However, the parties having access to the pool can with the use of data analytics use their asymmetric

---

[1863] ECJ, *Asnef Equifax and Administración des Estado*, 23 November 2006, C-238/05, EU:C:2006:734.
[1864] *Ibid*., §§ 58-61; I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing", *op. cit*., p. 7.
[1865] European Commission, "Antitrust: Commission sends Statement of Objections to Insurance Ireland", *Press release n° IP/21/3081*, 18 June 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3081.
[1866] Commission Staff Working Document, Evaluation of the Horizontal Block Exemption Regulation, *op. cit*., p. 29; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit*., p. 9 and 92-93 and 96-97.

information advantage to abuse the (market) power they hold, based on access to the data in the pool".[1867]

313. In light of the above, if a competition authority envisages to impose a data pooling remedy, it will need to carefully balance the potential procompetitive and anticompetitive effects of this option. As there is much uncertainty pertaining to this question, competition authorities might be better off imposing, for the time being, "unilateral" data sharing remedies on large data holders (which do not imply a reciprocal sharing of data from the data recipients nor any form of data exchange between the data recipients), at least until the Commission has completed the revision of its Guidelines on Horizontal Agreements.

* * *

314. To conclude this Section, the above-mentioned overarching considerations pertaining to compulsory B2B data sharing as a competition law remedy are summarised in Table 2.

Table 2: Overarching considerations pertaining to compulsory B2B data sharing as a competition law remedy

	Compulsory B2B data sharing as a competition law remedy
Data holders subject to the sharing obligation	Undertakings abusing their dominant position (essential facilities doctrine).[1868] Undertakings abusing their "relative market power" (abuse of economic dependence).[1869] Merged entities having "significant market power" and foreclosing the access to an important input (input foreclosure in vertical mergers).[1870]
Data recipients entitled to benefit from the sharing obligation	Only those:[1871] - for whom the access to the dominant undertaking's data is "indispensable"[1872]; - that are "dependent" on the non-dominant undertaking' data; or - that need access to the "important data" of the merged entity; in order to operate on a downstream market.
Types of data covered by the sharing obligation	Only actively provided and observed data (not acquired, nor inferred/derived data).[1873] Not *all of* the large data holder's actively provided and observed data, but rather only a *specific subset* of these actively provided and observed data, which will need to be determined on a case-by-case basis.[1874] Personal data should only be shared to the extent that this complies with the GDPR's principles and that there are lawful basis of processing allowing the sharing.[1875]

[1867] B. Lundqvist, "Competition and Data Pools", *op. cit.*, p. 150.
[1868] See Part III, Chapter 1, Section A.
[1869] See Part III, Chapter 1, Section B.
[1870] See Part III, Chapter 1, Section C.
[1871] See Part III, Chapter 1, Section D, a).
[1872] However, this indispensability condition should arguably not apply to constructive refusals to share data (See points 236 and 240 to 244; ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239, §§ 38-61).
[1873] See Part III, Chapter 1, Section D, b).
[1874] See point 307.

Remuneration of the data holder as compensation for the sharing obligation	FRAND remuneration (lower price for data generated as by-product than as core economic activity of the data holder).[1876] If the data holder(s) and data recipient(s) fail to agree on the data sharing price, price could be determined by an independent third party.[1877]
Technical implementation of the sharing obligation	Depending on the case, could be a static or dynamic data sharing remedy. The latter should only be imposed when the benefits of real-time access trump its costs.[1878] An independent third party could also determine the technical means of the sharing if the parties do not agree on them.[1879] If a data pooling remedy is envisaged, the potential procompetitive and anticompetitive effects of this option will need to be balanced[1880]

[1875] See Part III, Chapter 2, Section B.
[1876] See Part III, Chapter 1, Section D, c).
[1877] See points 308 and 309.
[1878] See Part III, Chapter 1, Section D, b).
[1879] See Part III, Chapter 1, Section D, c).
[1880] See Part III, Chapter 1, Section D, d).

Section E. The issue of the time-consuming process of competition intervention

315. In order for the B2B data sharing remedy imposed by the competition authority to be truly efficient, this competition intervention must also be timely. Indeed, if a long period of time elapses before the competition authority is able to establish the competition law infringement resulting from a refusal to share data, and to determine the appropriate data sharing remedy[1881], such a remedy may come too late for the access seeker. As outlined by Bourreau and de Streel, "the timing of antitrust decisions is often too slow and not aligned with the timing of market evolutions. This time lag is particularly harmful in the digital sector because, on the one hand, antitrust actions often take more time than average as new and complex technical and legal issues are raised while, on the other hand, markets are evolving more quickly than average due to rapid technological progress".[1882] As a result, the downstream market on which the access seeker wishes to operate, but for which it needs the access to the large data holder's data to do so, might tip in favour of the latter due to strong network effects. Consequently, the access seeker might be driven out of such market, due to the large data holder's refusal to share, before the competition intervention process is completed. Accordingly, there have been growing calls to speed up this competition process in order to better match these rapid digital market evolutions.[1883]

[1881] See Part III, Chapter 1, Section D, a) to d).

[1882] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 33.

[1883] See (EU) J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit*.; (Germany) H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *Report by the Commission "Competition Law 4.0" for the German Federal Ministry for Economic Affairs and Energy*, 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competitionframework.pdf?__blob=publicationFile&v=2; (Germany) H. Schweitzer, J. Haucap, W. Kerber and R. Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, Baden-Baden, Nomos, 2018 (also available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtigeunternehmen.html (an executive summary in English is available at https://ssrn.com/abstract=3250742)); (France) Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19 contribution adlc enjeux numeriques vf.pdf; (BeNeLux) J. Steenbergen, M. Snoep and P. Barthelmé, "Joint memorandum of the Belgian, Dutch and Luxembourg competition authorities on challenges faced by competition authorities in a digital world", 2 October 2019, available at https://www.belgiancompetition.be/en/about-us/publications/joint-memorandum-belgian-dutch-and-luxembourg-competition-authorities; (UK) J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel; (UK) UK Competition & Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study; (USA) Stigler Committee on Digital Platforms, "Final Report*"*, September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report; (Australia) Australian Competition and Consumer Commission, "Digital Platforms Inquiry – Final Report", 26 July 2019, available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report. For a comparative analysis of some of these reports, see W. Kerber, "Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia", September 2019, available at https://ssrn.com/abstract=3469624; and S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", 31 March 2020, available at https://ssrn.com/abstract=3565491.

a) Exploring the use of interim measures and market investigations

316. In substance, three evolutions have been suggested in order to tackle the above-mentioned issue. The first suggestion, that this thesis will simply briefly mention, is to create, like in Spain, deadlines for antitrust cases, similarly to what currently exists for merger cases, in order to ensure that these cases do not drag on for lengthy periods of time.[1884] Naturally, the imposition of such deadlines should be accompanied by safeguards in order to "alleviate adverse case selection and to ensure that the agencies will not focus merely on the easy cases that can be decided quickly and ignore the hard cases that can be more useful for the agencies and for the markets".[1885]

317. The second suggestion is that competition authorities should more frequently rely, in digital markets, on interim measures, which could be imposed on the large data holder, pending the outcome of the investigation, and which would be accompanied by financial penalties in cases of non-compliance.[1886] Indeed, Article 8 of Council Regulation on the implementation of Articles 101 and 102 of the TFEU provides that:

> "1. In cases of urgency due to the risk of serious and irreparable damage to competition, the Commission, acting on its own initiative may by decision, on the basis of a prima facie finding of infringement, order interim measures.
>
> 2. A decision under paragraph 1 shall apply for a specified period of time and may be renewed in so far this is necessary and appropriate".[1887]

Yet, these interim measures have rarely been used by the European Commission in the past 20 years, notably because the interim measure that it had imposed in the *IMS Health* case in 2001[1888] – by which it had required IMS Health to licence its brick structure, considered as being indispensable, to NDC Health[1889]– had been suspended by the Court of First Instance.[1890] Moreover, such interim measures entail high procedural requirements for the European Commission, which could delay the decision in the main proceedings, and the

---

[1884] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 34.
[1885] *Ibidem*.
[1886] See H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *op. cit.*, p. 71-73; Competition and Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, p. 348; Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 2 and 6; M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 33; P. Picht, "Towards an Access Regime for Mobility Data", *IIC*, 2020, Volume 51, Issue 8, p. 961.
[1887] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, *OJ L 1/1*, 4 January 2003.
[1888] European Commission, *NDC Health/IMS Health: Interim measures*, 3 July 2001, COMP D3/38.044, *OJ L 59/18*.
[1889] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 58.
[1890] CFI, *IMS Health, Inc. v Commission of the European Communities*, 10 March 2005, T-184/01, EU:T:2005:95; H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *op. cit.*, p. 71.

European Court of Justice has a wide leeway in deciding whether to suspend these measures during annulment proceedings brought before it.[1891]

However, it has to be pointed out that the European Commission has renewed with the use of such interim measures in its *Broadcom* decision of October 2019.[1892] This could be an encouraging sign that it is intending to rely more on such tools in the future, and this could reduce the time lag between competition law procedures and the rapid evolution of the digital markets "without sacrificing the due process and the quality of the final decision".[1893] Importantly, when assessing whether to impose such measures in the future, the European Commission will need to weigh the interests of all of the parties concerned, namely the "interest in the protection of competition and the interest of the companies affected by the interim measure; and (…) [i]n the case of high risks to competition, serious doubts as to the legality of the conduct may suffice to order interim measures, particularly in the earliest stages of examination".[1894] Yet, while these high risks to competition may indeed exist, in some circumstances, in the digital sector due to dynamic market evolutions and the risks of fast market tipping, it might be more tricky to raise serious doubts regarding the legality of the conduct at hand, as such conducts often raise new technical and legal issues.[1895]

318. The third suggestion was the creation of a "New Competition Tool", which would have allowed the European Commission to conduct market investigations in order address structural market failures in a timely and effective manner, similarly to what the Competition and Markets Authority can do in the United Kingdom.[1896] This is yet another measure that aims at ensuring that competition rules remain fit for an increasingly digital world.[1897] Indeed, to justify the creation of such a tool, the European Commission argued that there is a growing body of economic evidence suggesting the existence of structural competition problems that cannot be tackled under existing competition law rules (e.g. monopolisation strategies by non-dominant undertakings with market power) or, at least, not in the most effective manner (e.g. parallel leveraging strategies by dominant companies into multiple adjacent markets), and that

---

[1891] H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *op. cit.*, p. 71.

[1892] European Commission, *Broadcom*, 16 October 2019, AT.40608; H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *op. cit.*, p. 71.

[1893] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 33.

[1894] H. Schweitzer, M. Schalbruch, A. Wambach, W. Kirchhoff, D. Langeheine, J.-P. Schneider, M. Schnitzer, D. Seeliger, G. Wagner, H. Durz, M. Heider and F. Mohrs, "A New Competition Framework for the Digital Economy", *op. cit.*, p. 71-72.

[1895] M. Bourreau and A. de Streel, "Digital Conglomerates and EU Competition Policy", *op. cit.*, p. 33.

[1896] European Commission, Inception Impact Assessment: "*New Competition Tool ('NCT')*", June 2020, Ares(2020)2836004, p. 1; S. Vezzoso, "Competition Policy in Transition: Exploring Data Portability's Roles", *15th ASCOLA (Virtual) Conference*, June 2020, available at https://ssrn.com/abstract=3634736, p. 18-19. For a criticism of this proposition, notably of its effectivity and of its ability to foster timelier competition intervention, see Freshfields Bruckhaus Deringer, "New Competition Tool: Observations in the context of the Commission's Public Consultation", 8 September 2020, available at https://passle-net.s3.amazonaws.com/Passle/5832ca6d3d94760e8057a1b6/MediaLibrary/Document/2020-09-09-14-52-58-669-FreshfieldsSubmissionNewCT.pdf.

[1897] Communication from the Commission, "*Shaping Europe's digital future*", *op. cit.*, p. 8.

this results in inefficient market outcomes.[1898] Indeed, as outlined by the European Commission's inception impact assessment of this "New Competition Tool":

> "A few large platforms have become gatekeepers for many digital and non-digital products and services. Underlying this development are market characteristics such as extreme economies of scale and scope, strong network effects, zero pricing and data dependency, as well as market dynamics favouring sudden and radical decreases in competition ('tipping') and 'winner-takes-most' scenarios. (…) [T]hese characteristics can make a position of market power or dominance, once acquired, difficult to contest".[1899]

For the European Commission, these structural competition problems are two-fold.[1900] On the one hand, there are "structural risks for competition", which are scenarios in which certain market characteristics (network effects, economies of scale and scope, lock-in effects, etc.) and the conduct of several undertakings operating in these markets (e.g. unilateral strategies by non-dominant companies to monopolise a market through anti-competitive means) create a threat for competition (e.g. risks of market tipping), which could be prevented through early intervention. On the other hand, there are "structural lacks of competition", which are scenarios in which the structure of the market prevents it from working well and from delivering competitive outcomes due to systemic failures (high concentration and barriers of entry, lack of access to data, lock-ins, etc.).

In order to tackle these structural competition problems and to restore undistorted competition on these markets, the European Commission argued that it needed new tools at its disposal that would allow it to intervene in a timelier fashion, and that would provide it with more intervention powers than "sector inquiries", which only empower it to request information from undertakings but not to impose remedies outside the scope of individual infringement procedures.[1901] Concretely, what was proposed was to adapt the EU competition law framework in order to allow the Commission, in close cooperation with national competition authorities, to conduct market investigations in order to "intervene when a structural risk for competition or a structural lack of competition prevents the internal market from functioning properly. The tool would enable the Commission to impose behavioural and, where appropriate, structural remedies. The Commission could also recommend legislative action to improve the functioning of the market concerned. (…) [However] there would be no finding of an infringement, no fines and no damage claims".[1902] Naturally, these market investigations would have to respect the rights of defence of the undertakings concerned.[1903] Such market investigations could be particularly useful to address systemic market tipping issues. Indeed, as outlined by Prüfer:

[1898] European Commission, Inception Impact Assessment: "*New Competition Tool ('NCT')*", June 2020, Ares(2020)2836004, p. 1-2.
[1899] *Ibid*., p. 1.
[1900] *Ibid*., p. 2.
[1901] *Ibid*., p. 3.
[1902] *Ibidem*.
[1903] *Ibid*., p. 4.

> "Market tipping occurs in data-driven markets even if the [undertaking]'s conduct is flawless as it depends on data-driven indirect network effects, which are an unavoidable (and potentially very efficient) economic characteristic of such markets. Moreover, if a market is found to be data-driven, tipping can be predicted. [Anti-competitive behaviour] is not necessary to tip the market or to discourage competitors from innovating heavily. Therefore, what is needed is the option to intervene in such markets ex ante, that is, before the market has tipped and the [undertaking] can be accused of abusing its position (which perhaps it has not). Moreover, in order to avoid the cumbersome and lengthy process of repetitive legal cases, a quicker and more flexible tool that allows competition authorities to intervene in markets without invoking [a competition law infringement] is needed".[1904]

Four options were considered for the design of such a tool, as it could have applied either to competition concerns raised by dominant undertakings only, or also to competition concerns raised by non-dominant undertakings; and either to some specific sectors only, or horizontally to all sectors.[1905]

319. Eventually, the possibility to conduct market investigations has been included in the European Commission's proposal for a Digital Markets Act.[1906] However, it has been somewhat "downgraded" compared to the initial proposal mentioned above, following concerns raised by the "Regulatory scrutiny board", i.e. the European Commission's internal review panel.[1907]

According to this proposal, the European Commission can first conduct a market investigation in order to examine whether a provider of "core platform services"[1908] should be designated as a "gatekeeper"[1909]. [1910] This can be done on its own initiative, or if three or more Member States request it and if there are reasonable grounds to open such an investigation.[1911] The Commission will have to communicate its preliminary findings within 6 months of the opening of the investigation and will have to close the investigation within twelve months of its opening.[1912] If the Commission designates as a gatekeeper a large data holder that does not

---

[1904] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf, p. 9.
[1905] European Commission, Inception Impact Assessment: "*New Competition Tool ('NCT')*", June 2020, Ares(2020)2836004, p. 3.
[1906] See Articles 14 to 17 of the Proposal for a Digital Markets Act.
[1907] See S. Stolton, "Blacklist prohibitions to be 'very limited' to large platforms, Commission says", 9 December 2020, available at https://www.euractiv.com/section/digital/news/blacklist-prohibitions-to-be-very-limited-to-large-platforms-commission-says/. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*", Brussels, 15 December 2020, SWD(2020) 363 final, p. 77-78.
[1908] See Article 1.2 of the Proposal for a Digital Markets Act. For a definition of these services, see Articles 2.2 and 2.5 to 2.11 of the Proposal.
[1909] See Articles 2.1 and 3 of the Proposal for a Digital Markets Act. For more details on the designation of these gatekeepers, see points 397 and 398.
[1910] Article 15 of the Proposal for a Digital Markets Act.
[1911] Article 33 of the Proposal for a Digital Markets Act.
[1912] Articles 15.1 and 15.2 of the Proposal for a Digital Markets Act.

yet benefit from an entrenched and durable position in its operations[1913], but that it is foreseeable that it will enjoy such a position in the near future (likeliness of the market to tip), only the obligations that are appropriate and necessary to prevent this data holder from entrenching its position through unfair means shall be declared applicable to it.[1914]

Second, the European Commission can conduct a market investigation to determine whether a "gatekeeper" "has systematically infringed the obligations laid down in Articles 5 and 6 and has further strengthened or extended its gatekeeper position".[1915] A "gatekeeper" shall be deemed to have engaged in a systematic non-compliance if it has been the subject of at least three non-compliance or fining decisions issued by the Commission[1916] within a period of five years prior to the decision opening the market investigation.[1917] It shall be deemed to have further strengthened or extended its gatekeeper position if "its impact on the internal market has further increased, its importance as a gateway for business users to reach end users has further increased or [if] the gatekeeper enjoys a further entrenched and durable position in its operations".[1918] In such cases, the Commission can impose any behavioural or structural remedies on the "gatekeeper", which are proportionate to the infringement and are necessary to ensure compliance with the Digital Markets Act.[1919] However, structural remedies may only be imposed "either where there is no equally effective behavioural remedy or where any equally effective behavioural remedy would be more burdensome for the gatekeeper concerned than the structural remedy".[1920] Moreover, the Commission may order interim measures against a "gatekeeper", in case of urgency due to risks of serious and irreparable damage for business users or end users, on the basis of a *prima facie* finding of an infringement of Articles 5 and/or 6.[1921] Finally, the "gatekeeper" can offer commitments to ensure compliance with the Digital Markets Act.[1922] The Commission will have to communicate its objections to the "gatekeeper" within 6 months of the opening of the investigation and will have to close the investigation within twelve months of its opening.[1923] The Commission may however extend these deadlines, up to six months, if it is justified on objective grounds and proportionate.[1924]

Third, the European Commission "may conduct a market investigation with the purpose of examining whether one or more services within the digital sector should be added to the list of core platform services or to detect types of practices that may limit the contestability of core platform services or may be unfair and which are not effectively addressed by [the Digital

[1913] See Article 3.1.c) of the Proposal for a Digital Markets Act.
[1914] Article 15.4 of the Proposal for a Digital Markets Act. In this regard, only the obligations provided at Article 5.b) and Article 6.1.e), f), h) and i) can be declared applicable.
[1915] Article 16.1 of the Proposal for a Digital Markets Act.
[1916] See Articles 25 and 26 of the Proposal for a Digital Markets Act.
[1917] Article 16.3 of the Proposal for a Digital Markets Act.
[1918] Article 16.4 of the Proposal for a Digital Markets Act.
[1919] Article 16.1 of the Proposal for a Digital Markets Act.
[1920] Article 16.2 of the Proposal for a Digital Markets Act.
[1921] Article 22 of the Proposal for a Digital Markets Act.
[1922] Article 23 of the Proposal for a Digital Markets Act.
[1923] Articles 16.1 and 16.5 of the Proposal for a Digital Markets Act.
[1924] Article 16.6 of the Proposal for a Digital Markets Act.

Markets Act]".[1925] In such cases, it will have to issue a public report within 24 months from the opening of the investigation, which shall, where appropriate, be accompanied by proposals to amend the list of "core platform services" and by delegated acts amending the obligations laid down in Articles 5 and 6 of the Digital Markets Act.[1926]

b) Competition law may not be sufficient on itself: growing call for *ex ante* legislations imposing data sharing

320. While the three suggestions presented above could indeed reduce, to some extent, the time-consuming process of competition intervention and could allow competition authorities to better tackle systemic competition problems, it is increasingly argued that "competition policy alone cannot address all the systemic problems (…) [and that] additional rules may be needed to ensure contestability, fairness and innovation and the possibility of market entry".[1927] Indeed, even if the competition process is sped up through the above-mentioned suggestions, competition law intervention would still require substantial amounts of time to be implemented. In digital markets where quick reactions are indispensable, this serves as a key rationale for complementing competition law intervention with *ex ante* legislations imposing B2B data sharing, which would, notably, aim at avoiding the apparition of such systemic problems in the first place.[1928]

In fact, as outlined by Ennis and Fletcher, several reports pertaining to the modernisation of competition law echo the proposition that *ex ante* legislations could be a valuable complement to competition law.[1929] For instance, the European Commission's expert report on "Competition Policy for the digital era" suggests there are areas in which *ex ante* legislations might be appropriate to compliment competition law, in particular "where similar issues arise continuously and intervention may be needed on an ongoing basis"[1930], and where "competition law enforcement may be overburdened to deal with the implementation and oversight of interoperability mandates imposed on dominant players".[1931] In the same vein, the Furman report outlines that, in order to spur competition and innovation, *ex ante* obligations, to be monitored by a "Digital Markets Unit", should be imposed on undertakings having a "strategic market status"[1932], in order to complement competition enforcement that "moves too slowly and, intentionally, resolves only issues narrowly focused on a specific

[1925] Article 17.1 of the Proposal for a Digital Markets Act.
[1926] Articles 17.1 and 17.2 of the Proposal for a Digital Markets Act.
[1927] Communication from the Commission, "*Shaping Europe's digital future*", *op. cit.*, p. 9. See also Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 14; L. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. Valletti and M. Van Alstyne, "The EU Digital Markets Act: A Report from a Panel of Economic Experts", *EU Science Hub*, 2021, available at https://ec.europa.eu/jrc/en/publication/eu-digital-markets-act, p. 6.
[1928] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 58.
[1929] S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", *op. cit.*, p. 5-6.
[1930] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 70.
[1931] *Ibid*., p. 126.
[1932] Undertakings that are "in a position to exercise market power over a gateway or bottleneck in a digital market, where they control others' market access" (J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit.*, p. 55).

case".[1933] Similarly, the Stigler Committee report provides that *ex ante* obligations, to be monitored by a "Digital Authority", could be imposed on undertakings having "bottleneck power"[1934], in order to complement competition enforcement.[1935] Finally, as outlined by Kerber, the German experts' report for the modernisation of competition law also stresses that the imposition of *ex ante* data sharing obligations might be more suitable than competition law intervention to address specific problems, such as issues of interoperability and of lack of (real-time) access to data.[1936]

In light of the above, a bicephalous approach to the systemic problems that might emerge on digital markets due to their characteristics[1937] is therefore recommended, whereby an adaptation of competition law rules to the digital environment should be complemented by the creation of *ex ante* legislations imposing B2B data sharing.[1938] These legislations[1939] will be further addressed in Chapter 3.

[1933] *Ibidem*. See also Competition and Markets Authority, "Online platforms and digital advertising: Market study final report", *op. cit.*, p. 322-323.
[1934] Bottleneck power "describes a situation where consumers primarily single-home and rely upon a single service provider, which makes obtaining access to those consumers for the relevant activity by other service providers prohibitively costly" (Stigler Committee on Digital Platforms, "Final Report*"*, *op. cit*., p. 32).
[1935] *Ibid.*, p. 100-101.
[1936] W. Kerber, "Updating Competition Policy for the Digital Economy?", *op. cit.*, p. 38-39; H. Schweitzer, J. Haucap, W. Kerber and R. Welker, "Modernising the law on abuse of market power: Executive summary*"*, *op. cit.*, p. 10.
[1937] See Part I, Chapter 2, Section B, c).
[1938] See Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 5 and 13-14; European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 10.
[1939] See, for instance, the Proposal for a Digital Markets Act.

Chapter 2. Articulation between data protection and competition law

321. In the previous Chapter, it has been outlined that refusals to share data could lead to three types of competition law infringements[1940], and that, for each of these infringements, a potential remedy could be to impose on the large data holder an obligation to share (some of) its data with several third parties.[1941] Yet, as the data sharing remedy will likely cover personal data pertaining to multiple individuals, the personal data protection rules will need to be considered.[1942] Therefore, this Chapter will analyse how a competition authority's decision imposing to share personal data with a third party can be compatible with the General Data Protection Regulation ("GDPR")[1943] (**Section B**).

Prior to delving in such analysis, this Chapter will set the focus on another important friction point emerging from the articulation between competition and data protection law, namely the fact that several authors have started to put the spotlight on the potential anti-competitive effects of the GDPR, as this regulation might increase concentration in personal data and data-related markets (**Section A**).[1944]

Section A. Data protection and competition law: friends or foes regarding data sharing?

322. Even if it generates benefits, data sharing is not cost-free.[1945] On the one hand, it might entail economic costs. Indeed, data collection and processing, and consequently data sharing, entails costs for the data holder, and data sharing obligations might create disincentives for data collection and processing.[1946] The efficiency gains stemming from sharing (increased competition and innovation from third parties) shall be carefully weighed against the

---

[1940] See Part III, Chapter 1, Sections A to C.

[1941] See Part III, Chapter 1, Section D.

[1942] J. Haucap, "A German approach to antitrust for digital platforms", in *Digital Platforms and Concentration - Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (ed.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 12.

[1943] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), *OJ L 119*, 4 May 2016.

[1944] M. Gal and O. Aviv, "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*, September 2020, Volume 16, Issue 3, p. 349-391; T. Zarsky, "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review*, 2017, Vol. 47, No. 4(2), p. 995-1020; T. Zarsky, "The Privacy–Innovation Conundrum", *Lewis & Clark Law Review*, 2015, Vol. 19, No. 1, p. 115-168; D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech", *TILEC Discussion Paper DP 2020-012*, May 2020, available at https://ssrn.com/abstract=3598130; G. Johnson and S. Shriver, "Privacy & market concentration: Intended & unintended consequences of the GDPR", March 2020, available at https://ssrn.com/abstract=3477686.

[1945] B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing: an economic and legal analysis", *EU Science Hub*, 2020, available at https://ssrn.com/abstract=3658100, p. 5.

[1946] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era – Final report", 2019, available at http://ec.europa.eu/competition/publications/reports/ kd0419345enn.pdf, p. 76-77; P. Larouche, "The European Microsoft case at the crossroads of competition policy and innovation", *Antitrust Law Journal*, 2008, n° 75, p. 616-620; B. Martens, A. de Streel, I. Graef, T. Tombal and N. Duch-Brown, "Business to business data sharing", *op. cit.*, p. 5.

efficiency gains stemming from the data holder's data-driven network effects and economies of scope, scale and speed.[1947]

On the other hand, it might entail societal costs. Indeed, data sharing might create tensions with the GDPR, which aims to frame the use of personal data in the European internal market. In order to do so, this instrument aims at reaching an equilibrium between the fundamental right of the protection of personal data, on the one hand, and the fundamental right of the freedom to conduct a business, on the other hand.[1948] As technological developments and globalisation have transformed the economy, one of the aims of the GDPR is to facilitate the free flow of personal data within the European Union in order to support the development of the digital economy across the internal market.[1949] In this sense, the GDPR supports data sharing. However, the GDPR also aims at ensuring a high level of personal data protection and creating the necessary trust, by providing more control to the data subjects on "their" data.[1950] It is this second objective that might generate tensions with data sharing. Indeed, data sharing will often cover both personal[1951] and non-personal data mixed in the same dataset[1952], and favouring data sharing might lead to the broader dissemination of such personal data and to a loss of control by the data subjects.

Perhaps unsurprisingly, large data holders have started to use data protection considerations to justify refusals to share data with third parties[1953], and it is difficult to evaluate the legitimacy of such claims (dynamic nature of the notion of personal data, compliance with the purpose limitation principle,…).[1954] To some extent, this is echoed by the European Data Protection Supervisor, which calls "for cautious approach towards initiatives aimed at compulsory access to personal data in the competition context, i.e. access to personal data held by the incumbent undertaking by its competitors. Such sharing and access to data among competitors must be balanced against other policy concerns, especially data protection".[1955] These large data holders' behaviour has led to growing concerns, detailed in sub-section a), that the GDPR might limit competition and increase concentration on the data markets.

[1947] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability: case studies and data access remedies", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/, p. 75.
[1948] Recital 4 of the GDPR.
[1949] Recital 6 of the GDPR.
[1950] Recital 7 of the GDPR.
[1951] "Any information relating to an identified or identifiable natural person ('data subject')" (Article 4.1 of the GDPR).
[1952] I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, September 2018, available at http://ssrn.com/abstract=3256189; C. Wendehorst, "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 329-330.
[1953] See point 255. See for instance E. Egan, "Data Portability and Privacy", *Facebook White Paper*, September 2019, available at https://iapp.org/media/pdf/fb_whitepaper_sep_2019.pdf.
[1954] I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy" *op. cit.*, p. 10-11.
[1955] European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf, p. 12.

a) Growing concern that the GDPR limits competition and increases concentration

323. According to several authors, this use of data protection considerations by large data holders to justify refusals to share data with third parties, combined with the fact that these undertakings can better sink the large implementation costs of the GDPR than smaller competitors that are disproportionally burdened by this instrument, could create some serious competition issues.[1956] Indeed, this creates the paradoxical situation in which a tool that was adopted to empower individuals by providing them more control on "their" data[1957], and consequently aimed at restricting the data controllers' power on data, is actually used (although sometimes possibly as a pretext to justify controversial strategies)[1958] by large data holders in order to raise entry barriers on the data market vis-à-vis third parties. For example, taking the example of Google, Geradin *et al.* outline that:

> "Google has used the GDPR – or privacy concerns more generally – as an excuse to engage in practices that have strengthened its control on the ad tech ecosystem to the detriment of advertisers, publishers and smaller rivals. This could be referred to as the "weaponization" of the GDPR, i.e. the use of the GDPR by Google as a strategic tool to strengthen its grip on the ad tech market. Because of its market power, Google has become a de facto privacy regulator[1959] able to dictate to rival advertisers, publishers and rival ad tech players its interpretation of the GDPR and other privacy legislation, which is a worrying trend that needs to be countenanced".[1960]

[1956] See J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit*., p. 99. See also M. Gal and O. Aviv, "The Competitive Effects of the GDPR", *op. cit.*, p. 349-391; D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*; J. Campbell, A. Goldfarb and C. Tucker, "Privacy Regulation and Market Structure", *Journal of Economics & Management Strategy*, vol. 24, issue 1, 2015, p. 47-73; J. Jia, G. Zhe Jin and L. Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment", November 2019, available at https://papers.ssrn.com/abstract=32789128; T. Zarsky, "Incompatible: The GDPR in the Age of Big Data", *op. cit.*, p. 995-1020; T. Zarsky, "The Privacy–Innovation Conundrum", *op. cit.*, p. 115-168. For empirical evidence of this increased concentration, see G. Johnson and S. Shriver, "Privacy & market concentration", *op. cit*.

[1957] Recital 7 of the GDPR provides that "natural persons should have control of their own personal data".

[1958] For examples of cases in which Google potentially used data protection rationales as a pretext to justify controversial strategies, see D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 27-35. See also the UK Competition and Markets Authority's formal investigation into Google's "Privacy Sandbox" project, which "would disable third party cookies on the Chrome browser and Chromium browser engine and replace them with a new set of tools for targeting advertising and other functionality that they say will protect consumers' privacy to a greater extent" (Competition and Markets Authority, "CMA to investigate Google's 'Privacy Sandbox' browser changes", 8 January 2021, available at https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes).

[1959] It should be outlined here that this situation derives from the principle of accountability of the GDPR (Article 5.2) and is, as such, not specific to large data holders. Indeed, according to this accountability principle, any data controller is responsible for the application of, and should demonstrate compliance with, the GDPR. As such, any data controller could thus be seen as its own "first line *de facto* privacy regulator", while data protection authorities (the "official" regulators) come as a second line. However, the fact that large data holders, such as Google, hold troves of data and are capable of having an unprecedented impact on the individuals explains why the focus is set on these actors, as the results of their "first line *de facto* privacy refulation" can be significantly more problematic than that of a small data controller.

[1960] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 6.

For Gal and Aviv, the GDPR thus "limits competition and increases concentration in data and data-related markets, and potentially strengthens large data holders. It also further reinforces the already existing barriers to data sharing in the EU, thereby potentially reducing data synergies that might result from combining different datasets controlled by separate entities".[1961] These authors notably argue that while sharing data with third parties often entails high hurdles, data can circulate much more easily within the broad ecosystems of large data holders[1962], which they have constituted through market expansion and through mergers and acquisitions.[1963] In personal data protection terms, it could be argued that the data controller is the same throughout the whole ecosystem, namely the large data holder (Google, Facebook, Amazon…), as it is very likely that this large data holder will determine the purposes and means of the processing of the personal data in the different products/services of the ecosystem.[1964] Hypothesis of joint controllership are nevertheless also possible.[1965]

324. These critiques fit in the broader line of academic work arguing that these large data holders engage in "envelopment" tactics, in order to strengthen their position in the data markets.[1966] These envelopment tactics are often relied upon in data driven markets, and have notably been used by Google, Microsoft, LinkedIn or eBay.[1967] Some of these large undertakings have even engaged in "envelopment strategies through privacy policy tying"[1968], which is a strategy through which "the enveloper requests consumers to grant their consent to combining their data in both [the] origin and target market[s]".[1969] In short, if a user wants to use one of the services offered by the enveloper, she must consent to the circulation of her data across the entirety of the enveloper's ecosystem of services. This data combination allows the enveloper to entrench its dominant position in the origin market and to expand it in the other markets, as it can monetise data from each of its services in all of its other services.[1970]

[1961] M. Gal and O. Aviv, "The Competitive Effects of the GDPR", *op. cit.*, p. 352.
[1962] *Ibid*., p. 361-369.
[1963] For instance, since 2008, Google has acquired 168 undertakings (notably Waze, YouTube or DoubleClick that were potential competitors), Facebook has acquired 71 undertakings (including Instagram and WhatsApp that were also arguably potential competitors), and Amazon has acquired 60 undertakings, which is a respective average of around 15, 6 and 5 acquisitions per year (Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf, p. 9; Lear, "Ex-post Assessment of Merger Control Decisions in Digital Markets – Final Report", 9 May 2019, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803576/CMA_past_digital_mergers_GOV.UK_version.pdf, p. ii).
[1964] Article 4.7 of the GDPR.
[1965] Article 26 of the GDPR. See also European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 1.0, 2 September 2020, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.
[1966] See point 84. T. Eisenmann, G. Parker and M. Van Alstyne, "Platform Envelopment", *Strategic Management Journal*, 2011, Vol. 32(12), p. 1270; D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 25-26.
[1967] T. Eisenmann, G. Parker and M. Van Alstyne, "Platform Envelopment", *op. cit.*, p. 1271.
[1968] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", December 2019, available at https://ssrn.com/abstract=3504025.
[1969] *Ibid*., p. 1.
[1970] *Ibid*., p. 5.

This "envelopment through privacy policy tying" also leads to problematic "internal data free-for-all" situations, as large data holders active on separate markets thereby consolidate their various privacy policies, in order to combine the data collected across these various services and to create "unique user super-profiles", which not only represents a major threat for privacy, but also for competition.[1971] Indeed, from a competition perspective, "this form of envelopment may involve a potential exploitative abuse – the coercive tying of privacy policies – and a possible exclusionary abuse – the monopolization of the target market and the entrenchment of the dominant position in the origin market".[1972] Yet, as will be outlined below, regulatory authorities have been reluctant to address the legality of these "internal data free-for-all" practices.[1973]

325. While the above findings raise troubling concerns about the effect of the GDPR on competition, they seem to rely on the double premise that: i) the GDPR is more lenient towards personal data re-use within the ecosystem of these large data holders than it is towards the sharing of this personal data with third parties[1974]; and that ii) the way in which these large data holders re-use this data within their ecosystem complies with data protection law.[1975] Sub-section b) will assess whether these premises are accurate.

b) Challengeable nature of the premises on which this concern relies

326. In fact, these two premises can be challenged from a theoretical point of view. On the one hand, the same data protection principles and standards apply, whether data is shared internally in an ecosystem or with third parties. On the other hand, it is questionable whether these large data holders use personal data within their ecosystem in a way that complies with data protection law.

1. Premise 1: the GDPR is more lenient towards personal data re-use within the ecosystem of large data holders than it is towards the sharing of personal data with third parties

327. While it is true that, as mentioned above, large actors can better sink the large implementation costs of the GDPR than smaller competitors that are disproportionally burdened by this instrument, this does not imply that the GDPR is more lenient towards personal data re-use within the ecosystem of large data holders than it is towards the sharing of personal data with third parties. Indeed, in both these scenarios, the core principles of the GDPR, listed in Article 5, must be respected.

More specifically, according to the purpose limitation principle, data that has been collected for a specific purpose may not be shared with third parties, nor be re-used internally within the ecosystem of large data holders, if this further processing does not fit within this initial

---

[1971] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 24-26.
[1972] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", *op. cit.*, p. 39.
[1973] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 1.
[1974] M. Gal and O. Aviv, "The Competitive Effects of the GDPR", *op. cit.*, p. 361-369.
[1975] There is indeed a form of "trust" in the fact that these large data holders will use the data within their ecosystem in a way that complies with data protection law (D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 16).

purpose of processing.[1976] The initial purpose of processing must thus be sufficiently detailed in order for the data subject to be able to determine the kinds of processing included, or not, within the specified purpose.[1977] Accordingly, the principle of purpose limitation limits the possibility for large data holders to use data for any contingent purpose, as they cannot rely on broadly defined purposes as a justification to circulate their users' personal data within their ecosystem.[1978]

Rather, both internal re-use and sharing with third parties constitute further processing. If this further processing does not fit within this initial purpose of processing, this amounts to a new processing activity, distinct from the initial one, which requires a new lawful basis of processing, unless this new processing is compatible with the initial purpose[1979] (although this latter point is controversial[1980]).[1981] If the further processing is deemed to be "incompatible" with the initial purpose for which the data has been collected, this further processing may only be carried out if the data subjects have consented to it or if it is necessary to comply with a legal obligation.[1982]

328. It could be tempting to rely on this last point to argue that large data holders can collect such consents for internal data re-use, serving as a lawful basis of processing for the incompatible further re-use, more easily than other actors wishing to collect consents for data sharing, as the data subjects are already using the large data holders' services and ecosystem. Yet, it is interesting to point out that the European Commission's proposal for a Digital

---

[1976] Article 5.1.b) of the GDPR.

[1977] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 15. See also I. Hahn, "Purpose Limitation in the time of Data Power: Is there a way forward?", *European Data Protection Law Review*, 2021, Volume 7, Issue 1, p. 31-44.

[1978] S. Ranchordás and G. De Gregorio, "Breaking Down Information Silos with Big Data: A Legal Analysis of Data Sharing", *University of Groningen Faculty of Law Research Paper Series No. 44/2019*, September 2019, available at https://ssrn.com/abstract=3466313, p. 24. See also I. Hahn, "Purpose Limitation in the time of Data Power: Is there a way forward?", *op. cit.*; Brave, "Inside the Black Box: A Glimpse of Google's Internal Data Free-for-All", 2020, available at https://brave.com/wp-content/uploads/2020/03/Inside-the-Black-Box.pdf.

[1979] To be clear, this does not mean that this "compatible" new processing will not require a lawful basis of processing *at all*. Indeed, every processing needs to rely on a lawful basis of processing (Article 6.1 of the GDPR). Rather, what this means is that this "compatible" new processing will not require a *new* lawful basis of processing, distinct from the one that serves as the basis for the initial processing, because it fits within this initial processing. This "compatible" new processing thus, in fact, relies on a lawful basis of processing, namely the *same one* as the one that serves as a basis for the initial processing.

[1980] C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit.*, p. 335-336.

[1981] Article 6.4 and Recital 50 of the GDPR. On these matters, see C. de Terwangne, "Article 5. Principles relating to processing of personal data", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 309-320; W. Kotschy, "Article 6. Lawfulness of processing", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 321-344; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union, 2018, p. 122-125; C. de Terwangne, "Les principes relatifs au traitement des données à caractère personnel et à sa licéité", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 98-104; F. Gaullier, "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *Communication commerce électronique*, 2018/4, p. 45-52.

[1982] Article 6.4 of the GDPR. See also C. de Terwangne, "Article 5. Principles relating to processing of personal data", *op. cit.*, p. 316; W. Kotschy, "Article 6. Lawfulness of processing", *op. cit.*, p. 343; F. Gaullier, "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *op. cit.*, p. 51.

Markets Act[1983] provides that "gatekeepers" shall not make the obtaining of this consent more burdensome for third parties than for its own services.[1984] Moreover, this raises the question of the quality of the consents collected by these large data holders in order to justify their "internal data free-for-all".

Indeed, consent must be "freely given, specific, informed and unambiguous".[1985] First, consent must be *informed and unambiguous*, which implies that the data holder must be completely transparent towards the processing operations to which the data subjects consent. To do so, they shall take appropriate measures to provide any information referred to in Articles 13 and 14 of the GDPR to the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[1986] Second, consent must be *specific*, which implies that it has to be sufficiently granular and that the data subjects must understand the specific purposes to which they separately consent.[1987] Thirdly, and perhaps more importantly when it comes to internal re-use by large data holders, consent must be *freely given*. In this regard, the GDPR outlines that "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".[1988] This will especially be the case if there is a clear imbalance between the data controller and the data subject, and if the controller "does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance".[1989] These are the requirements of granularity and of absence of conditionality.[1990] Therefore, if

---

[1983] Proposal for a Digital Markets Act. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.

[1984] Article 11.2 of the Proposal for a Digital Markets Act.

[1985] Article 4.11 of the GDPR. See also Article 7 of the GDPR. For an interesting case analysing the validity of consent, see Norwegian Data Protection Authority, *Grindr LLC* (Advance notification), 24 January 2021, decision no. 20/02136-5, available at https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf.

[1986] Article 12.1 of the GDPR. See also Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP 260 rev.01, 11 April 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; R. Polčák, "Article 12. Transparent information, communication and modalities for the exercice of the rights of the data subject", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 398-412; T. Tombal, "Les droits de la personne concernée dans le RGPD", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 409-425.

[1987] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, May 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, p. 14. On consent, see also L. Bygrave and L. Tosoni, "Article 4(11). Consent", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 174-187; E. Kosta, "Article 7. Conditions for consent", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 345-354; C. de Terwangne, "Les principes relatifs au traitement des données à caractère personnel et à sa licéité", *op. cit.*, p. 120-131.

[1988] Recital 42 of the GDPR.

[1989] Recital 43 of the GDPR.

[1990] See European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, *op. cit.*, p. 10-12.

the data holder bundles the data subjects' consent with the acceptance of its terms of services, or if it ties the provision of a contract/service to the requirement to consent to unnecessary processing for the performance of that contract/service, consent will not be deemed to be freely given and will thus not be valid.[1991] In this perspective, if a data subject is required to consent to the circulation of her data throughout the whole ecosystem of the large data holder in order to simply use one of the many services offered by the latter, such a consent should not be considered as being *freely given*. Accordingly, and contrary to what the first premise might suggest, large data holders cannot rely on consents obtained in bulk, and which do not provide sufficient information regarding all of the specific data processing purposes that they are supposed to cover, as a justification to freely circulate their users' personal data within their ecosystem ("internal data free-for-all"). This has been confirmed by the Norwegian Data Protection Authority in its *Grindr* case, where it ruled that, since *Grindr* bundled the data subject's consent to the sharing of her personal data with advertisers with the acceptance of the privacy policy as a whole, such consent was in breach of the granularity requirement.[1992] Consequently, the consent was deemed invalid, as it was not *freely given* and thus deprived the data subjects of real control.[1993]

329. Moreover, the large data holders will also have to comply with the data minimisation principle, according to which only the adequate, relevant and necessary data for the fulfilment of the specific purpose of processing shall be processed.[1994] This implies that, in combination with the purpose limitation principle, the categories and amount of data that may be processed (for each internal re-use or for data sharing with third parties) should be limited to what is necessary to meet this purpose. Therefore, even if large data holders have collected troves of personal data from their users in the context of a first purpose of processing, they will not necessarily be allowed to re-use any/all of this data for a further purpose of processing. Rather, they shall only process the data that is adequate, relevant and necessary for this re-use. On the other hand, data within their ecosystem that would merely be useful, but not necessary, should not be re-used, as "this necessity requirement not only refers to the quantity, but also to the quality of personal data".[1995]

330. In light of the above, the argument can be made that the GDPR is *not* more lenient towards personal data re-use within the ecosystem of these large data holders than it is towards the sharing of this personal data with third parties. Indeed, as outlined in a joint statement of the UK competition and data protection authorities, "neither competition nor data protection regulation allows for a 'rule of thumb' approach, where intra-group transfers of personal data are permitted while extra-group transfers are not. Under both data protection

---

[1991] *Ibid*., p. 10.
[1992] Norwegian Data Protection Authority, *Grindr LLC* (Advance notification), 24 January 2021, decision no. 20/02136-5, available at https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf, p. 9-10.
[1993] *Ibid*., p. 10-12.
[1994] Article 5.1.c) of the GDPR.
[1995] C. de Terwangne, "Article 5. Principles relating to processing of personal data", *op. cit.*, p. 317.

law and competition law, a careful case-by-case assessment is needed".[1996] This first premise is thus questionable.

2. Premise 2: the way in which large data holders re-use this data within their ecosystem complies with data protection law

331. The second premise is that there is a form of "trust" in the fact that these large data holders will use the data within their ecosystem in a way that complies with data protection law. According to Geradin *et al*., this trust derives from three assumptions, namely that large data holders have the necessary resources to comply with the GDPR; that they must be compliant as they will be closely monitored by data protection authorities in light of their structural importance; and that they will be compliant because, as their business model is based on data collection and processing, a data protection scandal could greatly impact their profits.[1997] While the first assumption seems established, the other two can be challenged.[1998]

332. Regarding the third assumption, it can be questioned to what extent a potential data protection scandal would truly impact these large data holders' business model, especially if the data subjects are locked-in their services and face important switching costs, due to these large data holders' network effects and economies of scale, scope and speed.[1999] Indeed, in such situations, viable alternatives to the services offered by these large data holders may not exist and data subjects may thus not be able to exercise control on "their" data by "penalising" (repeated) violations of their right to personal data protection committed by these large data holders. Arguably, this might explain why Facebook did not lose many users after the "Cambridge Analytica" scandal, despite the fact that it faces civil class-action lawsuits[2000], and that was fined 1 million euros by the *Garante per la protezione dei dati personali* (Italian Data Protection Authority) and £500.000 by the *Information Commissioner's Office* (UK's Data Protection Authority) for allowing Cambridge Analytica to collect and use data from its users.[2001]

333. Regarding the second assumption, it is questionable whether these large data holders process their users' data within their ecosystem in a way that complies with data protection law. Indeed, coming back to the purpose limitation principle outlined above[2002], it can be questioned whether the vague purposes mentioned by large data holders in their privacy

---

[1996] Competition and Markets Authority and Information Commissioner's Office, "Competition and data protection in digital markets: a joint statement between the CMA and the ICO", 19 May 2021, available at https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, p. 26.
[1997] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 16.
[1998] *Ibid*., p. 14-16.
[1999] See M. Stucke and A. Grunes, *Big Data and Competition Policy*, Oxford, Oxford University Press, 2016; D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 339-381.
[2000] See https://www.mydataismine.com/. See also S. Bodoni, "Facebook Targeted in the U.K. Legal Action Over Cambridge Analytica", *Bloomberg*, 28 October 2020, available at https://www.bloomberg.com/news/articles/2020-10-28/facebook-targeted-in-u-k-legal-action-over-cambridge-analytica.
[2001] Garante per la protezione dei dati personali, *Facebook*, 14 June 2019, decision no. 9121486, available at https://perma.cc/LHV7-2THY; Information Commissioner's Office, *Facebook Ireland and Facebook Inc*, 24 October 2018, available at https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf.
[2002] See point 327. Article 5.1.b) of the GDPR.

policies ("provide our services", "improve our services", "develop new services") are specific enough to comply with the purpose limitation principle, as these purposes are not clear, specified and explicit.[2003] This is supported by the fact that the Article 29 Working Party (today the European Data Protection Board) expressly stated that vague or general-purposes will usually not meet this specificity requirement[2004], which has been confirmed by the Norwegian Data Protection Authority in its *Grindr* case.[2005] Moreover, these vague purposes, leading to "internal data free-for-all" practices by these large data holders, could also be seen as contradicting with the proportionality principle enshrined in the Modernised Convention 108, as this arguably creates an excessive interference with the rights and interests of the data subjects.[2006] Furthermore, this lack of specificity can also be linked to another issue, namely the compliance with the transparency requirement mentioned above.[2007] Indeed, large data holders' ecosystems are complex and obscure to the data subjects, and it is highly doubtful whether the vague and general information provided in their terms of services meet the thresholds of the transparency requirement.[2008] In fact, in its *Grindr* case, the Norwegian Data Protection Authority ruled that such requirement would not be met if the consent request appeared amongst all other information in a long privacy policy, as such request should be highlighted.[2009]

Additionally, the validity of the consent collected by large data holders through "privacy policy tying", leading to "internal data free-for-all" situations, can be questioned.[2010] Indeed, the *informed and unambiguous* nature of data subjects' consent can be challenged, as privacy policies are drafted in such a way that "regular people" do not understand them (if they even read them, which is often not the case) and as data controllers often resort to dark patterns.[2011] These dark patterns can make it more difficult to reject some terms of the privacy policy rather than to accept them all, or can prevent the data subject from using the service if she

---

[2003] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 25. See also I. Hahn, "Purpose Limitation in the time of Data Power: Is there a way forward?", *op. cit.*; Brave, "Inside the Black Box: A Glimpse of Google's Internal Data Free-for-All", *op. cit.*

[2004] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 16.

[2005] Norwegian Data Protection Authority, *Grindr LLC* (Advance notification), 24 January 2021, decision no. 20/02136-5, available at https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf, p. 13.

[2006] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, CM/Inf(2018)15-final, Article 5.1: "Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake".

[2007] See point 328.

[2008] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 25.

[2009] Norwegian Data Protection Authority, *Grindr LLC* (Advance notification), 24 January 2021, decision no. 20/02136-5, available at https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf, p. 14.

[2010] On the GDPR requirements for consent, see point 328.

[2011] On these dark patterns, see M. Nouwens, I. Liccardi, M. Veale, D. Karger and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", *CHI Conference on Human Factors in Computing Systems*, April 2020, available at https://arxiv.org/abs/2001.02479; P.-O. Pielaet, "La *privacy by design* à l'épreuve des « dark patterns »", *R.D.T.I.*, 2020, Issue 3, p. 33-45.

does not consent to all the terms.[2012] This has been confirmed by the Norwegian Data Protection Authority in its *Grindr* case.[2013] Moreover, because the data subject often has no other choice than to consent to the totality of the terms of services in order to use the service, this consent may be deemed as not being *freely given* if the large data holder is dominant on a specific market and no realistic alternatives are available for the data subject.[2014] Indeed, if a data subject is required to consent to the circulation of her data throughout the whole ecosystem of the large data holder in order to simply use one of the many services offered by the latter (but for which there are no realistic alternatives), such a consent should not be considered as being *freely given*. However, such practices are applied and this allows these large data holders to expand their market power across data markets, as, in order to use the dominant's firm service, data subjects are usually required to consent to the collection, processing and combination of data for other services of the large data holders' ecosystem as well.[2015]

334. The above critiques of the legality of personal data processing within these ecosystems are not merely theoretical, as large data holders have been fined by data protection authorities for infringing personal data protection legislation.[2016] For instance, on the 9th of December

---

[2012] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", *op. cit*., p. 26. See also M. Botta and K. Wiedemann, "The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey", *Antitrust Bulletin*, vol. 64, issue 3, 2019, p. 428-446.

[2013] Norwegian Data Protection Authority, *Grindr LLC* (Advance notification), 24 January 2021, decision no. 20/02136-5, available at https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf, p. 9-12 and 15-16.

[2014] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", *op. cit*., p. 26. See also D. Clifford, I. Graef and P. Valcke, "Pre-formulated declarations of data subject consent – Citizen-consumer empowerment and the alignment of data, consumer and competition law protections", *CiTiP Working Paper 33/2017*, February 2018, available at https://ssrn.com/abstract=3126706, p. 34-44; K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *IIC*, 2020, Volume 51, Issue 9, p. 1177-1178.

[2015] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", *op. cit*., p. 34.

[2016] See https://www.enforcementtracker.com/. See for example: (FR) Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, Deliberation of the Restricted Committee SAN-2019-001, available at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf; Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-012, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706; Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-013, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729; (BE) Autorité de Protection des Données, *X c/ Google*, 14 July 2020, decision no. 37/2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf; (SWE) Datainspektionen, *Google LLC*, 10 March 2020, decision no. DI-2018-9274, available at https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf; (IR) Data Protection Commission, *Twitter International Company*, 9 December 2020, decision no. IN-19-1-1, available at https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf; (IT) Garante per la protezione dei dati personali, *Facebook*, 14 June 2019, decision no. 9121486, available at https://perma.cc/LHV7-2THY; (UK) Information Commissioner's Office, *Facebook Ireland and Facebook Inc*, 24 October 2018, available at https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf; (NED) Autoriteit Persoonsgegevens, *TikTok Inc*., 9 April 2021, (confidential reference), available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf.

2020, the Irish *Data Protection Commission* fined Twitter 450.000 euros following a bug that had as a consequence that some users' private tweets were made public.[2017] On the 9th of April 2021, the *Autoriteit Persoonsgegevens* (the Dutch Data Protection Authority) fined TikTok 750.000 euros for a breach of its transparency obligations under the GDPR (Article 12.1), as the company did not provide a privacy policy in Dutch to its users – of which an important part are children –, but only provided one in English.[2018] On the 10th of March 2020, the *Datainspektionen* (the Swedish Data Protection Authority) fined Google 7 million euros for a breach of data subject's right to erasure.[2019] Similarly, on the 14th of July 2020, the *Autorité de Protection des Données* (the Belgian Data Protection Authority) fined Google 600.000 euros for the breach of a data subject's right to erasure, and for a breach of the principle of transparency, as Google did not explain sufficiently clearly the motives of its refusal to erase the data subject's data.[2020] In fact, it is interesting to point out that, in this decision, the Belgian Data Protection Authority outlined that large data holders such as Google have a "special responsibility" in applying the GDPR, as their duty to comply with the GDPR should be proportionate with their large turnover and with the broad use of their products/services by data subjects.[2021] This is a clear call for more scrutiny and a stricter enforcement of the GDPR against these large data holders.

335. More notoriously, on the 21st of January 2019, the *Commission Nationale de l'Informatique et des Libertés* (CNIL – the French Data Protection Authority) has fined Google 50 million euros for a lack of transparency and of accessibility of information, as well as for a lack of appropriate lawful basis of processing (the consent it had collected from its users was not valid in light of the lack of transparency and information).[2022] The CNIL's decision was confirmed by the French Conseil d'État on the 19th of June 2020, following an appeal by Google.[2023]

In substance, the CNIL found that Google's privacy policy and terms of services did not meet the transparency requirement of Article 12 of the GDPR, as there was an overall lack of accessibility to the information, due to the multi-layer architecture of Google's information

---

[2017] Data Protection Commission, *Twitter International Company*, 9 December 2020, decision no. IN-19-1-1, available at https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf. See also on this case: European Data Protection Board, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, 9 November 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf.

[2018] Autoriteit Persoonsgegevens, *TikTok Inc.*, 9 April 2021, (confidential reference), available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf.

[2019] Datainspektionen, *Google LLC*, 10 March 2020, decision no. DI-2018-9274, available at https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf.

[2020] Autorité de Protection des Données, *X c/ Google*, 14 July 2020, decision no. 37/2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf.

[2021] Autorité de Protection des Données, *X c/ Google*, 14 July 2020, § 175 (vii).

[2022] Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, Deliberation of the Restricted Committee SAN-2019-001, available at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf.

[2023] Conseil d'État, *Société Google LLC*, 19 June 2020, case no. 430810, available at https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042040546/.

provision[2024], which is excessively spread-out across multiple documents.[2025] Moreover, the CNIL held that the information was not clear and intelligible, as it did not allow data subjects to sufficiently understand the various purposes of processing, which were too generic, imprecise and incomplete.[2026] This was considered as being especially problematic in light of the very large amount of data processed[2027], including some very intimate categories of data.[2028] Regarding the validity of the consents collected by Google from its users, the CNIL ruled that the deficiencies in terms of transparency and information outlined above led to the conclusion that the data subjects' consents were not sufficiently *informed*.[2029] Finally, the CNIL found that the data subjects' consents were not *unambiguous*, as they were not given through a positive act, because the option of giving specific consent for each purpose should have been given before the options "Accept all" or "Refuse all", and should not have been subject to the necessity for data subjects to perform any particular action, such as clicking on "More options".[2030] This also echoes the need to have a stricter application of the data protection by design principle.[2031] Indeed, these large data holders increasingly resort to "nudging techniques" in order to ensure that data subjects act in a way that best meets their own interests, rather than the data subjects' interests.[2032] A clear example is dark patterns used to collect consent, as the data subjects are often presented with a first alternative between "Agree to all" and "More options", which requires extra efforts from the data subjects as they can only express their preferences on a second screen (where the boxes are even sometimes pre-ticked).[2033] This discourages the data subjects from voicing their true privacy preferences, especially when a nudging message appears saying that they will lose functionality if they do not consent to all/some of the processing.[2034]

[2024] In this regard, it is worth making a small digression in order to suggest that another type of multi-layer approach could be further investigated to solve this transparency issue. Indeed, the transparency requirement is complex to meet, as a fine line must be found between providing too much or too little information. This is because providing too little and vague information might not be specific enough, while providing too much information might make the privacy policy unreasonably long and might discourage (even further) people from reading it. To solve this issue, a three-layered approach, inspired from the Creative Commons Licences could be adopted (see https://creativecommons.org/about/cclicenses/). The first layer would be composed of standardised icons, easily understandable by the data subjects, as envisaged in Article 12.7 of the GDPR. The second layer would be composed of a "shortened privacy policy", explaining in clear and intelligible terms the main aspects of the processing (types of data collected, purposes, lawful basis…). The third layer would contain the full privacy policy, with all of the detailed information.

[2025] Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, §§ 96-103.

[2026] *Ibid*., §§ 104-128.

[2027] Arguably, this finding can be linked to the Belgian Data Protection Authority's finding that large data holders have a "special responsibility" in applying the GDPR (see point 334), as this special responsibility would also derive from the fact that they process very large amounts of data.

[2028] Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, § 109.

[2029] *Ibid*., §§ 141-148.

[2030] *Ibid*., §§ 149-167.

[2031] Article 25 of the GDPR.

[2032] M. Nouwens, I. Liccardi, M. Veale, D. Karger and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", *op. cit.*; P.-O. Pielaet, "La *privacy by design* à l'épreuve des « dark patterns »", *op. cit.*, p. 33-45.

[2033] M. Nouwens, I. Liccardi, M. Veale, D. Karger and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", *op. cit.*, p. 5-6.

[2034] *Ibid*., p. 9.

336. Recently, on the 7th of December 2020, the CNIL fined Google 100 million euros, notably for having placed advertising cookies on the computers of users of www.google.fr, residing in France, without prior consent or satisfactory information.[2035] In substance, the CNIL ruled that the information provided by Google, both in the banner and in the pop-up window, did not allow users residing in France, when they arrived on www.google.fr, to be clearly informed beforehand of the existence of processing allowing the access to information contained in their terminal and allowing the writing of such information (cookies).[2036] Consequently, the information provided by Google did not allow these users to be clearly informed beforehand about the purpose of these processing and of the means made available to them in order to oppose to their use.[2037] Moreover, it ruled that since 4 out of the 7 cookies written on the users' terminal pursued an advertising purpose, Google should have obtained the users' explicit consent before putting them on their terminal.[2038] This is because these cookies do not have, as exclusive purpose, the enabling or facilitation of communication by electronic means and they are not strictly necessary for the provision of an online communication service at the express request of the user.[2039]

On the same day, the CNIL also fined Amazon 35 million euros for substantially the same reasons.[2040] Here as well, it ruled that since more than 40 cookies written on the users' terminal pursued an advertising purpose, Amazon should have obtained the users' explicit consent before putting them on their terminal[2041], as they did not exclusively aim to enable or facilitate communication by electronic means, and as they were not strictly necessary for the provision of an online communication service.[2042] Moreover, it held that the information, relating to the cookies, provided by Amazon to the users was either incomplete or inexistent.[2043] Indeed, it ruled that the information banner shown on the homepage of www.amazon.fr only contained a general and approximative description of the purpose of the cookies, and that it did not provide any information on the means made available to the users in order to oppose to their use.[2044] The CNIL further held that the breach of the information requirement was even more flagrant for users arriving on www.amazon.fr through an

---

[2035] Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-012, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706.
[2036] *Ibid*., § 82.
[2037] *Ibidem*. In this regard, it is worth pointing out that even if Google took steps, during the procedure, to provide more information beforehand, the CNIL considered that this information was still too imprecise, as it still did not enable the users to understand the purposes of processing nor the means made available to them in order to oppose to their use (see §§ 86-94).
[2038] *Ibid*., § 100.
[2039] *Ibidem*. The CNIL however acknowledged that Google had solved this issue during the procedure (see § 102).
[2040] Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-013, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729.
[2041] *Ibid*., §§ 87-90.
[2042] *Ibid*., § 88.
[2043] *Ibid*., § 92.
[2044] *Ibid*., §§ 94-95.

advertisement published on the website of a third party as, in that case, no information at all was provided to the users regarding these cookies.[2045]

337. One must however acknowledge that these interventions by data protection authorities have been sporadic and that the fines imposed are quite derisory in comparison with these large data holders' turnovers.[2046] A notable exception to this is the Luxembourg's *National Data Protection Commission* decision to impose a 746 million euros fine on Amazon for a lack of valid consent as basis for its targeted advertising purposes, which has been issued on the 15th of July 2021, but is unfortunately not yet available on the authority's website.[2047] While this decision could mark the beginning of a new trend of more drastic interventions against Big Tech actors, it could also remain a remarkably exceptional island in a sea of restrained intervention by data protection authorities.

Indeed, up to now, and with the exception of this latest decision, there has been a form of impunity of the conduct of such data holders, which arguably continue to rely on "internal data free-for-all" practices and to ignore the core principles of the GDPR, and this allows them to obtain a considerable competitive advantage over GDPR-compliant competitors.[2048] In this perspective, it can be questioned whether these large data holders have solely acquired their strong market position through competition on the merits, or whether this position was, at least partly, acquired through dubious practices in a pre-GDPR era where there was less global awareness about these personal data protection issues, and where there was, in fact, uncertainty as to whether these non-European actors were bound by the rules of the Data Protection Directive.[2049] In any case, the data advantage that these large data holders have acquired now makes it practically impossible for third parties, in a post-GDPR era, to contest their position while respecting the data protection legislation.

Indeed, despite growing calls for taking personal data protection considerations into account in competition law assessments[2050], these considerations have often been set aside in light of

---

[2045] *Ibid*., §§ 96-97.

[2046] For instance, Google LLC had a turnover of more than 160 billion dollars in 2019, Google Ireland Ltd had a turnover of more than 38 billion euros in 2018, and Amazon Europe had a turnover of approximately 7,7 billion euros in 2019. See Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, §§ 2 and 3; Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, §1.

[2047] See S. Bodoni, "Amazon Gets Record $888 Million EU Fine Over Data Violations", 30 July 2021, available at https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach; L. Adam, "RGPD : Amazon écope d'une amende record à 746 millions d'euros", 30 July 2021, available at https://www.zdnet.fr/actualites/rgpd-amazon-ecope-d-une-amende-record-a-746-millions-d-euros-39926965.htm.

[2048] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 25.

[2049] Indeed, this uncertainty was only resolved through the European Court of Justice's decision in the *Google Spain* case (ECJ, *Google Spain and Google*, 13 May 2014, case C-131/12, EU:C:2014:317).

[2050] See, for instance, W. Kerber, "Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection", *MAGKS Joint Discussion Paper Series in Economics No. 14-2016*, February 2016, available at https://www.econstor.eu/bitstream/10419/144679/1/850599016.pdf; M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit.*; Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data*"*, 10 May 2016, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf; A. Ezrachi and V. Robertson, "Competition, Market Power and Third-Party Tracking", *World Competition: Law and Economics Review*, 2019, Vol. 42, No. 1, p. 5-19; G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *Bocconi Legal Studies Research Paper No.*

the premise that large/dominant data holders would be GDPR-compliant as they would be closely monitored by data protection authorities.[2051] As a result, competition authorities have often been encouraged to keep off the data protection authorities' grass. This has been expressly stated by the European Court of Justice in the *Asnef-Equifax* case, where it held that "any possible issues relating to the sensitivity of personal data are not, *as such*, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection" (emphasis added).[2052] This has also been confirmed by the European Commission in its *Google/DoubleClick* merger decision[2053], and later in its *Facebook/Whatsapp* merger decision, where it stated that "any privacy related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of the EU competition law rules but within the scope of the data protection rules"[2054].[2055] It also followed a similar approach in the *Microsoft/LinkedIn* merger decision.[2056] Yet, as data protection authorities failed to properly monitor these large data holders, the latter have arguably been able to consolidate their strong position in the various data markets through questionable practices in terms of data protection law.

338. Therefore, a lack of data protection enforcement has arguably led to a lack of competition enforcement, and has comforted these large data holders in their "internal data free-for-all" practices. One of the few exceptions to this lack of regulatory intervention is the notorious *Bundeskartellamt'*s case (the German Competition Authority) against Facebook.[2057] In that case, the German Competition Authority found, in interim proceedings, that the firm had abused its dominant position on the German social network market by making it compulsory for users, wishing to use its social network, to consent to the collection, by Facebook, of user data from third party websites[2058] and from other Facebook-owned services (e.g. Instagram and WhatsApp), and to consent to the combination of such data with the user data stemming from the social network.[2059]

2945085, 2 April 2017, available at https://ssrn.com/abstract=2945085, p. 7-9. On the contrary, some argue that data protection and competition law should be kept apart: see G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *op. cit.*, p. 9-11.

[2051] See OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 24-41.

[2052] ECJ, *Asnef Equifax and Administración des Estado*, 23 November 2006, C-238/05, EU:C:2006:734, § 63.

[2053] European Commission, *Google/DoubleClick*, 11 March 2018, case M.4731, § 368.

[2054] European Commission, *Facebook/WhatsApp*, 3 October 2014, case M.7217, § 164.

[2055] G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *op. cit.*, p. 5.

[2056] European Commission, *Microsoft/LinkedIn*, 6 December 2016, case M.8124, §§ 177-179; G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *op. cit.*, p. 5.

[2057] Bundeskartellamt (6th Division), *Facebook*, 6 February 2019, B6-22/16, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf. See also Bundeskartellamt, "Bundeskartellamt prohibits Facebook from combining user data from different sources", 7 February 2019, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[2058] For more details on the potential impact of third party tracking on competition and market power, see A. Ezrachi and V. Robertson, "Competition, Market Power and Third-Party Tracking", *op. cit.*, p. 5-19.

[2059] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 26. See also W. Wils, "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt", *Concurrences*, 2019, issue 3, p. 58-66; K. Wiedemann, "A Matter of Choice:

Indeed, the *Bundeskartellamt* found, on the one hand, that the inclusion of such a requirement in Facebook's terms of service constituted an exploitative abuse to the detriment of users, as it was the result of an unlawful data processing in breach of the principle of transparency and of the requirements for valid consent under the GDPR (Articles 5.1.a), 6.1.a) and 7). On the other hand, it found that this conduct impeded competition, as it unlawfully allowed Facebook to acquire a further competitive data advantage over its competitors, thus elevating entry-barriers and strengthening Facebook's market power.[2060] Although the *Bundeskartellamt*'s decision was based on Section 19(1) of the German Act against Restraints of Competition ("GWB")[2061], some argue that Article 102 TFEU could also be used to sanction the imposition of unfair terms infringing data protection law.[2062] Indeed, it derives from the case law of the European Court of Justice that the "fairness" of trading conditions (Article 102(a) of the TFEU) can be assessed on the basis of principles such as necessity, proportionality or transparency[2063], which are fundamental data protection law principles.[2064] These personal data principles could thus be used as a benchmark to assess the existence of an exploitative abuse under Article 102 TFEU, but this does not imply that any infringement of data protection law will automatically lead to a competition law infringement, as this will be function of the specific circumstances of the case.[2065] Yet, as pointed out by Wils:

> "In the Facebook Decision, the Bundeskartellamt conducts such an examination. In doing so, it finds not only that Facebook's terms of service constitute exploitative business terms to the detriment of consumers, but also that Facebook's conduct impedes competitors in that it gives Facebook access to a large number of further data sources, thus giving Facebook a further competitive edge over its competitors and reinforcing market entry barriers, which in turn strengthen Facebook's market power vis-à-vis consumers. The Facebook decision thus goes well beyond a mere 'recycling' of a finding of infringement of data protection law".[2066]

The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *IIC*, 2020, Volume 51, Issue 9, p. 1169-1170.

[2060] W. Wils, "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt", *op. cit.*, p. 61.

[2061] "Gesetz gegen Wettbewerbsbeschränkungen" (Act against Restraints of Competition, adopted on 26 August 1998 and lastly amended on 19 January 2021). The official English translation of the GWB is available at http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0066.

[2062] W. Wils, "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt", *op. cit.*, p. 63.

[2063] ECJ, *BRT and SABAM*, 21 March 1974, C-127/73, EU:C:1974:25; ECJ, *Der Grüne Punkt – Duales System Deutschland v Commission*, 16 July 2009, C-385/07 P, EU:C:2009:456, § 142; ECJ, *AstraZeneca v Commission*, 6 December 2012, C-457/10 P, EU:C:2012:770, § 93.

[2064] W. Wils, "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt", *op. cit.*, p. 63.

[2065] *Ibidem*. See also J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data: On Data-specific Theories of Harm and Remedies", *Max Planck Institute for Innovation and Competition Research Paper No. 19-05*, 31 May 2019, available at https://ssrn.com/abstract=3364792, p. 33-41.

[2066] W. Wils, "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt", *op. cit.*, p. 63.

339. Yet, Wils' enthusiasm was not shared by all, and some have strongly criticised the *Bundeskartellamt*'s decision[2067], notably in light of the Dusseldorf Higher Regional Court's decision to suspend the effects of the *Bundeskartellamt*'s ruling[2068], as it believed that the competition authority had failed to establish concrete anticompetitive effects and had rather derived them automatically from a violation of the GDPR.[2069] Indeed, the Court held that the competition authority had not established causality between Facebook's market dominance and the content of its terms of services, because "other companies were using similar conditions and the ''abusive'' terms of service were thus not deemed a result of market dominance".[2070] Moreover, the Court was of the opinion that Facebook users were free to refuse to consent to the terms of service, that Facebook had committed no exploitative abuse as competitors could collect the same data from users, and that the *Bundeskartellamt* had failed to demonstrate that Facebook's practices damaged competition, as users did not suffer any financial loss.[2071]

340. However, this decision of the Dusseldorf Higher Regional Court has been overturned by the *Bundesgerichtshof* (German Federal Court of Justice), which confirmed the *Bundeskartellamt*'s approach.[2072] Indeed, the *Bundesgerichtshof* held that there is no serious doubt about Facebook's dominant position in the German social networking market, nor that Facebook is abusing this dominant position through the terms of service sanctioned by the *Bundeskartellamt*.[2073] In reaching such a verdict, the *Bundeskartellamt* focussed on competition policy considerations, rather than on personal data protection concerns.[2074] Indeed, according to the *Bundesgerichtshof*, the decisive factor outlined by the *Bundeskartellamt* to find such an abuse is not that Facebook's data processing infringes the rules of the GDPR, but rather that Facebook's terms of services are abusive because the users have no other choice but to accept the processing of data from third party websites and from other Facebook-owned services (e.g. Instagram and WhatsApp), in order to use Facebook's social network.[2075] For the *Bundesgerichtshof*, "the fact that Facebook does not provide a less "data-intensive" option indicates that it can act on the market irrespective of user preferences,

---

[2067] See for instance P. Këllezi, "Data protection and competition law: non-compliance as abuse of dominant position", *Sui-generis*, 2019, p. 343-359.
[2068] Dusseldorf Higher Regional Court, *Facebook/Bunderskartellamt*, 26 August 2019, VI-Kart 1/19.
[2069] P. Këllezi, "Data protection and competition law: non-compliance as abuse of dominant position", *op. cit.*, p. 344.
[2070] K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1170.
[2071] *Ibidem*; OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 30.
[2072] BGH, *Facebook*, 23 June 2020, KVR 69/19, no. 080/2020. For a comment of this decision, see K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1168-1181.
[2073] See Bundesgerichtshof, "Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook," 23 June 2020, available at https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html.
[2074] K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1170. For more details, see p. 1170-1178.
[2075] See Bundesgerichtshof, "Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook," *op. cit*.

which in turn implies an abuse of dominance".[2076] This lack of choice constitutes an exploitative abuse of the users, as Facebook's access to a considerably larger amount of data than its competitors leads to lock-in effects and switching costs, which are relevant under competition law because competition can no longer effectively exercise its control function due to Facebook's dominant position.[2077] Indeed, it is much more difficult for Facebook's (potential) competitors to compete, as Facebook's strong network effects create high entry barriers, and as competitors are unable to collect as much quantitative and qualitative data about the users, and thus to compete for advertising contracts.[2078]

On the issue of causality, the *Bundesgerichtshof* relied on a normative approach, traditionally applied to exclusionary abuses[2079] rather than to exploitative abuses, to argue that it was Facebook's market dominance that allowed it to adopt terms of services that were not only detrimental to users, but also to competition.[2080] As summarised by Wiedemann, for the *Bundesgerichtshof*, "it does not matter if other, non-market-dominant companies would be factually able to impose the same terms of service on their users, as long as the damage to competition results from the market dominance of the company in question".[2081]

Finally, the *Bundesgerichtshof* outlined that the fact that the lack of choice for Facebook users' also (potentially) affected their right to informational self-determination[2082] and to personal data protection[2083] needed to be factored in the balancing of all the interests involved *in casu*.[2084] Indeed, even if Facebook is not directly bound by human rights because it is a private entity, these users' rights "must be protected from an overly far-reaching commercial exploitation of their personal data".[2085]

Since the *Bundesgerichtshof*'s decision was also rendered in interim proceedings, it remains to be seen whether a different ruling will be made in the main proceedings.[2086] It is also worth

---

[2076] K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1172.
[2077] See Bundesgerichtshof, "Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook," *op. cit*.
[2078] K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1171-1173.
[2079] See ECJ, *Europemballage Corporation and Continental Can Company v. Commission*, 21 February 1973, C-6/72, EU:C:1973:22, §§ 26–27; and ECJ, *Hoffmann-Laroche v. Commission*, 13 February 1979, C-85/76, EU:C:1979:36, § 91.
[2080] K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1172.
[2081] *Ibidem*.
[2082] See German Federal Constitutional Court, *Volkszählungsurteil*, 15 December 1983, 1 BvR 209/83 et al., 65 BVerfGE 1. On informational self-determination, see Part I, Chapter 2, Section C, b) "The "empowerment" rationale for data sharing and its impact on individuals' autonomy and self-determination".
[2083] However, the *Bundesgerichtshof* did not rule on whether the consent collected by Facebook constituted a "valid consent" in the sense of Article 6.1.a) of the GDPR.
[2084] K. Wiedemann, "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *op. cit.*, p. 1173.
[2085] *Ibid*., p. 1174.
[2086] It must be outlined here that, on the 24th of March 2021, the Dusseldorf Higher Regional Court has estimated that it needed a clarification from the European Court of Justice in order to rule on the matter. See S. Stolton, "German legal dispute over Facebook data use sent to European Court of Justice", 24 March 2021, available at

pointing out that Facebook has been sanctioned for a similar behaviour by the *Autorità Garante della Concorrenza e del Mercato* (the Italian Competition Authority)[2087], although on the grounds of consumer law.[2088]

341. In light of the above, and as for the first premise, the second premise, according to which large data holders allegedly re-use personal data within their ecosystem in a data protection law compliant manner, can also be challenged. Therefore, large data holders should, in theory, not be able to apply "double standards" when it comes to personal data protection rules. Said otherwise, they should not be able to apply low personal data protection standards to themselves in order to gain competitive advantages from (potentially unlawful) "internal data free-for-all" practices, while applying stricter data protection requirements to third parties wishing to re-use (some of) their data (which could potentially be seen as an anti-competitive way of raising entry barriers and strengthening their competitive/dominant position on the data markets).[2089].

However, even if these premises are challengeable from a theoretical point of view, large data holders do apply "double standards" in practice. Indeed, they adopt a very restrictive approach towards data sharing with third parties while massively circulating their users' data internally. One of the potential explanations for this is that there is less visibility (and also scrutiny) on internal data circulation than on data sharing with third parties. On the one hand, this allows the large data holders to claim that they are fully compliant with the data protection requirements, while this may not be true, as outlined by the cases mentioned above.[2090] On the other hand, it allows them to require "equivalent compliance" from third parties, who are asked to match the high level of compliance that large data holders claim to have achieved internally. Another potential explanation is that these large data holders fear to lose control on the data shared with third parties, as illustrated in the "Facebook / Cambridge Analytica" scandal mentioned above.[2091] Unfortunately, this "double standard" practice does not seem to be addressed appropriately by the controlling authorities, which have more often opted to intervened harshly against smaller actors instead.[2092] Sub-section c) will attempt to shed light on why this is the case.

c) Failure of controlling authorities to address the "double standards" applied by large data holders

342. As outlined above, although some large data holders, such as Google and Facebook, have been fined by data protection authorities for infringing personal data protection

---

https://www.euractiv.com/section/data-protection/news/german-legal-dispute-over-facebook-data-use-sent-to-european-court-of-justice/.

[2087] Autorità Garante della Concorrenza e del Mercato, *Facebook*, 29 November 2018, decision no. 27432 available at https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

[2088] See M. Botta and K. Wiedemann, "The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey", *Antitrust Bulletin*, vol. 64, issue 3, 2019, p. 428-446.

[2089] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 27-35.

[2090] See points 334 to 338.

[2091] See point 332.

[2092] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 1.

legislations[2093], these interventions have been quite rare and the amount of the fines were quite small in comparison with these large data holders' turnovers. Accordingly, and despite numerous complaints[2094], there is a form of impunity of the conduct of such data holders.[2095] This is arguably the result of a combination of two factors.

343. On the one hand, data protection authorities only have very limited financial resources and man-power, especially when compared to those of large data holders, to address these highly complex issues. Indeed, the combined budget of the EU's 45 data protection authorities is only 326 million euros a year; half of them have a budget lower than 10 million euros a year (the UK *Information Commissioner's Office*'s budget is the highest with 61 million euros a year); they only have a combined total of 305 tech specialists; and half of them only have five or fewer tech specialists.[2096] This might explain why they sometimes refrain from engaging in such complex and resource-consuming investigations, or why these investigations take a lot of time once initiated.

[2093] See https://www.enforcementtracker.com/. See for example: (FR) Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, Deliberation of the Restricted Committee SAN-2019-001, available at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf; Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-012, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706; Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-013, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729; (BE) Autorité de Protection des Données, *X c/ Google*, 14 July 2020, decision no. 37/2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf; (SWE) Datainspektionen, *Google LLC*, 10 March 2020, decision no. DI-2018-9274, available at https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf; (IR) Data Protection Commission, *Twitter International Company*, 9 December 2020, decision no. IN-19-1-1, available at https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf; (IT) Garante per la protezione dei dati personali, *Facebook*, 14 June 2019, decision no. 9121486, available at https://perma.cc/LHV7-2THY; (UK) Information Commissioner's Office, *Facebook Ireland and Facebook Inc*, 24 October 2018, available at https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf; (NED) Autoriteit Persoonsgegevens, *TikTok Inc*., 9 April 2021, (confidential reference), available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf.

[2094] See for instance: Privacy International, "Regulatory complaint against Google and other "ad tech" companies under Europe's GDPR by Johnny Ryan, Jim Killock, and Michael Veale", 12 September 2018, available at https://privacyinternational.org/examples/2983/regulatory-complaint-against-google-and-other-ad-tech-companies-under-europes-gdpr; Privacy International, "Panoptykon Foundation files complaint against Google and other "ad tech" companies with the with the Polish Data Protection Authority", 28 January 2019, available at https://privacyinternational.org/examples/2982/panoptykon-foundation-files-complaint-against-googleand-other-ad-tech-companies; Privacy International, "Ad Tech GDPR complaint is extended to four more European regulators", 20 May 2019, available at https://privacyinternational.org/examples/2992/ad-tech-gdpr-complaint-extended-four-more-european-regulators; J. Ryan, "Formal GDPR complaint against Google's internal data free-for-all", 16 March 2020, available at https://brave.com/google-internal-data-free-for-all/.

[2095] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 19; N. Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *Politico*, 27 December 2019, available at https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

[2096] Brave, "Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities", April 2020, available at https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf, p. 3-6; Access Now, "Three years under the EU GDPR: An implementation progress report", 2021, available at https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf, p. 10-12.

344. On the other hand, the fact that these large data holders are active globally also has a strong impact on enforcement. Indeed, the GDPR designates a lead supervisory authority for the investigation of cross-border processing, namely the data protection authority of the main establishment or of the single establishment of the controller/processor in the European Union.[2097] Accordingly, the other national data protection authorities will, in principle[2098], only be able to investigate cases that relate to an establishment in their Member State, or that substantially affect data subjects only in their Member State.[2099] Yet, there are substantial issues with this mechanism, due to the use of inadequate communication tools between the data protection authorities, to the potential incompatibility of their national procedures, to the lengthiness of the cooperation process and to the difficulties in identifying the lead authority.[2100] Moreover, this leads to a "forum shopping" scenario, as large data holders, who are active globally and carry cross-border processing, have an incentive to locate their main establishment in countries where the national data protection authorities are less active. As outlined by Geradin *et al.*, this one-stop-shop system "creates serious bottlenecks which, coupled with the reluctancy of certain [data protection authorities] to intervene, results in tech

---

[2097] Article 56.1 of the GDPR.

[2098] See, however, Opinion of Advocate General Bobek in *Facebook v. Gegevensbeschermingsautoriteit* (ECJ), C-645/19, delivered on 13 January 2021, EU:C:2021:5; and ECJ, *Facebook v. Gegevensbeschermingsautoriteit*, 15 June 2021, C-645/19, EU:C:2021:483, where the Court ruled that a supervisory authority of a Member State may exercise its powers "in relation to an instance of cross-border data processing even though it is not the 'lead supervisory authority' (…) provided that that power is exercised in one of the situations where Regulation 2016/679 confers on that supervisory authority a competence to adopt a decision finding that such processing is in breach of the rules contained in that regulation and that the cooperation and consistency procedures laid down by that regulation are respected" (§ 75). Moreover, the Court added that "it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, (…) that the controller with respect to the cross-border processing of personal data against whom such proceedings are brought has a main establishment or another establishment on the territory of that Member State" (§ 84); and that the supervisory authority may exercise its powers "both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power, in accordance with [§ 75]" (§ 96).

[2099] Article 56.2 of the GDPR. In this regard, it is interesting to point out that, in both of its decisions adopted on the 7th of December 2020, one against Google LLC and Google Ireland Limited and one against Amazon (on these decisions, see point 336), the CNIL concluded that it was competent to decide on these cases. See Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-012, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706; Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-013, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729.
In both of these decisions, the CNIL ruled that the "one-stop-shop" mechanism contained in the GDPR is not applicable for the control and the sanctioning of the processing at hand (operations to access or write cookies in the terminal of users of google.fr / amazon.fr, residing in France, in particular for advertising purposes), as it falls within the scope of the ePrivacy Directive (2002/58/EC) (Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, § 35; *Amazon Europe Core*, 7 December 2020, § 41). Moreover, it held that it was materially and territorially competent because the processing at hand (operations to access or write cookies in the terminal of users of google.fr / amazon.fr, residing in France, in particular for advertising purposes) is carried out as part of the activities of Google France / Amazon Online France on the French territory (Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, §§ 45-46; *Amazon Europe Core*, 7 December 2020, §§ 51-52).

[2100] Access Now, "Three years under the EU GDPR", *op. cit*, p. 15-19.

giants escaping close monitoring and liability, despite regularly engaging in dubious practices".[2101]

Indeed, in the tech sector, most large data holders, such as Google and Facebook, have located their main establishment, on the territory of the Union, in Ireland and Luxembourg, notably for fiscal reasons.[2102] Accordingly, the Irish *Data Protection Commission* and Luxembourg's *National Data Protection Commission* have a key role to play in the enforcement of the GDPR against these large data holders, and their "ability and willingness to investigate and sanction these companies therefore determines whether these companies will be able to get away with questionable data processing activities or will be held to account".[2103] While the Luxembourg's *National Data Protection Commission* seems to start realising the importance of its regulatory role[2104], the Irish *Data Protection Commission*, which is the lead authority for tech firms such as Google or Facebook, has been reluctant to intervene strongly against these large data holders.[2105] This is notably due to the fact that it has a very limited budget (16.9 million euros per year, the 6th in Europe)[2106] and staff (140 investigators, lawyers and technologists)[2107] to deal with an extreme case load. Indeed, since the entry into force of the GDPR on the 25th of May 2018, the Irish *Data Protection Commission* has received more than 8.800 complaints, 9.600 data breach notifications and 593 cross-border processing complaints through the one-stop-shop system.[2108] Moreover, from a political perspective, the Irish *Data Protection Commission* is in an uncomfortable position as Ireland is strongly dependent on these large data holders, such as Google and Facebook, and this might explain why it has not been more active in investigating these actors.[2109] Unsurprisingly, this is generating a lot of

---

[2101] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 18. See also N. Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *op. cit.*

[2102] See N. Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *op. cit*.

[2103] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 13.

[2104] See point 337.

[2105] It should however be mentioned that the *Data Protection Commission* is expected to impose a fine against WhatsApp by the end of August 2021, for having unsufficiently informed its users about the data it shares with its parent company Facebook, which constitutes a breach of the transparency obligations contained in Articles 12 to 14 of the GDPR (L. Bertuzzi, "Irish watchdog given one month to finalise Whatsapp privacy ruling", 29 July 2021, available at https://www.euractiv.com/section/data-protection/news/irish-watchdog-given-one-month-to-finalise-whatsapp-privacy-ruling/; European Data Protection Board, "EDPB adopts Art. 65 decision regarding WhatsApp Ireland", 28 July 2021, available at https://edpb.europa.eu/news/news/2021/edpb-adopts-art-65-decision-regarding-whatsapp-ireland_en).

[2106] A. Satariano, "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates", *The New York Times*, 27 April 2020, available at https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.

[2107] Brave, "Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities", *op. cit.*, p. 7.

[2108] See (Irish) Data Protection Commission, "Annual Report: 25 May – 31 December 2018", 2019, available at https://www.dataprotection.ie/sites/default/files/uploads/2019-02/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf; (Irish) Data Protection Commission, "Annual Report: 1 January – 31 December 2019", 2020, available at https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf; D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 20.

[2109] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 20.

criticism against the Irish *Data Protection Commission* from other European data protection authorities and from members of the European Parliament.[2110]

345. However, it would be too simplistic to reject all of the fault on the Irish *Data Protection Commission* and on Luxembourg's *National Data Protection Commission*. Rather, they are the flagships of the worrying observation that data protection authorities across Europe do not have sufficient resources to fulfil their duties and do not sufficiently cooperate, leading to a lack of data protection enforcement.[2111] In turn, this leads to a lack of competition enforcement because data protection considerations have often been set aside in competition law assessments[2112], in light of the erroneous premise that large/dominant data holders would be GDPR-compliant as they would be closely monitored by data protection authorities.[2113] As data protection authorities failed to monitor these large data holders, they have been able to consolidate their strong position in the various data markets through questionable practices in terms of data protection law. In turn, this also reduces personal data protection.

346. Finally, it should be added that while a lack of enforcement might arguably be the main cause of the above-mentioned problems, another potential cause is the over-reliance on the fact that data subjects are able to make informed decisions when it comes to the processing of their data[2114], and that they will actually make use of the rights that are granted to them by the GDPR if they stumble upon unlawful processing.[2115]

[2110] See V. Manancourt, "Irish data regulator pulls out of 'perverse' MEP hearing as tensions boil over", 18 March 2021, available at https://pro.politico.eu/news/irish-data-regulator-pulls-out-of-perverse-mep-hearing-as-tensions-boil-over; S. Stolton, "MEPs rue lack of GDPR sanctions issued by Irish data authority", 26 March 2021, available at https://www.euractiv.com/section/data-protection/news/meps-rue-lack-of-gdpr-sanctions-issued-by-irish-data-authority/.

[2111] See N. Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *op. cit.*; Access Now, "Three years under the EU GDPR", *op. cit*.

[2112] See, for instance, W. Kerber, "Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection", *MAGKS Joint Discussion Paper Series in Economics No. 14-2016*, February 2016, available at https://www.econstor.eu/bitstream/10419/144679/1/850599016.pdf; M. Stucke and A. Grunes, *Big Data and Competition Policy*, *op. cit*.; Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data*", op. cit*.; A. Ezrachi and V. Robertson, "Competition, Market Power and Third-Party Tracking", *World Competition: Law and Economics Review*, 2019, Vol. 42, No. 1, p. 5-19; G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *Bocconi Legal Studies Research Paper No. 2945085*, 2 April 2017, available at https://ssrn.com/abstract=2945085, p. 7-9. On the contrary, some argue that data protection and competition law should be kept apart: see G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *op. cit.*, p. 9-11.

[2113] See OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 24-41; G. Colangelo and M. Maggiolino, "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *op. cit.*

[2114] For a strong criticism of the "notice and consent paradigm", see E. Okoyomon, N. Samarin, P. Wijesekera, A. Elazari Bar On, N. Vallina-Rodriguez, I. Reyes, Á. Feal and S. Egelman, "On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies", *The Workshop on Technology and Consumer Protection*, 2019, available at https://blues.cs.berkeley.edu/blog/2019/05/10/on-the-ridiculousness-of-notice-and-consent-contradictions-in-app-privacy-policies-conpro-19/.

[2115] See N. Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *op. cit*. For more information on consumers' attitude towards privacy, notably the fact that they have heterogeneous preferences and behavioural biases, see OECD, *Consumer Data Rights and Competition*, *op. cit*., p. 35-37.

d) Crucial need for more enforcement by controlling authorities

347. It thus stems from the above that while the growing concern that the GDPR limits competition and increases concentration relies on two premises that are challengeable in theory (the GDPR is *not* more lenient towards personal data re-use within the ecosystem of these large data holders than it is towards the sharing of this personal data with third parties; and the way in which these large data holders re-use personal data within their ecosystem *might arguably not* comply with data protection law), large data holders do apply "double standards" in practice. Indeed, they adopt a very restrictive approach towards data sharing with third parties while massively circulating their users' data internally. This is mainly the result of a lack of data protection enforcement, which led, in turn, to a lack of competition enforcement.

Therefore, to solve this "double standards" issue, there is a crucial need for more enforcement of the existing rules by data protection authorities. For instance, there should be an increased scrutiny of the large data holders' "internal data free-for-all" practices[2116], as has been done by the French *Commission Nationale de l'Informatique et des Libertés* in its cases against Google, where it imposed a 50 million euros fine and a 100 million euros fine, and in its case against Amazon, where it imposed a 35 million euros fine.[2117]

348. To ensure more enforcement, the lead authority mechanism might need to be rethought in order to avoid the bureaucratic logjam and the bottlenecks mentioned above, as these might end up having a chilling effect on data subjects seeking to assert their rights against these large data platforms.[2118] In this perspective, the personal data protection legislation could be adapted, in order to enable lead authorities to delegate some cases to other data protection authorities.[2119] At the very least, cooperation between the various data protection authorities, through sharing of legal insights but also of resources, needs to be increased. Indeed, data protection authorities, and especially those dealing with the majority of "tech cases", need more (financial and staff) support to tackle these complex cases. In this regard, it is interesting to point out that the European Parliament has asked the European Commission "to ensure that Member States provide national supervisory authorities with the adequate financial means and human resources and enforcement powers to carry out their functions effectively and to

---

[2116] On this point, see I. Graef and S. Van Berlo, "Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility", *European Journal of Risk Regulation*, November 2020, available at https://doi.org/10.1017/err.2020.92.

[2117] See points 335 and 336. Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, Deliberation of the Restricted Committee SAN-2019-001, available at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf; Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-012, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706; Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-013, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729.

[2118] See N. Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *op. cit*.

[2119] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability: case studies and data access remedies", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/, p. 84.

contribute to their respective work".[2120] In order to do so, some authors have suggested to create a "specialised "tech" unit" at the EU level, potentially within the European Data Protection Board, which could help the data protection authorities to deal with the technical aspects of their investigations, by providing them with supporting technical experts.[2121] Others have suggested that "an EU authority (e.g., the Commission [or the EDPB]) could be put in charge in cases involving a large platform with pan-European systemic importance".[2122] Whatever form this support might take, it is urgent to relieve some of the data protection authorities' burden and to ensure swifter enforcement, for the benefit of all.

Through this increased enforcement, additional scrutiny should be put on the large data holders, notably in light of the "special responsibility" they have in applying the GDPR.[2123] In this regard, some have suggested to increase the data protection standards that these large data holders must meet, notably through a strengthening of the consent requirements[2124] or through a limitation of their ability to combine user data across their various services (data silos).[2125] In this perspective, it is interesting to outline that, in its Facebook case[2126], the *Bundeskartellamt* ordered, for the first time, an "internal unbundling of data held by a dominant platform".[2127] In fact, it seems that the European Commission has piggy-backed on this idea, as it has included, in its proposal for a Digital Markets Act[2128], a provision restricting certain forms of personal data combination by "gatekeepers".[2129] Indeed, these "gatekeepers" shall refrain from combining personal data originating from their core services with personal data from any other services they offer or with personal data from third party

---

[2120] European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 20.

[2121] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 39.

[2122] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 84.

[2123] See point 334. Autorité de Protection des Données, *X c/ Google*, 14 July 2020, decision no. 37/2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf, § 175 (vii). On this point, see also I. Graef and S. Van Berlo, "Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility", *op. cit.*

[2124] There should, for instance, be an increased scrutiny regarding the fact that it should be as easy for data subjects to refuse to consent rather than to provide consent, and that these alternatives should be clearly displayed at the same place and with the same emphasis being put on each option. Yet, nowadays, it often requires more steps for data subjects to signal that they do not consent, or that they only consent to some of the processing, than to consent to all the processing (see point 335).

[2125] D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", *op. cit.*, p. 43-44; J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *op. cit.*, p. 82-84.

[2126] Bundeskartellamt (6th Division), *Facebook*, 6 February 2019, B6-22/16, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf.

[2127] D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 26. See also Bundeskartellamt, "Bundeskartellamt prohibits Facebook from combining user data from different sources", 7 February 2019, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[2128] Proposal for a Digital Markets Act. For more details on this Digital Markets Act, see points 319, 382 and 397 to 398.

[2129] Article 5.a) of the Proposal for a Digital Markets Act.

services, as well as from signing in users to other services they offer in order to combine personal data, unless the users have been presented with this specific choice and have explicitly consented to it.[2130] In the same vein, these "gatekeepers" shall refrain from requiring their users to subscribe or register to any other services they offer as a condition to access, sign up or register to their core service.[2131]

349. Moreover, a stronger data protection enforcement would also be beneficial for competition, as GDPR-compliance could become a competitive factor leading to the appearance of new competitors. Indeed, a stricter data protection enforcement against these large data holders would shed more light on some of their dubious practices, which in turn could reduce their trustworthiness and could pave the way for the emergence of more GDPR-compliant and trustworthy competitors. This in turn would increase data protection standards and the control that data subjects can exercise on "their" data as well, as being GDPR-compliant would become a competitive argument. There is thus an urgent need to move away from the *vicious circle* mentioned above (a lack of data protection enforcement leads to a lack of competition enforcement, which increases data markets' concentration and reduces personal data protection standards and control by data subjects) towards a *virtuous circle* (more data protection enforcement increases data protection standards, which also increases competition, which in turns increases data protection standards and control by data subjects, etc.). Data protection, which might presently be somewhat of a foe to competition in light of the "double standards" situation, could become a friend if enforced with more pugnacity against large data holders, as it would not only reinforce the protection of data subjects but would also ensure the existence of a healthier competitive environment. As summarised by Kerber, "the basic idea is that a better privacy / data protection law that gives the consumers more control of their data might also lead to less market power of the large digital platforms".[2132]

350. Finally, to truly address the "double standards" situation, the other side of the coin must also be tackled, namely that large data holders should not be able to raise data protection requirements as a pretext to justify controversial strategies in order to raise entry barriers on the data markets vis-à-vis third parties and to strengthen their competitive position by refusing to share (some of) their data.[2133] In this regard, it is no longer the data protection authorities but the competition authorities that must increase their scrutiny against such allegations, in order to determine whether such data protection defence is truly genuine or whether it is a "smokescreen for anti-competitive conduct".[2134] To do so, the competition authorities should require these large data holders to lay down and substantiate the data protection concerns they raise in order to refuse data sharing with third parties, and they should cooperate with data protection authorities in order to assess whether the data protection standards imposed on

---

[2130] Article 5.a) of the Proposal for a Digital Markets Act.
[2131] Article 5.f) of the Proposal for a Digital Markets Act.
[2132] W. Kerber, "Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia", September 2019, available at https://ssrn.com/abstract=3469624, p. 40.
[2133] See D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 27-35.
[2134] *Ibid*., p. 36-37.

third parties by these large firms are (suspiciously) higher than the ones they apply to themselves.[2135]

In fact, an analogy can be made with the European Court of Justice's reasoning in the *Hilti*[2136] and the *Tetra Pak*[2137] cases, in which dominant undertakings invoked consumer safety and health considerations as an objective justification for their tying practices. In *Hilti*, the Court of First Instance held that "there are laws attaching penalties to the sale of dangerous products and to the use of misleading claims as to the characteristics of any product. There are also authorities vested with powers to enforce those laws. In those circumstances it is clearly not the task of an undertaking in a dominant position to take steps on its own initiative to eliminate products which, rightly or wrongly, it regards as dangerous or at least as inferior in quality to its own products".[2138] This decision was confirmed by the European Court of Justice.[2139] This finding was repeated by the Court of First Instance in *Tetra Pak*[2140], whose decision was, once again, confirmed by the European Court of Justice.[2141] Accordingly, if these decisions were to be applied, by analogy, to refusals by large data holders to share data with third parties on the basis of personal data protection considerations, it could be argued that it is not for these large data holders to decide on the level of data protection and security that should be offered by third parties, as the protection of personal data is guaranteed by a separate set of legislations, and as specific authorities are in charge of enforcing them.[2142]

Naturally, the strength of this argument will be function of the effective level of enforcement of personal data protection rules by the data protection authorities. Indeed, this argument will have little weight if data protection authorities fail to adequately enforce personal data protection rules in practice, which they are blamed for at the moment. Therefore, in order to address the two aspects of the "double standards" issue, it will be crucial for personal data protection authorities to strengthen their enforcement practice against large data holders. On the one hand, this should lead to a limitation/reduction of these large data holders' "internal data free-for-all" practices. On the other hand, this should limit the cases in which large data holders should be able justify the refusal to share data with third parties on the basis of personal data protection considerations.

[2135] *Ibidem*.
[2136] CFI, *Hilti AG v. Commission of the European Communities*, 12 December 1991, T-30/89, EU:T:1991:70; ECJ, *Hilti AG v. Commission of the European Communities*, 2 March 1994, C-53/92 P, EU:C:1994:77.
[2137] CFI, *Tetra Pak International SA v Commission of the European Communities*, 6 October 1994, T-83/91, EU:T:1994:246; ECJ, *Tetra Pak International SA v Commission of the European Communities*, 14 November 1996, C-333/94 P, EU:C:1996:436.
[2138] CFI, *Hilti AG v. Commission of the European Communities*, 12 December 1991, T-30/89, EU:T:1991:70, § 118.
[2139] ECJ, *Hilti AG v. Commission of the European Communities*, 2 March 1994, C-53/92 P, EU:C:1994:77, §§ 11-16; I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *Yearbook of European Law*, 2019, p. 40.
[2140] CFI, *Tetra Pak International SA v Commission of the European Communities*, 6 October 1994, T-83/91, EU:T:1994:246, § 138.
[2141] ECJ, *Tetra Pak International SA v Commission of the European Communities*, 14 November 1996, C-333/94 P, EU:C:1996:436; I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 41.
[2142] See I. Graef, "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *op. cit.*, p. 40-41.

Section B. Data sharing as a competition law remedy: articulation with the GDPR[2143]

351. In light of the previous Section, it appears that while large data holders might attempt to objectively justify refusals to share data on the basis of personal data protection considerations, they might be overstepping their role in doing so and, in fact, this might conceal anti-competitive tactics.[2144] As a consequence, some undertakings may not be able to access certain data at all.[2145] Yet, under EU competition law, if an undertaking holding a dominant position refuses to share (some of) its data with another undertaking, this could potentially lead to the application of the essential facilities doctrine case law[2146] and to an abuse precluded by Article 102 TFEU.[2147] Moreover, such a refusal to share data might also, in certain circumstances, amount to an abuse of economic dependence[2148] or to input foreclosure in vertical mergers.[2149]

As outlined above[2150], for each of these infringements, a potential pro-competitive remedy could be to impose on the large data holder an obligation to share (some of) its data with several third parties. This is because the digital economy is characterised by extreme returns to scale, network externalities and the prominent role of data as a key competitive parameter.[2151] These characteristics lead to strong economies of scope who benefit large data holders who have access to more (recent) data than their competitors, which makes it complicated to dislodge them.[2152]

352. Yet, as the data sharing remedy will likely cover personal data pertaining to multiple individuals, some tensions might emerge between competition law and personal data

---

[2143] This Section is partly based on T. Tombal, "The GDPR: A Shield to a Competition Authority's Data Sharing Remedy?", *Deep Diving into Data Protection*, J. Herveg (coord.), Bruxelles, Larcier, 2021, p. 67-94.
[2144] See point 350. D. Geradin, T. Karanikioti and D. Katsifis, "GDPR Myopia", *op. cit.*, p. 36-37.
[2145] M. Barbero, D. Cocoru, H. Graux, A. Hillebrand, F. Linz, D. Osimo, A. Siede and P. Wauters, "Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*"*, 25 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and, p. 92-93.
[2146] ECJ, *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18; ECJ, *AB Volvo v Erik Veng (UK) Ltd*, 5 October 1988, C-238/87, EU:C:1988:477; ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98; ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569; ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257; CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289.
[2147] See Part III, Chapter 1, Section A. See J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*"*, *Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975, p. 44. On the applicability of the essential facilities doctrine to data, see also: I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, Alphen aan den Rijn, Kluwer, 2016; I. Graef, S. Wahyuningtyas and P. Valcke, "Assessing data access issues in online platforms", *Telecommunications Policy*, 2015, Vol. 39, p. 375-387; G. Colangelo and M. Maggiolino, "Big data as misleading facilities", *European Competition Journal*, 2017, Issue 13, Vol. 2-3, p. 249-281.
[2148] See Part III, Chapter 1, Section B. See also W. Kerber, "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *JIPITEC*, 2018, Issue 9, p. 329; T. Tombal, "Economic dependence and data access", *IIC*, 2020, Volume 51, Issue 1, p. 70-98.
[2149] See Part III, Chapter 1, Section C.
[2150] See Part III, Chapter 1, Section D.
[2151] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit.*, p. 19-24.
[2152] *Ibid*., p. 3 and 24.

protection law.[2153] Indeed, while competition law might require the sharing of personal data in order to stimulate innovation and to ensure a level playing field between large data holders and undertakings who need access to these data, the GDPR subjects the processing of personal data to the principles of purpose limitation and data minimisation.[2154] According to the purpose limitation principle, data that has been collected for a specific purpose cannot be shared with third parties if this act of sharing does not fit within this initial purpose. According to the data minimisation principle, the categories and amount of data that can be shared should be limited to what is necessary to meet this purpose. This outlines the importance of clearly defining the specific purpose of the data sharing remedy, as the GDPR prevents "over-sharing", i.e. sharing more data than what is relevant and necessary for the purpose of the processing.

However, competition law and personal data protection law considerations are not necessarily incompatible, and sharing personal data can be beneficial for society, governments, undertakings and individuals.[2155] The challenge is thus not whether one should prevail over the other, but rather to determine how they can be reconciled.[2156] To shed some light on how competition law and personal data protection law can be reconciled on this matter, this Section will analyse how a competition authority's decision imposing to share personal data with a third party can be compatible with the GDPR.

353. As a preliminary consideration, it should be outlined that one way to circumvent the application of the GDPR would be to anonymise the personal data before sharing it. While this might be possible in some cases (e.g. search data), there are other cases where this might reduce the value of the dataset and, in any case, truly effective anonymisation[2157] is difficult to achieve.[2158] This is especially true in light of the constant development of *Big Data*[2159]

[2153] J. Haucap, "A German approach to antitrust for digital platforms", in *Digital Platforms and Concentration - Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (ed.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 12. On the articulation between competition law, personal data protection law and consumer law: see I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper DP 2019-005*, November 2019, available at https://ssrn.com/abstract=2956308.

[2154] Article 5.1.b) and c) of the GDPR.

[2155] For a "Code of practice" on *voluntary* data sharing, which aims at serving as a guide for businesses wishing to share personal data in a privacy-compliant way, see Information Commissioner's Office, "Data sharing code of practice", 17 December 2020, available at https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/.

[2156] K. Muralidhar, R. Sarathy and H. Li, "'To Share or Not to Share. That is Not the Question' - A Privacy Preserving Procedure for Sharing Linked Data", 3 July 2014, https://ssrn.com/abstract=2462152, p. 2.

[2157] The ISO 29100 standard defines anonymisation as the: "process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party*"* (ISO 29100:2011, point 2.2, available at https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en).

[2158] J. Drexl, "Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy", *Max Planck Institute for Innovation & Competition Research Paper No. 18-23*, 31 October 2018, available at https://ssrn.com/abstract=3274519, p. 4. See also I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy" *op. cit.*, p. 6; and C. Wendehorst, "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 330-331.

analytics, which increase the risk of re-identification of the data subjects. This failure to effectively anonymise personal data has been demonstrated several times in the literature[2160], leading to the conclusion that what is often presented as anonymisation techniques are, in fact, merely pseudonymisation[2161] techniques. Yet, pseudonymised data remain personal data covered by the GDPR, given that the data subject can still be re-identified.

In the vast majority of cases, the data will thus remain personal and the data sharing remedy will therefore have to comply with the rules of the GDPR. This requires, on the one hand, to have a lawful basis for the data sharing[2162], and, on the other hand, to comply with the general principles of personal data protection.[2163] Moreover, competition and data protection authorities will need to cooperate in order to define and implement this remedy.

a) Lawful basis for the data sharing

354. A remedy imposing data sharing would require a lawful basis at two levels, namely at the level of the undertaking that transfers the data and at the level of the undertaking that will receive the data, although these two lawful bases do not need to be the same.[2164] Therefore, this thesis will first address the potential lawful bases for the data holder before turning to the potential lawful bases for the data recipient.

1. Lawful basis for the data holder

355. Transferring data to a third party as a consequence of a data sharing remedy imposed by a competition authority amounts to a new processing[2165] for the data holder and is therefore in need of a lawful basis.[2166] This raises a first preliminary question, namely whether a new separate lawful basis is necessary in order for the data sharing to be GDPR-compliant. Indeed, according to Article 6.4 and Recital 50 of the GDPR, a separate lawful basis is not necessary if the new purpose (*in casu* the data sharing as a remedy) is "compatible" with the initial

---

[2159] ""Big data" is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software" (https://en.wikipedia.org/wiki/Big_data).

[2160] L. Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality", *Journal of Law, Medicine & Ethics*, 1997, Vol. 25, Issues 2 & 3, p. 98-110; L. Rocher, J. Hendrickx and Y.-A. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, 2019, Vol. 10, n°3069, available at https://www.nature.com/articles/s41467-019-10933-3.

[2161] "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Article 4.5 of the GDPR).

[2162] Article 6 of the GDPR.

[2163] Article 5 of the GDPR.

[2164] C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit.*, p. 334-337.

[2165] Processing means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4.2 of the GDPR).

[2166] C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit.*, p. 334-335.

purpose for which the data has been collected.[2167] The question is thus whether imposing data sharing as a remedy could be considered as being compatible with the purpose of the initial data processing. To assess this compatibility, the following elements should be considered:[2168]

- Any link between the initial purpose and the purpose of the intended further processing;
- The context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- The nature of the personal data;
- The consequences of the intended further processing for data subjects; and
- The existence of appropriate safeguards in both the original and intended further processing operations.

A key consideration here will be whether the data subjects could reasonably expect that the data holder might have to share the personal data it holds with another undertaking as a result of a competition law remedy. Can it be said that if a data subject provides its data to Facebook or Google, she can reasonably expect that these firms might abuse their dominant position and that, as a consequence, they will have to share the personal data they hold with competitors? In conducting this assessment, the types of services that the competitors intend to offer and the potential safeguards that they would set in place, such as pseudonymisation mechanisms, should be considered. Moreover, this assessment of the compatibility of the purposes from a data protection perspective is interesting to compare with the assessment of the re-use purpose from a competition law perspective, as they might actually lead to contradictory findings. Indeed, from a data protection perspective, if the recipient intends to use the data for another type of service, this will likely not be considered as a compatible purpose. In contrast, from a competition law perspective, it will be easier to force a data holder to share its data with a recipient wishing to offer "new" types of services.[2169]

356. Ruling that the transfer is compatible with the initial purpose of processing would spare the necessity of identifying a separate lawful basis for the data holder and would thus facilitate the implementation of the data sharing remedy. If, on the other hand, the further processing deriving from the remedy imposing data sharing is deemed to be "incompatible" with the initial purpose for which the data has been collected (and this will likely always be the case), this further processing can only be carried out if the data subjects have consented to it or if it is mandated by a legal obligation.[2170] Indeed, only two of the six lawful bases listed

---

[2167] This is however contested by some authors, who argue that the final text of the GDPR fails to reflect the agreement that was reached during the negotiations (see C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit.*, p. 335-336 and references cited in footnote 25 of that paper).
[2168] Article 6.4 and Recital 50 of the GDPR.
[2169] See, in this regard, the essential facilities doctrine, according to which a refusal to provide the access to an essential facility will be considered as being an abuse of dominant position if the following exceptional circumstances are met: (i) The access to the facility is indispensable to compete on the downstream market; (ii) the refusal to grant access excludes all effective competition on the downstream market and (iii) prevents the introduction of a *new product/technological innovation*; and (iv) there is no objective justification for the refusal (emphasis added). See Part III, Chapter 1, Section A.
[2170] Article 6.4 of the GDPR.

in Article 6.1 of the GDPR can be relied upon to legitimise an incompatible further processing. This is the result of a compromise reached between the European Commission, the Working Party 29 (today the European Data Protection Board) and the European Parliament during the negotiations of the final text of the GDPR.[2171] While the Commission only wanted to exclude the possibility to rely on the "legitimate interests" legal basis[2172] for incompatible further processing[2173], the Working Party 29 and the European Parliament wanted to exclude the possibility to rely on any lawful basis at all because, by essence, such an incompatible further processing would be unlawful and therefore prohibited.[2174] Indeed, according to the Working Party 29, "legalising an otherwise incompatible data processing activity simply by changing the terms of a contract with the data subject, or by identifying an additional legitimate interest of the controller, would go against the spirit of the purpose limitation principle and remove its substance".[2175] Yet, such a drastic position would have been highly problematic in the perspective of *Big Data* and *Open Data*. Accordingly, a compromise was reached[2176], having in mind that the key concern of the GDPR is to provide control to the data subjects on what happens with "their" data. In order to avoid opacity towards incompatible further processing and to ensure transparency, it was thus decided that these incompatible processing could only be carried out if the data subjects had consented to them or if they were mandated by a legal obligation.[2177]

[2171] See C. de Terwangne, "Article 5. Principles relating to processing of personal data", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 316; W. Kotschy, "Article 6. Lawfulness of processing", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 343; F. Gaullier, "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *Communication commerce électronique*, 2018/4, p. 51; C. de Terwangne, "Les principes relatifs au traitement des données à caractère personnel et à sa licéité", *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 98-104.

[2172] Article 6.1.f) of the GDPR.

[2173] See Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM/2012/011 final, Article 6.4: "Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1".

[2174] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 12 March 2014, *OJ C 378/399*, 9 November 2017, p. 428 (where Article 6.4 of the Commission's proposal is deleted); Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 36-37; F. Gaullier, "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *op. cit.*, p. 51.

[2175] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, *op. cit.*, p. 36.

[2176] Article 6.4 of the Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ C 159/1*, 3 May 2016.

[2177] F. Gaullier, "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *op. cit.*, p. 51.

In light of the above, two lawful bases could potentially be used for the transfer of the personal data covered by the competition law remedy, namely consent and the necessary processing for the compliance with a legal obligation to which the data holder is subject.[2178]

i. Consent

357. The first possibility for the data holder would be to obtain the explicit freely given, specific, informed and unambiguous consent of the data subjects at hand *after* the competition authority's decision.[2179] Indeed, obtaining a general consent *before* the decision will lack the specificity and explicitness required for the consent to be compliant with the GDPR.[2180] The data holder will therefore have to seek the consent to share the data with one or several specific recipients identified in the competition authority's decision.[2181] In this context, the data holder should request some basic information from the various data recipients (such as the purpose for which they will process the data or the types of data they will process[2182]) in order to provide the data subjects with sufficient information allowing them to make a specific and informed choice about whether to consent to the transfer or not. However, it might be extremely complex and burdensome to do so in practice.

The French *GDF Suez*[2183] case has been mentioned by several authors to illustrate this point.[2184] In that case, the French *Autorité de la concurrence* (French Competition Authority) found that GDF Suez had abused its dominant position in the market for natural gas and required GDF Suez to share certain customer information data with its competitors.[2185] More precisely, the *Autorité*, after having consulted the *Commission Nationale de l'Informatique et des Libertés* (the French data protection authority), ordered GDF Suez to inform the data subjects about the sharing of their data with their competitors and to give them the possibility to object to this transfer.[2186] Some authors have argued that this remedy relied on an "opt-out

[2178] Articles 6.1.a) and c) of the GDPR.
[2179] Articles 4.11 and 6.1.a) of the GDPR.
[2180] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *Max Planck Institute for Innovation and Competition Research Paper No. 19-04*, 2019, available at https://ssrn.com/abstract=3337524, p. 27-28.
[2181] *Ibid*., p. 28.
[2182] The data recipient could, for instance, produce a short form that would be filled by the recipients and that would be presented to the data subjects when asking for their consent.
[2183] Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, available at https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf.
[2184] See I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit*., p. 271-272; V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 28.
[2185] Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, p. 52, Article 1.
[2186] *Ibid*., p. 52-53, Articles 5 and 6. The following information had to be sent to the clients: "The Competition Authority ordered GDF Suez, by decision No. 14-MC-02 of 9 September 2014, to give access to its competitors to certain data contained in the files of the clients having a supply contract at the regulated gas sales tariff, in order to re-establish the conditions for effective competition (...). If you do not want your data to be transmitted for commercial prospecting purposes to suppliers who have requested access to the GDF SUEZ customer database, please return this form by ticking the box below. If you do not object within the next 30 days, your data will automatically be made available to these suppliers" (author's translation).

consent", as, at the time, the Data Protection Directive[2187] was still in force and this legislation was silent about whether such an opt-out solution was admissible.[2188] Yet, such an interpretation is erroneous, as the *Autorité* did not subject the sharing to an "opt-out consent", but rather held that GDF Suez had to inform the data subjects about the sharing with competitors, in order for them to be able to exercise their right to object to the processing[2189] (i.e. the sharing).[2190] Therefore, it seems that, in this case, the lawful basis for the sharing was not consent, but rather that the transfer was necessary for the compliance with a legal obligation to which GDF Suez was subject, namely the *Autorité*'s decision.[2191]

What can be inferred from the above is that, while reliance on consent as a lawful basis is possible in theory, this will arguably be unrealistic in practice. This is especially the case now that the GDPR is in force, as requiring the data subjects to opt-out of the transfer, rather than to opt-in to the transfer, would not be GDPR-compliant, as, according to Article 4.11 of the GDPR, the data subject has to explicitly consent to the transfer.[2192] The necessity of an explicit consent has been confirmed by the European Court of Justice[2193] and this makes it much more cumbersome for the data holder and will surely affect the efficiency in practice of the data sharing remedy if the data holder relies on consent as a lawful basis for the transfer, as it is very likely that there will be fewer data subjects who opt-in than data subjects who do not opt-out.[2194] The intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent.[2195] Additionally, relying on consent might also weaken this remedy as, according to Article 7.3 of the GDPR, the data subjects are free to withdraw their consent at any time.

ii. Necessary for the compliance with a legal obligation to which the data holder is subject

358. The second possibility for the data holder would be to demonstrate that the transfer is necessary for the compliance with a legal obligation to which it is subject.[2196] The issue is whether a decision by a competition authority could qualify as such a legal obligation. Here,

---

[2187] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281*, 23 November 1995.

[2188] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 28. It should however be underlined that according to some authors, consent under the Directive still required an (explicit) action from the data subject and couldn't be inferred from a lack of action (see E. Kosta, "Construing the Meaning of 'Opt-Out': An Analysis of the European, U.K. and German Data Protection Legislation", *European Data Protection Law Review*, 2015, Vol. 1, p. 16-31).

[2189] Article 21 of the GDPR.

[2190] Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, p. 52-53, Articles 5 and 6.

[2191] On this lawful basis, see point 358.

[2192] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 28.

[2193] ECJ, *Planet 49*, 1 October 2019, C-673/17, EU:C:2019:801.

[2194] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 28-29. See also J. Campbell, A. Goldfarb and C. Tucker, "Privacy Regulation and Market Structure", *Journal of Economics & Management Strategy*, vol. 24, issue 1, 2015, p. 47-73.

[2195] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 28.

[2196] Article 6.1.c) of the GDPR.

different views are expressed. While Graef indicates that a data sharing remedy imposed by a competition authority would amount to such a legal obligation[2197], Kathuria and Globocnik argue, on the contrary, that a competition authority's decision will not qualify as a legal obligation for the data sharing, because this term presupposes the existence of an underlying generally applicable law.[2198]

Article 5.3 GDPR indeed provides that the basis for the processing shall be laid down in Union law or Member State law. However, the word "law" is not defined anywhere in the GDPR. In that regard, the interpretation, by the European Court of Human Rights, of the requirement of the legality of an interference with a fundamental right[2199] should be reminded. The Court consistently holds that the term "law" must not be given a "formal interpretation", which would necessarily imply the existence of a written statute having a legislative value, but rather a "material interpretation"[2200], which not only covers the written statutes, but all the legal rules in force.[2201] Indeed, the European Court of Human Rights has, at the outset, recognised that in countries having a *Common Law* legal tradition, unwritten rules of law could be considered as satisfying the requirement of legality of interference in a fundamental right.[2202] Importantly, the Court then also subsequently recognised a wider margin of manoeuvre for countries having a *Continental Law* legal tradition as to what should be incorporated under the term "law".[2203] In particular, the Court acknowledged that decisions, regulations or unwritten rules of law, such as case law decisions, could satisfy the requirement of legality.[2204] Arguably, a similar interpretation could be given to the words "law" and "legal obligation" in the GDPR. In fact, it seems that this is the approach that has been taken by the French *Autorité de la concurrence*, although not explicitly, in the French *GDF Suez* case mentioned above.[2205] This interpretation is supported by the fact that Recital 41 of the GDPR provides that "where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned".

[2197] I. Graef, *EU competition law, data protection and online platforms: data as essential facility*, *op. cit.*, p. 319.
[2198] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 21-22.
[2199] *In casu* article 8 of the European Convention on Human Rights (Right to respect for private and family life), in which personal data protection is rooted.
[2200] E. Degrave, *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier - Collection du CRIDS, 2014, p. 144.
[2201] R. Ergec, *Protection européenne et internationale des droits de l'homme*, Bruxelles, Larcier, 2014, p. 232.
[2202] ECtHR, *Sunday Times v. United Kingdom*, 26 April 1979, App. No. 6538/74, §§ 46-53.
[2203] ECtHR, *Hüvig v. France*, 24 April 1990, App. No. 11105/84, § 28; and ECtHR, *Kruslin v. France*, 24 April 1990, App. No. 11801/85, § 29. See P. De Hert, "Artikel 8. Recht op privacy", *Handboek EVRM, Deel 2. Artikelsgewijze commentaar*, J. Vande Lanotte and Y. Haeck (ed.), Antwerp, Intersentia, 2004, p. 716.
[2204] P. De Hert, "Artikel 8. Recht op privacy", *op. cit.*, p. 716.
[2205] Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, available at https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf. See point 357. The same reasoning could also be made in the case of a bankruptcy, where a court's decision to grant undertaking B the right to take over undertaking A's business, including the data pertaining to its clients, could be assimilated to a legal obligation and thus serve as the lawful basis for the transfer of the data (see G. Detroux et F. George, "La protection des données à caractère personnel dans le cadre d'une faillite", *J.T.*, 2019, n°6783, p. 582-583).

However, Recital 41 of the GDPR also provides, in accordance with the case-law of the European Court of Human Rights and the European Court of Justice, that this "law" must be formulated in clear and precise terms, and be sufficiently predictable and accessible.[2206] The requirement of predictability implies that anyone must be able to foresee, with a reasonable degree of certainty, the potential effects of this "law".[2207] This is where difficulties might emerge from a *Continental Law* perspective, as this would require for the case law on data sharing as a competition law remedy to be well-established, so that it has become clear and predictable. Yet, in practice, such case law is scarce and it might therefore be argued that the "law" is not sufficiently predictable at this point. Nevertheless, with time, such case law could develop more clearly and systematically, rendering it "predictable" and, as a consequence, a competition authority's decision imposing to provide access to data could qualify as a "legal obligation". As this is a key issue for the future, a clarification by the European Data Protection Board and/or the European Data Protection Supervisor on the matter would be highly welcomed.

In any case, in order to be GDPR-compliant, the data sharing remedy imposed by the competition authority will have to be specific enough. Indeed, Article 5.3 of the GDPR provides that the legal obligation should[2208] specify the purpose for which the data is shared (e.g. to remedy a specific competition issue), the undertakings with whom the data is shared, and the types of data and the data subjects concerned by the data sharing remedy. Moreover, Article 5.3 of the GDPR adds that this legal obligation should meet an objective of public interest (*in casu* ensuring a competitive environment that will benefit the consumers) and be proportionate to the legitimate aim pursued. In this regard, the competition authority must ensure that its decision does not disproportionally affect the data subjects' interests and rights.[2209]

2. Lawful basis for the data recipient

359. While the data holder has to have a lawful basis to transfer the data towards the recipient, this recipient also needs its own specific lawful basis for the processing of the data that will be done once it has received the data covered by the data sharing remedy.[2210] As for the data holder, this raises a first preliminary question, namely whether a new separate lawful basis is necessary in order for the data sharing to be GDPR-compliant. In this regard, the data recipient could attempt to demonstrate that it will re-use the data for scientific research[2211] or

---

[2206] See also R. Ergec, *Protection européenne et internationale des droits de l'homme*, *op. cit*., p. 232.
[2207] *Ibidem*.
[2208] Article 5.3 of the GDPR uses the word "may" but, in light of the decision of the European Court of Human Rights in the *Rotaru* (ECtHR, *Rotaru v. Romania*, 4 May 2000, App. No. 28341/95) and *Shimolovos* (ECtHR, *Shimovolos v. Russia*, 21 June 2011, App. No. 30194/09) cases, this thesis argues that the appropriate word should be "should".
[2209] On this issue, see point 362.
[2210] C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit*., p. 334-337.
[2211] According to Recital 159 of the GDPR, scientific research purposes "should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research (…) [and] should also include studies conducted in the public interest in the area of public health".

statistical[2212] purposes, as, in those cases, the further processing is considered as compatible with the initial purpose of processing and no separate lawful basis is necessary.[2213] In such cases, appropriate technical and organisational safeguards, such as pseudonymisation, would, however, have to be set.[2214] As pointed out by Mayer-Schönberger and Padova, this could notably be possible for some *Big Data* applications.[2215]

360. If the data recipient is not able to rely on the above-mentioned exemption for scientific research or statistical purposes, it will have to rely on a new lawful basis of processing. However, contrary to the data holder[2216], it will have the ability to rely on any of the six lawful bases contained in Article 6.1 of the GDPR.[2217] This is because the potential incompatibility of purposes will have arguably been "purged" either by the consent or the legal obligation that has been used as a lawful basis for the transfer of the data from the holder to the recipient. In practice, the data recipient will rely either on consent or on "legitimate interests" for the further processing. Indeed, contrary to the data holder, the recipient should not be able to argue that this further processing is necessary for the compliance with a legal obligation to which it is subject. This is because, while the competition authority's decision to impose a data sharing remedy could be considered as a legal obligation for the data holder that must comply with this decision[2218], this decision does not impose any obligation on the data recipient to process the shared data. Therefore, the recipient cannot argue that it must necessarily process the data as a result from the competition authority's decision.

i. Consent

361. The first lawful basis for the data recipient could thus be the obtaining of the explicit freely given, specific, informed and unambiguous consent of the data subjects at hand *after* the competition authority's decision.[2219] In this regard, the data recipient will have to be very specific about the purpose for which it will use this data, as the data subject's consent should be asked for a well-defined purpose and should not remain general.[2220] While data subjects might not see the added-value of consenting to the processing of their personal data by a data recipient that would offer them a service that is similar to (or a copy of) the data holder's service (unless it is offered at better conditions, notably in terms of data protection), they might have more incentives to consent to the processing of their personal data by a data

---

[2212] Statistical purposes mean "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that (…) the personal data are not used in support of measures or decisions regarding any particular natural person" (Recital 162 of the GDPR).
[2213] Article 5.1.b) and Recital 50 of the GDPR.
[2214] Article 89.1 of the GDPR.
[2215] V. Mayer-Schönberger and Y. Padova, "Regime change? Enabling Big Data through Europe's new Data Protection Regulation", *Columbia Science & Technology Law Review*, Vol. XVII, 2016.
[2216] See *supra* point 356.
[2217] Namely: (i) consent, (ii) processing necessary for the performance of a contract; (iii) processing necessary for compliance with a legal obligation; (iv) processing necessary in order to protect the vital interests; (v) processing necessary for the performance of a task carried out in the public interest; and (vi) processing necessary for legitimate interests.
[2218] See *supra* point 358.
[2219] Articles 4.11 and 6.1.a) of the GDPR.
[2220] Article 6.1.a) and 8.2 of the GDPR.

recipient that would offer them a "new" type of service or an alternative service that interoperates with the data holder's service.[2221] In this perspective, the objectives of data protection are aligned with the objectives of competition law, as competition authorities will be more reluctant to force a data holder to share its data with a recipient wishing to offer similar services than to force a data holder to share its data with a recipient wishing to offer "new" types of services.[2222]

However, and as for the data holder, it might be too troublesome to do so in practice and the intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent.[2223]

ii. Necessary for the purposes of the legitimate interests pursued by the data recipient

362. The other possibility for the data recipient would be to argue that the data processing is necessary for the purposes of the legitimate interests that it pursues, and that these interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.[2224] This requires to identify legitimate interests for the data recipient, to demonstrate that the data processing resulting from the data sharing remedy is necessary to fulfil these legitimate interests, and to strike a balance between the interests of the data recipient, on the one hand, and the interests of the data subjects, on the other hand.

For the data recipient, the legitimate interests of the access would be the opportunity to offer (privacy-oriented) alternative products or services to the consumers, to restore competition on the market where the data holder has committed an abuse, and to reduce the latter's competitive advantage.[2225] Moreover, processing the data covered by the remedy would arguably be necessary for the data recipient in order to fulfil these legitimate interests, as, in principle, the competition authority will have ordered the data sharing precisely because there was no other remedy to achieve these interests in light of the competition law infringement committed by the data holder (i.e. the data sharing remedy is imposed because it is the only way to reduce the data holder's competitive advantage and to restore competition, and the recipient has to use this data if it wants to be able to offer alternative products or services).[2226]

[2221] On the necessity to go further than data portability and the necessity to ensure interoperability between services, see J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 58-60.

[2222] See, in this regard, the essential facilities doctrine, according to which a refusal to provide the access to an essential facility will be considered as being an abuse of dominant position if the following exceptional circumstances are met: (i) The access to the facility is indispensable to compete on the downstream market; (ii) the refusal to grant access excludes all effective competition on the downstream market and (iii) prevents the introduction of a *new product/technological innovation*; and (iv) there is no objective justification for the refusal (emphasis added). See Part III, Chapter 1, Section A.

[2223] See point 357. V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 28.

[2224] Article 6.1.f) of the GDPR.

[2225] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 25.

[2226] See Part III, Chapter 1, Section D, a) to c).

The key question is therefore whether the data recipient's legitimate interests outweigh the data subjects' interests. At first glance, the data sharing deriving from the competition authority's decision might look like it will always risk to affect the data subjects' rights, as more undertakings will get access to their personal data, thus potentially reducing the data subjects' privacy. Moreover, it might also arguably increase the risks of de-anonymisation of other data.[2227] Accordingly, there might be some cases where the data subjects will be worse off because of this data sharing. In such cases, the legitimate interests of the data recipient should not prevail over the data subjects' interests, and Article 6.1.f) of the GDPR should not be considered as a viable lawful basis.

However, there are other cases where this data sharing might allow competitors to create (privacy-oriented) alternatives to existing services, which would benefit the data subjects in the long term. Indeed, the development of competitive alternatives is necessary to prevent data subjects from being "locked in" the services of the existing providers, as more switching possibilities would allow the data subjects to resort to services offering more guarantees in terms of personal data protection. To support this argument, the "About Data About Us" report should be mentioned.[2228] It is the result of a collaboration in the United Kingdom between the Open Data Institute, Luminate, and the Royal Society for the encouragement of Arts, Manufactures and Commerce. These institutions explored, via focus groups and a workshop, how UK citizens feel about "their" data and about the (lack of) control and protection they experience.[2229] The report outlines that people have much more awareness and understanding about these issues than what they are traditionally given credit for by politicians and in the press (where they are traditionally painted as naïve or ignorant), and that people do have clear expectations on how "their" data should be protected.[2230] They desire more transparency, more control, more fairness and more compliance with personal data protection principles from the undertakings that process their data.[2231] Therefore, if the data recipients were to offer (more privacy-oriented) alternatives to the data holder's services, the legitimate interests of the data recipients could prevail over the data subjects' interests – and might actually be aligned with these interests –, and accordingly the data could be shared on the basis of Article 6.1.f) of the GDPR.

In order to achieve the above-mentioned balancing exercise between the interests of the data recipient and those of the data subjects, the data recipient will need to be very specific about the use it will make of the shared data (e.g. which products or services it intends to offer thanks to the data, whether they are privacy-oriented or not, etc.), as this will allow to determine if this further processing would be harmful, or on the contrary beneficial, to the data subjects. Naturally, the data subjects will remain free to oppose to this processing, on the

---

[2227] V. Kathuria and J. Globocnik, "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *op. cit.*, p. 26 and 32.
[2228] R. Samson, K. Gibbon and A. Scott, "About data about us," September 2019, available at https://www.thersa.org/globalassets/pdfs/reports/data-about-us-final-report.pdf.
[2229] *Ibid*., p. 3.
[2230] *Ibid*., p. 39.
[2231] *Ibid*., p. 36-38.

basis of Article 21.1 of the GDPR, if they disagree with the outcome of the balance of interests.

b) Compliance with the general principles of personal data protection

363. In order for data sharing as a remedy to be compatible with the data protection rules, the data holder and the data recipient must not only rely on a lawful basis for the processing (respectively for the transfer and for the further processing of the data). They must also comply with the general principles of personal data protection.

364. First, both the data holder and the data recipient will have to inform the data subjects about the personal data processing deriving from this data sharing remedy, in a fair and transparent manner.[2232] On the one hand, the data holder will have to inform the data subjects that it has been compelled by a competition authority to make some of the personal data concerning them available to a third party as a remedy to an abuse.[2233] On the other hand, the data recipient will have to inform the data subjects about the further processing it will conduct thanks to the data covered by the remedy.[2234] In this regard, the data recipient will notably have to inform the data subjects about the categories of personal data concerned, about the purposes of the processing for which the personal data are intended and about the period for which the personal data will be stored.[2235]

The data recipient will have to provide this information within a reasonable period after obtaining the personal data. This period should be determined by considering the specific circumstances in which the personal data are processed, and should, in any case, never be longer than one month.[2236] Nevertheless, if these personal data are used by the data recipient to communicate with the data subjects, this information will have to be provided at the latest at the time of the first communication.[2237] According to the Article 29 Working Party (today the European Data Protection Board), this does not preclude the one-month time limit mentioned above, and therefore the data recipient will have to provide the information at the time of the first communication (if it takes place less than one month after having obtained the data) or at the latest one month after having obtained the data.[2238]

However, there are situations where this information duty will not apply. On the one hand, it will not apply if the data subject already has the information.[2239] A data recipient might thus be tempted to say that the data subjects have already been informed by the data holder. Nevertheless, this will rarely be the case because the data holder will have provided information about the *transfer* but not about the *further processing* done by the data recipient

---

[2232] Articles 5.1.a) and 12 to 14 of the GDPR.
[2233] See the example of the GDF Suez case at point 357 (Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, available at https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf).
[2234] Article 14 of the GDPR.
[2235] Articles 14.1.c) and d) and 14.2.a) of the GDPR.
[2236] Article 14.3.a) of the GDPR.
[2237] Article 14.3.b) of the GDPR.
[2238] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 16.
[2239] Article 14.5.a) of the GDPR.

(the former might allegedly not even be aware of the concrete processing that will be accomplished by the latter). On the other hand, this information duty will not apply if the provision of such information proves impossible or would involve a disproportionate effort.[2240] Here, it should be mentioned that it will not always be easy for the data recipient to identify all the data subjects concerned by the data sharing, as the shared data should arguably be pseudonymised or aggregated personal data that cannot be immediately linked to well-identified data subjects. In this context, it can be questioned whether the recipient has a duty to make sure that the data holder will pass on the necessary contact details of the data subjects, as this would likely conflict with the data minimisation principle[2241], because this would entail the sharing of more data than is necessary for the purpose of the processing.[2242] In fact, Article 11.1 of the GDPR provides that data that is not necessary for the purpose of the processing should not be processed for the sole purpose of complying with the GDPR. Accordingly, additional data should not be transferred solely in order to be able to inform the data subjects about the sharing. Therefore, if, in light of the above, these details are not passed on, it might be impossible or disproportionate for the data recipient to inform the data subjects.

365. Second, both the data holder and the data recipient will have to comply with the purpose limitation principle.[2243] For the data holder, the purpose of the sharing will be the compliance with the competition authority's decision. For the data recipient, it will be important to define in advice, and ideally already in the competition authority's decision, for which specific purpose the data will be processed (e.g. which products or services does the data recipient intend to offer thanks to the shared data).

366. Third, the data holder and the data recipient will have to comply with the data minimisation principle, and only the necessary data for the fulfilment of the specific purpose justifying the data sharing shall be transferred by the data holder and processed by the data recipient.[2244] To facilitate the compliance with this principle, the use of pseudonymised data and of privacy-preserving techniques should be encouraged. Once again, this outlines the importance of defining in advance, and ideally already in the competition authority's decision, the specific purpose of the processing, in order for the data sharing remedy to cover only the data that is necessary to fulfil it. In the same vein, the accuracy of the shared data should be ensured and it should be stored by the data recipient for no longer than is necessary for this specific purpose.[2245]

367. Fourth, the data holder and the data recipient will have to ensure that the data subjects' rights, such as their right to object to the processing[2246], are given their fullest effect.[2247]

[2240] Article 14.5.b) of the GDPR.
[2241] Article 5.1.c) of the GDPR.
[2242] C. Wendehorst, "Of Elephants in the Room and Paper Tigers", *op. cit.*, p. 340-341.
[2243] Article 5.1.b) of the GDPR.
[2244] Article 5.1.c) of the GDPR.
[2245] Article 5.1.d) and e) of the GDPR
[2246] Article 21 of the GDPR. See the example of the GDF Suez case at point 357 (Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, available at https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf).

Accordingly, if a data holder receives, from a data subject, a valid request for rectification or erasure[2248] of some of the personal data covered by the data sharing remedy, it will have to notify it to the data recipient so that the data is also rectified or erased in the latter's dataset as well.[2249]

368. Finally, the data holder and the data recipient will have to implement appropriate technical and organisational measures in order to ensure the security of the data during the transfer and during the further processing[2250], and they will have to document how the implementation of the data sharing remedy complies with all of the above-mentioned principles, in light of the accountability principle.[2251]

c) Need for competition and data protection authorities to cooperate

369. It stems from the above analysis that, while some tensions might emerge between competition law and personal data protection law, they are not incompatible, and they can be reconciled by making a competition law duty to share data compliant with data protection principles. Yet, this is no easy task and it might be quite complex in certain specific situations. In practice, this implies the need for competition and data protection authorities to cooperate on this matter. Indeed, a competition authority might not be the best suited to handle these personal data protection aspects alone.[2252] Accordingly, the competition authorities should solicit the help of data protection authorities in defining the appropriate data sharing remedy, as the French *Autorité de la concurrence* has done in the *GDF Suez* case[2253], where it consulted the *Commission Nationale de l'Informatique et des Libertés* (the French data protection authority). The data protection authority could then be put in charge of supervising the correct implementation of the remedy from a personal data protection perspective. This might however create practical challenges, such as overlaps between the powers of the competition and personal data protection authorities. One way to address these challenges would be to organise regular meetings between these authorities, in order to follow-up on the implementation of the remedies and to deal with potential overlaps in a concerted way. Finally, this implies the need to interpret data protection law and competition law provisions in a coherent manner, in order to minimise conflicts and to maximise complementarity between these regimes.[2254]

[2247] Articles 13 to 22 of the GDPR.
[2248] Articles 16 and 17 of the GDPR.
[2249] Article 19 of the GDPR.
[2250] Article 5.1.f) and 32 of the GDPR.
[2251] Article 5.2 of the GDPR
[2252] See the discussions pertaining to the *Bundeskartellamt*'s (the German competition authority) decision in the *Facebook* case, summarised at point 338.
[2253] Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014, available at https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//14mc02.pdf. See point 357.
[2254] I. Graef, T. Tombal and A. de Streel, "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *op. cit.*, p. 31.

d) Articulating a competition law data sharing remedy with the GDPR: no incompatibility but risk of inefficiency

370. It derives from the above analysis that the effectivity of a competition remedy imposing data sharing might, in fact, be highly uncertain. Indeed, on the one hand, the data holder might arguably not be able to rely on the "legal obligation" lawful basis for the transfer of the data as long as the case law is not sufficiently clear and predictable. On the other hand, the data recipient might not always be able to rely on "legitimate interests" for its further processing, as there might be cases where its legitimate interests should not prevail over the data subjects' interests. Therefore, the effectivity of a competition remedy imposing data sharing might ultimately depend on the data subjects' consent. Yet, it might be illusory to obtain such consent and the competition remedy's aim might therefore not be achieved if only a handful of the data subjects effectively consent. Such a finding further supports the argument, made above[2255], according to which *ex post* competition law intervention might not, on itself, be sufficient to address efficiently the systemic market failures deriving from insufficient data sharing.[2256] This finding also supports the argument that "additional rules may be needed to ensure contestability, fairness and innovation and the possibility of market entry, as well as public interests that go beyond competition or economic considerations".[2257]

371. Accordingly, a bicephalous approach is recommended in this thesis, whereby *ex ante* legislations imposing B2B data sharing should complement competition law rules that have been adapted to the characteristics of the digital markets.[2258] These *ex ante* legislations will be further discussed in the next Chapter.

[2255] See Part III, Chapter 1, Section E, b) "Competition law may not be sufficient on itself: growing call for *ex ante* legislations imposing data sharing".

[2256] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Shaping Europe's digital future*", Brussels, 19 February 2020, COM(2020) 67, p. 9.

[2257] *Ibidem*.

[2258] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", Brussels, 19 February 2020, COM(2020) 66, p. 5 and 13-14; European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 10.

Chapter 3. Towards more *ex ante* legislations imposing B2B data sharing for economic purposes

372. This third Chapter will be dedicated to considerations pertaining to *ex ante legislations imposing B2B data sharing for economic purposes*. As outlined by the European Commission, such legislations could promote a wider sharing and availability of data, in order to ensure that markets stay open and fair.[2259] In essence, such *ex ante* legislations could be sectoral (**Section A**) or a could have a more general horizontal scope (**Section B**). Each of these options, which are not necessarily exclusive from one another, entail their own balancing exercises, which this thesis aims to analyse.

Section A. "ex ante" sectoral legislations imposing B2B data sharing for economic purposes

373. The first option is thus to adopt *ex ante* sectoral legislations imposing B2B data sharing. In fact, to this day, the EU's regulatory initiatives pertaining to compulsory B2B data sharing have mostly been sectoral. Compulsory data sharing legislations have notably been adopted in the banking and in the energy sector.[2260] However, these initiatives are classified, in the context of this thesis, in the *"empowerment" initiatives imposing B2B data sharing*[2261], as they could be seen as sector-specific complements to the personal data portability right contained in Article 20 of the GDPR, aiming at addressing specific market failures through the sharing of individual level data.[2262] On the other hand, in terms of *economic initiatives imposing B2B data sharing*, a sector-specific data sharing legislation has been adopted in the automotive sector[2263], which will be presented below. Moreover, in the agricultural sector, the European Commission supported the creation, by stakeholders from the sector, of the EU Code of conduct on agricultural data sharing by contractual agreement which can be joined by agri-businesses on a voluntary basis and sets some non-binding principles, notably in terms of data access, control and portability.[2264] However, as this instrument does not impose any data sharing obligation, it will not be further analysed in the context of this thesis.

[2259] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 5 and 14.
[2260] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015; Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, *OJ L 158/125*, 14 June 2019.
[2261] See Part II, Chapter 1, Section B, b) and c).
[2262] See G. Colangelo and O. Borgogno, "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule", *Stanford-Vienna European Union Law Working Paper No. 35*, 2018, available at https://law.stanford.edu/publications/no-35-data-innovation-and-transatlantic-competition-in-finance-the-case-of-the-access-to-account-rule/, p. 3; S. Vezzoso, "Fintech, Access to Data, and the Role of Competition Policy", 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106594, p. 12-13.
[2263] Regulation (EU) 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, *OJ L 171/1*, 29 June 2007, articles 6 and 7; Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L 151/1*, 14 June 2018. See articles 61 to 66, 86 and annexes X and XI.
[2264] See https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf.

a) The current strong reliance on sectoral legislations

374. In practice, most of the data sharing takes place within a single business sector, rather than in a horizontal way (across sectors). One of the reasons for this is that the European legislative framework itself favours sectoral approaches when it comes to data sharing.[2265] This was already apparent from the Communication "Towards a European Data Economy", where the European Commission indicated that it had stemmed from the stakeholder dialogue that it was too early for any form of horizontal legislation on data sharing.[2266] Accordingly, the Commission has chosen to let the data market self-regulate itself and to rely on contractual freedom, while nevertheless proposing key principles for the undertakings wishing to engage in *voluntary* B2B data sharing agreements.[2267] Nevertheless, the Commission indicated it that would continue to assess whether such key principles prove to be sufficient in order to maintain fair and open markets, and that it would address the situation, if necessary, "by taking appropriate action and *sector-specific measures*" (emphasis added).[2268] As outlined by several legal scholars, the advantage of resorting to sector-specific legislation is that they are much more targeted and adapted to the sector's needs, characteristics and data standardisation challenges.[2269] Moreover, in terms of personal data protection, it will be easier to comply with the requirement according to which the legislation serving as the lawful basis of the processing must be clearly formulated and must be sufficiently precise (for instance regarding the determination of the purposes of processing and of the categories of data that can be processed)[2270] if this legislation addresses a specific sectoral issue. In fact, the European Commission has confirmed this sectoral approach in its "Data Strategy", where it indicated that, through the means of a "Data Act" to be adopted in 2021, sector-specific data sharing could be made compulsory when "specific circumstances" dictate it.[2271]

375. As outlined by the European Commission, "specific circumstances" justifying the adoption of such a compulsory data sharing legislation would notably be established in situations where a (systemic) market failure (data concentration, data conglomeration, etc.)[2272]

[2265] See point 373.
[2266] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Towards a common European data space*", Brussels, 25 April 2018, COM(2018) 232 final, p. 9.
[2267] *Ibid*., p. 6-8. See points 64 and 65.
[2268] *Ibid*., p. 10-11.
[2269] J. Drexl, R. Hilty, J. Globocnik, F. Greiner, D. Kim, H. Richter, P. Slowinski, G. Surblytė, A. Walz and K. Wiedemann, "Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation on Building the European Data Economy"", *Max Planck Institute for Innovation and Competition Research Paper No. 17-08*, 2017, available at https://ssrn.com/abstract=2959924, p. 12-16; J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 159; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*"*, *op. cit*., p. 74; W. Kerber, "From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *Joint Discussion Paper Series in Economics No. 40-2020*, 26 August 2020, available at https://ssrn.com/abstract=3681263, p. 15-16.
[2270] Article 6.3 of the GDPR.
[2271] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 13, footnote 39. See also European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 1 and 4.
[2272] See Part I, Chapter 2, Section B, c), 3. "Data market failures".

is identified or can be foreseen in a specific sector, and cannot be (efficiently) remedied by competition law intervention alone[2273].[2274]

In fact, such "specific circumstances" have been observed in the automotive sector, which led, already in 2007, to the adoption of Regulation 715/2007 that notably compelled car manufacturers to share the vehicle repair and maintenance information that they hold with independent operators.[2275] In 2018, this data sharing obligation has been removed from Regulation 715/2007 and has been included in a new Regulation 2018/858[2276] that is applicable since the 1st of September 2020.[2277] This sectoral intervention is justified by the potential market failure that would arise on the aftermarkets for vehicle "on-board diagnostics" information services[2278], and for vehicle repair and maintenance information services[2279], if car manufacturers[2280] refused to share such data with independent operators[2281] active on those markets, while using it themselves and/or sharing it with authorised dealers or

---

[2273] See Part III, Chapter 1, Section E, b) "Competition law may not be sufficient on itself: growing call for *ex ante* legislations imposing data sharing".

[2274] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 13, footnote 39.

[2275] Regulation (EU) 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, *OJ L 171/1*, 29 June 2007, articles 6 and 7.

[2276] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L 151/1*, 14 June 2018. See articles 61 to 66, 86 and annexes X and XI.

[2277] Article 91 of Regulation 2018/858. For a comment on the data sharing aspects of this Regulation, see W. Kerber and D. Gill, "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation", *JIPITEC*, 2019, Issue 10, p. 244-256.

[2278] Vehicle on-board diagnostic (OBD) information means "the information generated by a system that is on board a vehicle or that is connected to an engine, and that is capable of detecting a malfunction, and, where applicable, is capable of signalling its occurrence by means of an alert system, is capable of identifying the likely area of malfunction by means of information stored in a computer memory, and is capable of communicating that information off-board" (Article 3.49 of Regulation 2018/858).

[2279] Vehicle repair and maintenance information means "all information, including all subsequent amendments and supplements thereto, that is required for diagnosing, servicing and inspecting a vehicle, preparing it for road worthiness testing, repairing, re-programming or re-initialising of a vehicle, or that is required for the remote diagnostic support of a vehicle or for the fitting on a vehicle of parts and equipment, and that is provided by the manufacturer to his authorised partners, dealers and repairers or is used by the manufacturer for the repair and maintenance purposes" (Article 3.48 of Regulation 2018/858).

[2280] Manufacturer "means a natural or legal person who is responsible for all aspects of the type-approval of a vehicle, system, component or separate technical unit, or the individual vehicle approval, or the authorisation process for parts and equipment, for ensuring conformity of production and for market surveillance matters regarding that vehicle, system, component, separate technical unit, part and equipment produced, irrespective of whether or not that person is directly involved in all stages of the design and construction of that vehicle, system, component or separate technical unit concerned" (Article 3.40 of Regulation 2018/858).

[2281] Independent operator "means a natural or legal person, other than an authorised dealer or repairer, who is directly or indirectly involved in the repair and maintenance of vehicles, and include repairers, manufacturers or distributors of repair equipment, tools or spare parts, as well as publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment for alternative-fuel vehicles; it also means authorised repairers, dealers and distributors within the distribution system of a given vehicle manufacturer to the extent that they provide repair and maintenance services for vehicles in respect of which they are not members of the vehicle manufacturer's distribution system (Article 3.45 of Regulation 2018/858). An independent repairer "means a natural or legal person who provides repair and maintenance services for vehicles and who does not operate within the manufacturer's distribution system" (Article 3.47 of Regulation 2018/858).

repairers[2282] active on those markets.[2283] Accordingly, such a data sharing obligation aims at ensuring effective competition on these aftermarkets, by allowing independent operators to compete with the car manufacturers themselves and/or authorised dealers or repairers.[2284] As the main objective is to promote competition on these aftermarkets, this justifies that Regulation 2018/858 is considered, in the context of this thesis, as an *economic initiative imposing B2B data sharing.*

More concretely, Regulation 2018/858 imposes on car manufacturers the obligation to share vehicle "on-board diagnostics" and repair and maintenance information with independent operators in an unrestricted, standardised, non-discriminatory and easily accessible manner, in the form of machine-readable and electronically processable datasets.[2285] Such sharing is, however, not free of charge, as manufacturers may charge reasonable and proportionate fees, which can be transaction-based or duration-based.[2286] Nevertheless, fees that discourage the sharing, because they fail to consider the extent to which the independent operator uses the information, will be considered unreasonable or disproportionate.[2287] Moreover, the details of the technical requirements for the sharing, notably the technical specifications on how the vehicle repair and maintenance information are to be provided, are laid down in Annex X of the Regulation.[2288]

376. Yet, with the advent of connected (automated) cars, the scope of this Regulation could be considered as being quite limited. Indeed, vehicles (will) increasingly generate a huge amount of data that are not only valuable for the car manufacturers, authorised dealers/repairers and independent operators involved in the repair and maintenance of vehicles, but also for a wide array of stakeholders who have an interest in accessing these in-vehicle data to provide additional services.[2289] These competing interests raise controversial questions about the control/sharing of these in-vehicle data.[2290] As explained by Kerber and Frank, three models of control/sharing can potentially be rolled-out:[2291]

- Firstly, the "extended vehicle" model, in which all in-vehicle data are transferred on central servers, outside of the car, controlled by the car manufacturers. In this model,

---

[2282] Authorised repairer "means a natural or legal person who provides repair and maintenance services for vehicles and who operates within the manufacturer's distribution system" (Article 3.46 of Regulation 2018/858).
[2283] Recital 52 of Regulation 2018/858.
[2284] *Ibidem*. See also W. Kerber and D. Gill, "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation", *op. cit.*, p. 245-247.
[2285] Article 61.1 of Regulation 2018/858.
[2286] Article 63.2 of Regulation 2018/858.
[2287] Article 63.1 of Regulation 2018/858.
[2288] Article 61.4 of Regulation 2018/858.
[2289] See W. Kerber, "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *JIPITEC*, 2018, Issue 9, p. 310-331.
[2290] See, for instance, D. Geradin, "Access to In-Vehicle Data by Third-Party Service Providers: Is there a Market Failure and, if so, How Should it be Addressed?", January 2020, available at https://ssrn.com/abstract=3545817; W. Kerber, "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *op. cit.*, p. 310-331; W. Kerber and D. Gill, "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation", *op. cit.*, p. 244-256; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 940-976.
[2291] W. Kerber and J. Franck, "Data Governance Regimes in the Digital Economy: The Example of Connected Cars", 3 November 2017, available at https://ssrn.com/abstract=3064794.

the recipients access the data on those remote servers (one for each car manufacturer), rather than directly in the car;

- Secondly, an adapted version of the "extended vehicle" model in which, instead of having one server for each car manufacturer, all the in-vehicle data would be transferred to a "shared server", controlled by a neutral party or a consortium rather than by the car manufacturers. In this model, while the recipients would still have to access the data on this remote server, it is a neutral third party that would decide whether these recipients can get access to the car manufacturers' data;
- Thirdly, the "on-board application platform" model, in which the data is not transferred on an external server, but rather remains in the vehicle that itself becomes the platform through which the recipients can access and use the in-vehicle data. The main difference with the two previous options is that it is now the car owner (or driver) that is in control of the access and that decides whether the recipients can get access to this data.

In practice, tensions arise from the fact that car manufacturers wish to opt for the "extended vehicle" model, giving them exclusive (almost monopolistic) control over these in-vehicle data. As explained by Kerber, repairers and independent service providers see this privileged position of manufacturers as a risk of competitive problems, and therefore call for regulatory initiatives imposing the sharing of such data, with a view to ensuring fair and undistorted competition.[2292] More specifically, they demand that the "extended vehicle" model be abandoned in favour of the "on-board application platform" model. On the one hand, this would allow these independent repairers and service providers to have access to data directly on the vehicle, in real time, rather than having to access the data via an external server controlled by the manufacturers, which necessarily implies a latency time. On the other hand, this solution makes it possible to break the manufacturers' *de facto* monopoly on this information, by entrusting the control of the access to the in-vehicle data to the vehicle owner (since the access terminal is located on board the vehicle), and no longer to the manufacturers, which is the case when the terminal is an external server located outside of the vehicle. Car manufacturers, on the other hand, are opposed to the adoption of such a model of "on-board application platform" for safety reasons. The argument often put forward in this respect is that by allowing access to data directly in the vehicle, rather than via an external server, this creates the risk that the vehicle could be hacked and that these hackings could potentially cause accidents. However, a report drafted by TRL for the European Commission demonstrated that an "on-board application platform" could be developed in such a way that a high and adequate level of security is ensured.[2293]

Although the European Commission is aware of these heated debates, it has indicated that it will, for the time being, limit itself to adopting a non-binding recommendation to improve

---

[2292] See W. Kerber, "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *op. cit.*, p. 310-331.

[2293] TRL, "Access to In-Vehicule Data and Resources – Final Report", *Study for the European Commission*, May 2017, available at https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf, p. 77-79.

access and reuse of mobility and vehicle data for commercial and non-commercial purposes. However, it indicated that it would continue to monitor developments and would stand ready to intervene, if necessary, to establish a more binding framework for in-vehicle data sharing in order to ensure fair competition.[2294] As outlined by Geradin, such an intervention would have to be based on the establishment of a market failure as this could create severe compliance costs for the car manufacturers.[2295] It would also have to precisely define (for instance by relying on market power considerations) the scope of the undertakings (manufacturers) that would be subject to such a data sharing obligation.[2296]

The automotive sector example provided above thus shows that the "specific circumstances" justifying the adoption of a compulsory data sharing legislation could be established in situations where a market failure is identified, or can be foreseen, in a specific sector, and cannot be (efficiently) remedied by competition law intervention alone.[2297]

b) Balancing exercises to be considered when adopting sectoral legislations

377. Importantly, the advantages offered by sectoral legislations, described above, must be balanced with the fact that sector-specific data sharing regimes might actually backfire and be more beneficial to large data holders than to small competitors, and could thus fail to make markets open and fair.[2298]

On the one hand, there is a risk that the sector-specific legislation might be more beneficial to the existing large data holders active in the sector. Indeed, as outlined by Kerber, such sector-specific legislations create a risk of "regulatory capture", namely that "important stakeholders in the sector might use their closeness to policy-makers to influence the regulation in favour of their own interests (rent-seeking behaviour), leading to wrong regulations that do not achieve (sufficiently) the intended policy objectives of more competition and innovation (regulatory failure)".[2299]

On the other hand, there is a risk that the sector-specific legislation might be more beneficial to large data holders active across sectors. This can be illustrated by the revised Directive on

---

[2294] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*On the road to automated mobility: An EU strategy for mobility of the future*", Brussels, 17 May 2018, COM(2018) 283, p. 13.

[2295] D. Geradin, "Access to In-Vehicle Data by Third-Party Service Providers: Is there a Market Failure and, if so, How Should it be Addressed?", *op. cit.*, p. 9-10. See also P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 947-948.

[2296] P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 963.

[2297] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 13, footnote 39.

[2298] See M. de la Mano and J. Padilla, "Big Tech Banking", *Journal of Competition Law & Economics*, 2018, Issue 14(4), p. 494–526; F. Di Porto and G. Ghidini, "'I Access Your Data You Access Mine'. Setting a Reciprocity Clause for the 'Access to Account Rule' in the Payment Services Market", 2019, available at https://ssrn.com/abstract=3407294, p. 23. See also European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf, p. 8.

[2299] See W. Kerber, "From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *op. cit.*, p. 16.

payment services in the internal market ("PSD2")[2300], presented above.[2301] Indeed, although it mainly aims at empowering consumers by giving them more control on their banking data and operations, and by providing them with more choice and transparency[2302], its secondary aim is to boost the emergence of (European) small FinTechs.[2303] Yet, as outlined by de la Mano and Padilla, such an instrument might arguably eventually be more beneficial to the existing (American) large data holders for which PSD2 has opened the gate of the payment service market.[2304] For instance, Apple has launched an "Apple Pay" service.[2305] Indeed, a sector-specific data sharing regime like PSD2 benefits these large data holders in two ways. Firstly, they can leverage all the non-banking data they already have about consumers to further refine the banking data they obtain via PSD2, in order to provide better payment services than the small FinTechs, but also than the traditional banks. Secondly, they can use this banking data to improve all their other data-driven services and strengthen their position on all the other data-driven markets in which they are active. This is because the value of data does not only come from the scale of data, but also from the scope of data, and these large data holders have a 360° view on the consumers' preferences. In short, such a sector-specific instrument might have the unwanted effect of making large data holders operating across sectors stronger, while exposing the data holders burdened with a sectoral data sharing obligation to fierce competition on their core business, and while potentially missing the original aim, namely boosting small competitors. This is mainly because these large data holders, operating horizontally across markets, have, so far, no comparable *ex ante* data sharing obligation.[2306]

Importantly, this analysis is not only applicable to the banking sector, but can be extended to any sector in which the European legislator would consider to adopt a sector-specific legislation imposing B2B data sharing. For instance, if one reverts to the above discussions pertaining to the control/sharing of in-vehicle data[2307], the same risk might appear, in the sense that a data sharing legislation imposing an obligation, on car manufacturers, to share such in-vehicle data with independent service providers might arguably be more beneficial for large data holders, who would thereby be offered the possibility to enter such markets, than for small independent service providers. Indeed, whatever the sector, large data holders can leverage all the non-sectoral data they already have about consumers to further refine the

---

[2300] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015.
[2301] See Part II, Chapter 1, Section B, b), 1. "Access to and use of banking data in PSD2".
[2302] See Recitals 5, 6, 28 and 67 of the Directive 2015/2366.
[2303] See Recital 67 of the Directive 2015/2366.
[2304] See M. de la Mano and J. Padilla, "Big Tech Banking", *op. cit.*, p. 494–526. See also Netherlands Authority for Consumers and Markets, "Big Techs in the payment system", 16 November 2020, available at https://www.acm.nl/en/publications/acm-study-big-techs-dutch-payment-system, specifically p. 37-38 and 41-48.
[2305] See https://www.apple.com/befr/apple-pay/; Netherlands Authority for Consumers and Markets, "Big Techs in the payment system", *op. cit*., p. 21-24 (see p. 24-31 for explanations on the Google Pay, Amazon Pay and Facebook Pay services). It should be noted that the European Commission has opened, in June 2020, a formal antitrust investigation into Apple's conduct in connection with Apple Pay (see https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1075).
[2306] See however Part III, Chapter 3, Section B, b).
[2307] See point 376.

sectoral data they obtain, in order to provide better services than the small sectoral competitors. Moreover, they can use this sectoral data to improve all their other data-driven services.

378. One way to alleviate this risk and to solve this balance would be to exclude the large data holders from the benefit of such sector-specific compulsory data sharing legislations. However, this might be difficult to justify because this could arguably lead to an unlawful discrimination against these large data holders. Indeed, when entering the market, they will likely be small competitors like all the others. In this perspective, it might not be objectively justifiable to refuse to share data with them merely on the basis of the "potentiality" of the advantage that they could gain from data leveraging practices. Indeed, they might end up developing a product/service that is not as good as the one developed by a smaller actor in the specific (niche) market, and completely denying them the opportunity to compete could be seen as excessive.

Alternatively, Di Porto and Ghidini suggest another way to alleviate this risk and to solve this balance, namely adding a reciprocity clause in the sector-specific legislation, according to which large data holders[2308] relying on this legislation to get access to the sectoral data should provide the undertakings that are compelled to share data with a reciprocal right to access some of their data (such as behavioural data), provided that the individuals consented to this.[2309] However, it must be pointed out that such a reciprocity clause would not address the totality of this issue, as it would only benefit the undertakings that are subject to the sector-specific data sharing legislation, but not the smaller service providers trying to compete with these undertakings and with the large data holders.

379. Moreover, the advantages of resorting to sector-specific data sharing must be balanced with the fact that data is a non-rivalrous and general-purpose resource that could be re-used for completely different purposes in another sector.[2310] In fact, a study by Deloitte has estimated that 24% to 36% of the benefits of data sharing will derive from cross-sectoral data sharing.[2311] Such cross-sectoral re-use could indeed generate additional economic value (one could think of data collected by sensors on machines in an car assembly line, which could be re-used for other purposes in other sectors). Accordingly, limiting the scope of the compulsory data sharing legislation to re-uses within a single sector would not enable the generation of such additional economic value.

[2308] Di Porto and Ghidini refer to "digital conglomerates".

[2309] F. Di Porto and G. Ghidini, "'I Access Your Data You Access Mine'. Setting a Reciprocity Clause for the 'Access to Account Rule' in the Payment Services Market", *op. cit.*, p. 23.

[2310] See point 52.

[2311] Deloitte, "Realising the economic potential of machine-generated, non-personal data in the EU", *Report for Vodaphone Group*, July 2018, available at https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf, p. 32. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final, p. 15.

Section B. Creation of horizontal "ex ante" legislations imposing B2B data sharing for economic purposes: necessary balancing exercises

380. As demonstrated in the previous Section, while sectoral legislations imposing data sharing present advantages, they also entail some risks and they present some limitations. Therefore, in parallel to these sectoral approaches, *ex ante* compulsory B2B data sharing initiatives having a more horizontal scope could be pursued.[2312] Indeed, these two approaches are not mutually exclusive, as these horizontal legislations could be seen as a subsidiary form of intervention, providing for a minimal level-playing field across sectors and in sectors where no sector-specific legislation exists.[2313] They could also be used to address economic concerns that extend beyond specific sectors.

381. Yet, like any other initiative imposing B2B data sharing, such horizontal *ex ante* legislations will entail balancing exercises. In substance, the economic benefits deriving from the wider data sharing that such legislations would entail would have to be balanced with the data holder's business interests. Indeed, data sharing might deter innovation by the data holder that is compelled to share its data, as it might no longer want to invest in data collection that used to provide him with a competitive advantage, as it fears free-riding.[2314] Moreover, it should also be factored that imposing data sharing for economic purposes (addressing data market failures)[2315] might also deter innovation by third parties (expectation to free-ride). Additionally, these horizontal legislations will have to comply with the personal data protection rules.[2316]

382. One way to address these issues would be to consider, by analogy with what has been said for sectoral legislations[2317], that such horizontal *ex ante* legislations imposing B2B data sharing should only be created when "specific circumstances" justify it. Indeed, such legislations should only be adopted if they are proportional and necessary to address these "specific circumstances", in order to achieve an optimal balance with the data holder's freedom to conduct a business.

From an economic perspective, such "specific circumstances" would notably be established in situations where a (systemic) market failure[2318] is identified or can be foreseen, and cannot be (efficiently) remedied by competition law intervention alone[2319].[2320] In this regard, the

---

[2312] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 159-161.
[2313] *Ibid*., p. 160. See also W. Kerber, "From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *op. cit.*, p. 16; European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 5.
[2314] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 374.
[2315] See Part I, Chapter 2, Section B, c), 3. "Data market failures".
[2316] See points 91 and 96 and Part III, Chapter 2 and Chapter 3, Section B, b). See European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, *op. cit*., p. 8.
[2317] See points 374 and 375.
[2318] See Part I, Chapter 2, Section B, c), 3. "Data market failures".
[2319] See Part III, Chapter 1, Section E, b) "Competition law may not be sufficient on itself: growing call for *ex ante* legislations imposing data sharing".
[2320] Communication from the Commission, "*A European strategy for data*", *op. cit*., p. 13, footnote 39.

European Commission had announced, in the past, that it would consider the adoption of a horizontal *ex ante* regulation to address systemic issues related to platforms and data.[2321]

More recently, the European Commission has proposed the adoption of a "Digital Markets Act"[2322] in the context of its Digital Services Act package.[2323] This Act is an "*ex ante* regulatory instrument for large online platforms with significant network effects acting as gatekeepers[2324] in the European Union's internal market".[2325] According to the European Commission, the "specific circumstances" justifying the adoption of such a regulation are that these gatekeepers benefit from strong network effects due to their large user base and that, as a result, they "exercise control over whole platform ecosystems in the digital economy and are structurally extremely difficult to challenge or contest by existing or new market operators, irrespective of how innovative and efficient these may be".[2326] Moreover, due to these gatekeepers' ability to leverage their data advantage from their core market to adjacent markets, there is a risk that these adjacent markets could also tip in favour of these gatekeepers, to the detriment of consumer choice and innovation.[2327] There is thus a risk that innovative new actors (SMEs, start-ups, etc.) could be unfairly excluded from entry.[2328]

In order to tackle (or even prevent) these market failures, the proposal for a Digital Markets Act suggests that the European Commission should be empowered to determine whether a

---

[2321] *Ibid*., p. 14. See also Communication from the Commission, "*Shaping Europe's digital future*", *op. cit*., p. 9.

[2322] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*", Brussels, 15 December 2020, SWD(2020) 363 final.

[2323] For recommendations and comments pertaining to this this DMA proposal, see A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *CERRE Recommendations Paper*, November 2020, available at https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/; A. de Streel, B. Liebhaberg, A. Fletcher, R. Feasey, J. Krämer and G. Monti, "The European Proposal for a Digital Markets Act: A First Assessment", *CERRE Assessment Paper*, January 2021, available at https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/; L. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. Valletti and M. Van Alstyne, "The EU Digital Markets Act: A Report from a Panel of Economic Experts", *EU Science Hub*, 2021, available at https://ec.europa.eu/jrc/en/publication/eu-digital-markets-act; A. de Streel and P. Larouche, "The European Digital Markets Act proposal: How to improve a regulatory revolution", *Concurrences*, 2021, N° 2, p. 46-63.

[2324] See Articles 2.1 and 3 of the Proposal for a Digital Markets Act. A data holder will be considered as gatekeepers if: "(a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future" (Article 3.1 of the Proposal). For more details on the designation of these gatekeepers, see points 397 and 398.

[2325] European Commission, Inception Impact Assessment: "*Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market*", June 2020, Ares(2020)2836174, p. 1.

[2326] Recital 3 of the Proposal for a Digital Markets Act.

[2327] Recitals 25 and 26 of the Proposal for a Digital Markets Act. See also European Commission, Inception Impact Assessment: "*Digital Services Act package*", *op. cit.*, p. 2.

[2328] Recitals 3, 36 and 56 of the Proposal for a Digital Markets Act. See also p. 1-3 of the Explanatory memorandum of this Proposal; European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 35.

specific data holder offering a "core platform service"[2329] meets the "gatekeeper" threshold.[2330] In this regard, it shall work in close cooperation and coordination with the Member States[2331], and it shall be assisted by the Digital Markets Advisory Committee[2332], composed of Member States' representatives having an expertise in the platform economy.[2333] If a large data holder is designated as a "gatekeeper", it will have to comply, within six months of its inclusion in the "list of gatekeepers"[2334], with Articles 5 and 6 of the proposal for a Digital Markets Act, which contain a series of obligations, as well as prohibited practices that limit contestability or that are unfair.[2335] For instance, "gatekeepers" will have to ensure specific types of data sharing, as they will notably have to provide "to any third party providers of online search engines, upon their request, access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data".[2336] This would ensure that the markets impacted by such gatekeepers would remain fair and contestable[2337], by potentially arousing the entrance of innovative new actors, and would thereby promote consumer choice and drive innovation beyond what can be achieved on the sole basis of competition law enforcement.[2338] The measures implemented by the "gatekeeper" to comply with these obligations and to abstain from adopting such prohibited practices will have to be

---

[2329] See Article 1.2 of the Proposal for a Digital Markets Act. "Core platform services" are: "(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; (h) advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g)" (Article 2.2 of the Proposal). For a definition of these services, see Articles 2.5 to 2.11 of the Proposal. For more information on why these services are considered as "core platform services", see Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*", Brussels, 15 December 2020, SWD(2020) 363 final, p. 37-45, 64-78, 82, 85 and 96-120.

[2330] See points 397 and 398.

[2331] Articles 1.7 and 19.6 of the Proposal for a Digital Markets Act.

[2332] Article 32 of the Proposal for a Digital Markets Act.

[2333] Proposal for a Digital Markets Act, p. 9.

[2334] Articles 3.7 and 4.3 of the Proposal for a Digital Markets Act.

[2335] Article 3.8 of the Proposal for a Digital Markets Act. Gatekeepers are, for example, prohibited from engaging in some forms of personal data combination (Article 5.a)), of tying of ancillary services (Articles 5.e) and f)), and of self-preferencing (Articles 6.1.a) and d)); and from adopting most-favoured-nation clauses (Article 5.b)). Moreover, they will have to allow specific types of data sharing (Articles 6.1.h), i) and j)) and of interoperability (Articles 6.1.c) and f)). On the rationale for the inclusion of these obligations and prohibited practices in the Proposal, see Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*", Brussels, 15 December 2020, SWD(2020) 363 final, p. 50-60, 64-78, 82, 85 and 96-120. For an assessment of these obligations and prohibitions, see A. de Streel, B. Liebhaberg, A. Fletcher, R. Feasey, J. Krämer and G. Monti, "The European Proposal for a Digital Markets Act: A First Assessment", *op. cit.*, p 6-7 and 16-23.

[2336] Article 6.1.j) of the Proposal for a Digital Markets Act. See also the data sharing obligations contained in Article 6.1.h), presented at point 169, and Article 6.1.i), presented at point 182. See also Recitals 54 to 56.

[2337] European Commission, Inception Impact Assessment: "*Digital Services Act package*", *op. cit.*, p. 1.

[2338] European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 19.

effective and proportionate, and can be specified by the Commission if need be.[2339] The Commission will monitor the effective implementation and compliance with these provisions and it may issue non-compliance or fining decisions in case of breach of these provisions.[2340] The "gatekeeper" can also offer commitments to ensure compliance with the Digital Markets Act.[2341] This list of obligations and prohibited practices can be updated by the Commission, on the basis of delegated acts, in order to address new practices that might emerge and that might be unfair or limit the contestability of data markets.[2342] According to Article 10.2 of the Proposal, a practice should be considered as unfair or as limiting the contestability of data markets if "(a) there is an imbalance of rights and obligations on business users and the gatekeeper is obtaining an advantage from business users that is disproportionate to the service provided by the gatekeeper to business users; or (b) the contestability of markets is weakened as a consequence of such a practice engaged in by gatekeepers".

383. Furthermore, if such "specific circumstances" are established, the need to find a balance with the data holder's business interests and the need to comply with the individuals' right to personal data protection will also have to be factored in the determination of the provisions to be included in the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes (b). To do so, some guiding principles could be sought in the fields of government-to-business (G2B)[2343] and business-to-government (B2G)[2344] data sharing (a).

a) Valuable insights from the fields of G2B and B2G data sharing

384. While this thesis focusses on compulsory business-to-business data sharing (B2B data sharing), it must not be overlooked that data sharing also occurs between governments and businesses (G2B and B2G data sharing). Accordingly, when reflecting on the determination of the provisions to be included in the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes, insights could be sought in these fields.

1. G2B data sharing: PSI Directive

385. Guiding principles could first be sought in the field of compulsory government-to-business (G2B) data sharing, which has a clear legal framework since the beginning of this millennium. Indeed, in 2003, the European legislator adopted the Public Sector Information (PSI) Directive, which invited public sector bodies to open their public sector information for

---

[2339] Article 7 of the Proposal for a Digital Markets Act.
[2340] See Articles 24 to 26 of the Proposal for a Digital Markets Act.
[2341] Article 23 of the Proposal for a Digital Markets Act.
[2342] Articles 10 and 34 of the Proposal for a Digital Markets Act.
[2343] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019; H. Richter, "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *Max Planck Institute for Innovation and Competition Research Paper No. 20-03*, 2020, available at: https://ssrn.com/abstract=3565762.
[2344] High-Level Expert Group on Business-to-Government Data Sharing, "Towards a European strategy on business-to-government data sharing for public interests – Final report", 2020, available at https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more; H. Richter, "The Law and Policy of Government Access to Private Sector Data ('B2G Data Sharing')", *Max Planck Institute for Innovation and Competition Research Paper No. 20-06*, 2020, available at: https://ssrn.com/abstract=3594109.

re-use.[2345] However, given that the public sector bodies had the choice, rather than the obligation, to open their data, only few of them did so. To remedy that weakness, the PSI Directive was amended in 2013 to force public sector bodies to make their public sector information re-usable for commercial or non-commercial purposes, for free or with charges limited to the marginal costs incurred for their reproduction, provision and dissemination.[2346] More recently, in June 2019, the European legislator adopted a recast version of the PSI Directive, that will have to be transposed in all Member States by July 2021.[2347] This string of legislations was motivated by the fact that public sector data are highly valuable resources that can be used to foster accountability and transparency, and to foster the European economy by generating digital innovation and preventing the distortion of competition in the internal market.[2348]

The last recast of the PSI Directive brings substantial modifications. Firstly, the scope of the Directive is extended to publicly funded research data.[2349] Secondly, there are modifications in terms of the price that can be charged by the public sector bodies. Indeed, the publicly funded research data mentioned above will have to be shared for free.[2350] Another new category of public data, namely "high-value datasets"[2351] – the list of which will have to be laid down in an implementing act by the European Commission[2352]–, will also have to be shared for free.[2353] These "high-value datasets" must also be made available for re-use in machine-readable format, via suitable APIs and, where relevant, as a bulk download.[2354] Thirdly, the recast provides that public sector bodies shall make dynamic data[2355] available for

[2345] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ L 345/90*, 31 December 2003.
[2346] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, *OJ L 175/1*, 27 June 2013, Articles 3.1 and 6.1.
[2347] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019.
[2348] See Recitals, 3, 7, and 11 of the Directive 2019/1024.
[2349] Article 10 of the Directive 2019/1024.
[2350] Article 6.6.b) of the Directive 2019/1024.
[2351] "Documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets" (Article 2.10 of the Directive 2019/1024). See also Annex 1 of Directive 2019/1024 for a list of thematic categories of high-value datasets.
[2352] The Commission indicated in its "Data Strategy" that it aimed to adopt such an act in 2021 (Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 13).
[2353] Articles 6.6.a) and 14.1 of the Directive 2019/1024.
[2354] Article 5.8 of the Directive 2019/1024.
[2355] "Documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data" (Article 2.8 of the Directive 2019/1024).

re-use immediately after collection, via suitable APIs.[2356] Finally, the scope of the PSI Directive has been extended to the data held by public undertakings.[2357]

Building on the PSI Directive, the European Commission also proposed, at the end of 2020, a Data Governance Act, which notably aims at laying down the conditions for the re-use of certain categories of data held by public sector bodies, such as those that are "protected" on the grounds of commercial or statistical confidentiality, or on the grounds of the protection of the intellectual property rights of third parties.[2358] For those types of data, re-use could be authorised if the data have been pre-processed in order to delete commercially confidential information, or if the access and re-use take place in a secure environment provided and controlled by the public sector body, either remotely or physically if remote access cannot be allowed without jeopardising the rights and interests of third parties.[2359] In this context, "the public sector body shall be able to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties".[2360] If it is not possible for the public sector body to pre-process the data or to provide a secure environment for the re-use, such re-use will only be allowed if it is permitted by the legal entity whose rights and interests may be affected.[2361]

It should however be added that, contrary to the 2019 PSI Directive, this proposed Data Governance Act would not apply to data held by public undertakings.[2362] The proposed Data Governance Act also outlines that its provisions complement, and are thus without prejudice to, the rules contained in the PSI Directive and its national transpositions.[2363] Finally, the proposed Data Governance Act does not create any *compulsory* G2B data sharing obligation, but rather aims at stimulating *voluntary* G2B data sharing. In this perspective, the European Commission seems to repeat the "experimental" approach that it adopted for the PSI Directive, which did not contain any *compulsory* G2B data sharing obligation either in its first version of 2003.

[2356] Article 5.5 of the Directive 2019/1024. An application programming interface (API) "is an interface or communication protocol between a client and a server intended to simplify the building of client-side software. It has been described as a "contract" between the client and the server, such that if the client makes a request in a specific format, it will always get a response in a specific format or initiate a defined action" (https://en.wikipedia.org/wiki/Application_programming_interface).

[2357] Article 1.1.b) of the Directive 2019/1024. Public undertaking are the undertakings "over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly: (a) hold the majority of the undertaking's subscribed capital; (b) control the majority of the votes attaching to shares issued by the undertaking; (c) can appoint more than half of the undertaking's administrative, management or supervisory body" (Article 2.3 of the Directive 2019/1024).

[2358] Articles 1.1.a) and 3 to 8 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*

[2359] Articles 5.3 and 5.4 of the Proposal for a Data Governance Act.

[2360] Article 5.5 of the Proposal for a Data Governance Act.

[2361] Articles 5.6 to 5.8 of the Proposal for a Data Governance Act.

[2362] Article 3.2.a) of the Proposal for a Data Governance Act.

[2363] Article 3.3 of the Proposal for a Data Governance Act. See also p. 1 and 7 of the "Explanatory memorandum" contained in that Proposal.

386. While this thesis will not delve extensively in these initiatives pertaining to G2B data sharing, since it focusses on B2B data sharing, the fact that the scope of the PSI Directive has been extended to the data held by public undertakings[2364] is worth pointing out in the context of this thesis because, as outlined by Richter, public undertakings "lie at the state-market interface".[2365] Indeed, they have a hybrid nature because while some of their activities aim at serving public interest objectives, they also have commercial activities for which they face competition and aim for profitability.[2366] Therefore, their inclusion in the scope of the PSI Directive implied a need "to reconcile market rationale with the public interest".[2367] This is because "many public undertakings fear a structural competitive disadvantage should regulation mandate only them – and not private undertakings – to share their data with everyone (including competitors)".[2368]

In the PSI Directive, this reconciliation between business and public interests stems from three important mitigating factors of the extension of the scope of the Directive to public undertakings. First, the Directive only applies to certain categories of public undertakings, namely those active in the public utilities (gas, water, electricity) and the transport sectors.[2369] Second, it only applies to public undertakings' data that have been produced in the context of the services of general interest that they provide, and therefore does not extend to data produced in the context of activities for which they are directly exposed to competition.[2370] Third, public undertakings have the choice to allow the re-use of their data, although if they do share their data with at least one re-user, they will arguably have to share it with any potential re-user wishing to use it for commercial or non-commercial purposes, including potential competitors.[2371]

387. In fact, such a reconciliation between business and public interests is also needed when considering the adoption of horizontal *ex ante* legislations imposing B2B data sharing for economic purposes, as the economic considerations justifying the sharing must be balanced

---

[2364] Article 1.1.b) of the Directive 2019/1024. Public undertaking are the undertakings "over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly: (a) hold the majority of the undertaking's subscribed capital; (b) control the majority of the votes attaching to shares issued by the undertaking; (c) can appoint more than half of the undertaking's administrative, management or supervisory body" (Article 2.3 of the Directive 2019/1024).

[2365] H. Richter, "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *Max Planck Institute for Innovation and Competition Research Paper No. 20-03*, 2020, available at: https://ssrn.com/abstract=3565762, p. 1.

[2366] *Ibid*., p. 2.

[2367] *Ibid*., p. 7.

[2368] *Ibid*., p. 8.

[2369] Namely the public undertakings that are "(i) active in the areas defined in Directive 2014/25/EU; (ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007; (iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008; or (iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Regulation (EEC) No 3577/92" (Article 1.1.b) of the Directive 2019/1024).

[2370] Article 1.2.b) of the Directive 2019/1024.

[2371] See Recital 22 and Articles 3.2 and 12 of the Directive 2019/1024. On this point, see H. Richter, "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *op. cit.*, p. 12-13 and 16-17.

with the data holder's business interests. Accordingly, some guiding principles developed for the sharing of public undertakings' data can be of value in the context of this thesis.

The first valuable principle to consider is that the data produced in the context of the public undertakings' activities for which they are directly exposed to competition are excluded from the scope of the PSI Directive.[2372] This is because these data are the ones that are the most commercially sensitive for the public undertakings. By analogy, when adopting horizontal *ex ante* legislations imposing B2B data sharing for economic purposes, the European legislator could consider to exclude from its scope of application the data that are the most commercially sensitive for the data holders.[2373] In this perspective, this could amount to excluding the holder's inferred/derived data from the scope of such legislations.[2374]

The second valuable principle to consider is that, while the PSI Directive now makes it explicit that public sector bodies should not exercise their database rights[2375] to restrict the re-use of their data, this provision does not apply to public undertakings.[2376] Therefore, public undertakings could rely on such a right to refuse to share some of their data (i.e. those that fall within the scope of this database right), as they have no general obligation to allow the re-use of their data.[2377] However, if they allow the re-use of such data by at least one re-user, they will arguably have to share it with any potential re-user wishing to use it for commercial or non-commercial purposes, in accordance with the rules of the PSI Directive.[2378] Nevertheless, the Directive allows them to subject this re-use to a licence and to a remuneration.[2379] In a way, these public undertakings are thus subject to a compulsory licensing scheme. Regarding the licence, it must be pointed out that the re-use can only be subject to conditions that are objective, proportionate and non-discriminatory, and that these conditions cannot unnecessarily restrict possibilities for re-use nor be used to restrict competition.[2380] Once subject to the PSI Directive, a public undertaking could thus not refuse to share its data with a competitor. Regarding the remuneration, given the fact that public undertakings are presumed to be active in competitive economic environments[2381], they do not have to share the data free of charge, but can rather recoup "the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and — where applicable — the anonymisation of personal data and measures taken to protect commercially

---

[2372] Article 1.2.b) of the Directive 2019/1024.
[2373] On this necessity to respect the data holder's commercial interests, see also Communication from the Commission, "*Towards a common European data space*", *op.cit.*, p. 10.
[2374] See Part III, Chapter 3, Section B, b), 3, i.
[2375] See point 58. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 77/20*, 27 March 1996.
[2376] Article 1.6 of the Directive 2019/1024.
[2377] Recital 26 of the Directive 2019/1024.
[2378] See Recital 22 and Articles 3.2 and 12 of the Directive 2019/1024. On this point, see H. Richter, "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *op. cit.*, p. 12-13 and 16-17.
[2379] Articles 6 and 8 of the Directive 2019/1024.
[2380] Article 8 of the Directive 2019/1024.
[2381] Recital 36 of the Directive 2019/1024. On this point, see H. Richter, "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *op. cit.*, p. 18.

confidential information".[2382] Public undertakings can, however, not charge any fee for publicly funded research data or "high-value datasets"[2383], unless sharing these "high-value datasets" for free would distort competition in the relevant markets where the public undertaking is active.[2384] By analogy, horizontal *ex ante* legislations imposing B2B data sharing for economic purposes could provide that the data holder is compelled to licence any potential database right that it may have on the data covered by the scope of the legislation.[2385] These legislations could also provide that the conditions of these licences should not restrict re-use possibilities and competition, and that they should be objective, proportionate and non-discriminatory. In exchange for this compulsory licencing, the legislations could nevertheless provide that the data holder is entitled to a remuneration.[2386]

The third valuable principle to consider is that the PSI Directive does not imply an obligation for public undertakings to create/collect new data or to adapt existing data in order to enable the re-use by data recipients, if this would involve disproportionate efforts going beyond a simple technical operation.[2387] Similarly, public undertakings are not required to continue processing and storing data that is no longer useful for it simply because a re-user relies on it for its activities.[2388] Nevertheless, in the latter case, it should make those decisions publicly known, at the earliest opportunity.[2389] By analogy, the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes could provide that the data holder does not have the obligation to create/collect new data or to adapt existing data in order to enable the re-use by data recipients, if this would involve disproportionate efforts going beyond a simple technical operation. Moreover, the legislations could provide that the data holder would not have the obligation to keep collecting and processing data that is no longer useful for it simply because a re-user relies on it for its activities. In the latter case, these legislations could nevertheless require the data holder to be transparent about this and to make its decision publicly known as soon as possible, in order for the data re-users to adapt.

388. Additionally, guidance can be sought in the PSI Directive in order to find a way to reap the economic benefits deriving from the wider data sharing that horizontal *ex ante* legislations would entail, while complying with the right to privacy and to personal data protection of the multiple individuals whose data would be shared.[2390] In this regard, the PSI Directive outlines that its provisions shall not affect the individuals' protection of their personal data.[2391] This notably means that the re-use of personal data will only be permissible to the extent that it

---

[2382] Article 6.1 of the Directive 2019/1024.
[2383] Article 6.6 of the Directive 2019/1024.
[2384] Article 14.3 of the Directive 2019/1024.
[2385] J. Drexl, "Data Access and Control in the Era of Connected Devices", *Study on Behalf of the European Consumer Organisation (BEUC)*, 2019, available at https://www.beuc.eu/publications/beuc-x-2018 121_data_access_and_control_in_the_area_of_connected_devices.pdf, p. 164.
[2386] On this remuneration, see Part III, Chapter 3, Section B, b), 4.
[2387] Recital 33 and Articles 5.3 and 5.7 of the Directive 2019/1024.
[2388] Articles 5.4 and 5.7 of the Directive 2019/1024.
[2389] Recital 45 of the Directive 2019/1024.
[2390] European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf, p. 8.
[2391] Recital 52 and Article 1.4 of the Directive 2019/1024.

complies with the GDPR's principles, such as purpose limitation[2392], and that it relies on a lawful basis of processing[2393].[2394] Interestingly, the PSI Directive outlines that one of the ways to reconcile these two seemingly contradictory bodies of law (the GDPR limits data re-use while the PSI Directive calls for more data openness and re-use) would be to anonymise the data, and that the marginal costs incurred for the anonymisation of personal data can be charged to the re-users.[2395] By analogy, the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes should also make it explicit that they shall not affect the individuals' protection of their personal data, and that the re-use of such personal data would only be permissible to the extent that it complies with the rules of the GDPR.[2396] Moreover, these legislations could provide that if the data holder anonymises the personal data before sharing it, it could charge the marginal costs incurred for the anonymisation to the re-users. However, it is difficult to truly anonymise a dataset.[2397]

389. Finally, it is interesting to point out that the PSI Directive plays an overarching horizontal standardisation role for G2B data sharing, which leaves room for more sector-specific regimes of access and re-use[2398], as illustrated by the INSPIRE Directive that establishes an infrastructure for spatial data in order to support environmental policies[2399], or the ITS Directive that establishes a framework to support the coherent and coordinated deployment and use of Intelligent Transport Systems.[2400] While such sectoral regimes globally rely on the same model as the PSI Directive, they essentially go further in terms of technical standardisation and interoperability requirements for the sharing.[2401] By analogy,

---

[2392] Article 5.1.b) of the GDPR.
[2393] Article 6 of the GDPR.
[2394] Recital 52 of the Directive 2019/1024.
[2395] Article 6.1 of the Directive 2019/1024.
[2396] On this articulation, see Part III, Chapter 2, Section B; and Part III, Chapter 3, Section B, b), 3, ii.
[2397] See point 353. See also J. Drexl, "Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy", *Max Planck Institute for Innovation & Competition Research Paper No. 18-23*, 31 October 2018, available at https://ssrn.com/abstract=3274519, p. 4. See also I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, September 2018, available at http://ssrn.com/abstract=3256189, p. 6; and C. Wendehorst, "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 330-331; L. Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality", *Journal of Law, Medicine & Ethics*, 1997, Vol. 25, Issues 2 & 3, p. 98-110; L. Rocher, J. Hendrickx and Y.-A. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, 2019, Vol. 10, n°3069, available at https://www.nature.com/articles/s41467-019-10933-3.
[2398] See H. Richter, "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *op. cit.*, p. 25-27.
[2399] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), *OJ L 108/1*, 25 April 2007. Spatial data are "any data with a direct or indirect reference to a specific location or geographical area" (Art. 3.2).
[2400] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, *OJ L 207/1*, 6 August 2010. Intelligent Transport Systems are "systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport" (Art. 4.1).
[2401] See Articles 5 to 10 of the Inspire Directive and Articles 6 and 8 of the ITS Directive.

and as argued above[2402], *ex ante* compulsory B2B data sharing initiatives having a horizontal scope could be created as a subsidiary form of intervention, providing for a minimal level-playing field across sectors and in sectors where no sector-specific legislation exists.[2403] They could also be used to address economic concerns that extend beyond specific sectors.

2. B2G data sharing

390. Guiding principles could also be sought in the field of business-to-government (B2G) data sharing. Indeed, considerations pertaining to B2G data sharing were notably evoked, at the European level, in 2017 during the public consultation pertaining to the latest recast of the PSI Directive.[2404] More concretely, the European Commission initiated, in its public consultation, a discussion on whether a new provision could be included in the PSI Directive, according to which data held by private companies, and deemed to be of public interest, should be shared with public sector bodies.[2405] Yet, while 88% of the 205 respondents to the public consultation, across all types of contributors, supported this proposition, such a provision was finally not included in the recast of the Directive.[2406] However, it should be pointed out that Recital 19 of the 2019 PSI Directive provides that "Member States may also decide to apply the requirements of this Directive to private undertakings, in particular those that provide services of general interest". This has notably been done, to a certain extent, in France.[2407]

The reason why such a provision was eventually not included in the PSI Directive is that many stakeholders responding to the public consultation had outlined that the Commission had failed to provide a sufficiently clear definition of these "public interests" and that the objectives and scope of such a proposition also lacked clarity.[2408] According to these stakeholders, further discussions were needed regarding these B2G data sharing initiatives.[2409] To conduct such further discussions, the European Commission appointed a High-Level Expert Group on Business-to-Government Data Sharing.[2410] Its mandate was notably to evaluate the key principles for the supply of private sector data to public sector bodies under

---

[2402] See point 380.
[2403] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 160.
[2404] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019. On this recast, see point 385.
[2405] See https://ec.europa.eu/info/consultations/public-consultation-review-directive-re-use-public-sector-information-psi-directive_en.
[2406] European Commission, "Consultation on PSI Directive review – Synopsis report", 25 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-revision-directive-reuse-public-sector-information, p. 8.
[2407] Loi n° 2016-1321 pour un république numérique du 7 octobre 2016, *J.O.*, 8 octobre 2016. See specifically Articles 17 to 24, according to which private undertakings that have been delegated to manage a public service (such as industrial, commercial, statistical, road utility or electricity and gas distribution and transport public services), have to share, with the delegating public authority, the data collected and processed in the context of the exploitation of this public service that are essential for its execution.
[2408] European Commission, "Consultation on PSI Directive review – Synopsis report", *op. cit.*, p. 8.
[2409] *Ibidem*.
[2410] See https://ec.europa.eu/digital-single-market/en/news/commission-appoints-expert-group-business-government-data-sharing.

preferential conditions for re-use, which were contained in the European Commission's Communication "Towards a common European data space".[2411]

391. On the basis of these discussions, this High-Level Expert Group suggested a series of principles for "scalable, responsible and sustainable B2G data sharing for the public interest".[2412] Some of these principles, pertaining to *voluntary* B2G data sharing[2413], can be of value in the context of this thesis, as they address the need to find a balance with the data holder's business interests on the one hand, and the need to comply with the right to privacy and to personal data protection of the multiple individuals whose data would be shared, on the other hand. These selected principles are the following:

- Proportionality: "Requests for the supply and use of private-sector data should be justified by clear and demonstrable public interest. The potential benefits of the public interest pursued should be reasonably balanced against the interests of other stakeholders. The requested private-sector data should be necessary, relevant and proportionate in terms of detail (e.g. type of data, granularity, quantity, frequency of access) with regard to the intended public interest pursued. The cost and effort required for the supply and use of private sector data should be reasonable and proportionate to the public-interest benefits pursued";[2414]

- Data-use limitation: "The business-to-government collaboration agreement or the decision that requires data sharing should clearly specify the intended public-interest purpose or purposes. (…) The data obtained may be further used only for compatible purposes to the extent necessary and proportionate. (…) The public sector should be able to combine the private-sector data with other data sources";[2415]

- Risk mitigation and safeguards: "The risks, including damage due to the request for and use of private-sector data, should be taken into account and mitigated. Business-to-government data collaborations must ensure that legitimate private-sector interests, notably commercially sensitive information such as trade secrets, are respected.[2416] (…) Business-to-government data-collaboration agreements or decisions should contain appropriate safeguards as regards the use of private-sector data in order to

---

[2411] Communication from the Commission, "*Towards a common European data space*", *op.cit.*, p. 13-14. See also Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication "*Towards a common European data space*", Brussels, 25 April 2018, SWD(2018) 125 final.

[2412] High-Level Expert Group on Business-to-Government Data Sharing, "Towards a European strategy on business-to-government data sharing for public interests – Final report", 2020, available at https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more, p. 7.

[2413] For an analysis of the benefits, risks and limits of compulsory B2G sharing/access rules, see H. Richter, "The Law and Policy of Government Access to Private Sector Data ('B2G Data Sharing')", *Max Planck Institute for Innovation and Competition Research Paper No. 20-06*, 2020, available at: https://ssrn.com/abstract=3594109.

[2414] High-Level Expert Group on Business-to-Government Data Sharing, "Towards a European strategy on business-to-government data sharing for public interests – Final report", *op. cit.*, p. 80.

[2415] *Ibid*., p. 81.

[2416] In essence, this would mean that such commercially sensitive information should only be shared with a public authority if the latter is subject to a confidentiality obligation preventing it from disclosing the information at hand to third parties.

protect the rights (e.g. privacy, data security, non-discrimination) of stakeholders, in particular the individuals whose data is used";[2417]

- Compensation: the level of compensation should be determined on the basis of the other principles, in particular the principles of proportionality and of risk mitigation and safeguards.[2418]

392. This thesis argues that such principles could be imported in the realm of compulsory B2B data sharing. In this regard, the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes could provide that only the recipients that can demonstrate clear economic benefits to be gained from the sharing can access the data.[2419] To do so, the recipient would have to specify its intended economic initial purpose(s), and would only be allowed to further re-use the data for compatible purposes to the extent necessary and proportionate, in full compliance with the GDPR where applicable.[2420] However, the recipient should not be prevented from combining the data with other data sources in order to achieve its initial purpose(s).[2421]

It could also be provided that, in conducting this assessment, these benefits will need to be reasonably balanced with the interests of the data holder and of the potential individuals whose data would be shared, and more specifically with the costs in terms of business interests, privacy and security that such sharing would entail. To limit these costs, the data sharing could be organised "in testing environments ('sandboxes') for pilot testing ('pilots') to help assess the potential value of data for new situations in which a product or service could potentially be used ('use cases')".[2422] Moreover, the use of privacy-preserving technologies could be considered.[2423] As a consequence, such sharing should only be mandated if these costs are reasonable and proportionate to the economic objectives pursued, and only the data that are necessary, proportionate and relevant for these objectives, should be shared.[2424] To mitigate these costs, the data holder could receive a compensation for this sharing, which should be proportionate in order to strike a fair balance between the business interests of the data holder and the economic purposes of the recipients.[2425]

393. Finally, it should be mentioned that discussions pertaining to the need for improved B2G data sharing have reappeared in the European Commission's inception impact assessment on its future "Data Act", where it indicated that "a more flexible framework for access and use of [private] data sources, including data-sharing requirements, transparency requirements and safeguards, could be designed. (…) In a high intensity option, legislation would lay down a

---

[2417] *Ibid*., p. 82.
[2418] *Ibid*., p. 83.
[2419] See Part III, Chapter 3, Section B, b), 2.
[2420] See Article 6.4 of the GDPR.
[2421] See Part III, Chapter 3, Section B, b), 3.
[2422] High-Level Expert Group on Business-to-Government Data Sharing, "Towards a European strategy on business-to-government data sharing for public interests – Final report", *op. cit.*, p. 7.
[2423] *Ibid*., p. 9.
[2424] See Part III, Chapter 3, Section B, b), 3.
[2425] See Part III, Chapter 3, Section B, b), 4.

right of public sector to access privately-held data for a range of defined public interest purposes".[2426]

b) Factoring these balancing exercises in the provisions to be included in horizontal *ex ante* legislations imposing B2B data sharing for economic purposes

394. As outlined above[2427], if "specific circumstances" justify the adoption of horizontal *ex ante* legislations imposing B2B data sharing for economic purposes, the provisions of such legislations will nevertheless need to find a balance between the economic benefits of the sharing and the costs on the data holder's business interests, and they will need to comply with the individuals' right to privacy and to personal data protection. This will require tackling fundamental questions such as: Who will have to share data and who can receive the data? To which types of data would this apply? Should this be remunerated? How could this be implemented technically? How will these legislations be enforced?

When answering these questions, some guidance could be sought in the principles for G2B and B2G data sharing identified above.[2428] Moreover, it should be outlined that there is no "one size fits all" answer to these questions. Instead, the balancing exercises underlying each of these questions should be factored, on a case-by-case basis, when creating a specific horizontal *ex ante* legislation.[2429]

1. Who will have to share data?

395. First, the data holders that will be subject to the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes have to be identified. Indeed, as such compulsory sharing will entail costs for these data holders, it is fundamental to ensure that it will only apply to the data holders whose data is considered as necessary to achieve the economic objectives underlying the legislation.

396. If the "specific circumstances" justifying the adoption of these legislations are economic – namely that (systemic) market failures (data concentration, data conglomeration, etc.)[2430] are identified or can be foreseen, and cannot be (efficiently) remedied by competition law intervention alone[2431]–, legal scholars seem to agree on the fact that the data sharing obligation should only be imposed to a specific sub-set of data holders.[2432] In this regard, it is

---

[2426] European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 5.
[2427] See point 382.
[2428] See points 387, 388 and 392.
[2429] On this point, see W. Kerber, "From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *Joint Discussion Paper Series in Economics No. 40-2020*, 26 August 2020, available at https://ssrn.com/abstract=3681263.
[2430] See Part I, Chapter 2, Section B, c), 3. "Data market failures".
[2431] See Part III, Chapter 1, Section E, b) "Competition law may not be sufficient on itself: growing call for *ex ante* legislations imposing data sharing"; Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 13, footnote 39.
[2432] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability: Towards a Governance Framework*"*, *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/, p. 56-68; A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", CERRE Recommendations Paper,

worth reminding[2433] that the European Commission has proposed the adoption of a "Digital Markets Act"[2434], which should empower the European Commission to determine whether a specific data holder meets the "gatekeeper" threshold[2435], in which case it will have to ensure some forms of data sharing.[2436] In the same vein, the Furman report outlines that, in order to spur competition and innovation, *ex ante* data sharing obligations, to be monitored by a "Digital Markets Unit", should be imposed on undertakings having a "strategic market status"[2437].[2438] Similarly, the Stigler Committee report provides that *ex ante* data sharing obligations, to be monitored by a "Digital Authority", could be imposed on undertakings having "bottleneck power"[2439].[2440]

One of the key common points between these propositions is that they are limited to a specific sub-set of data holders meeting a certain threshold ("gatekeepers"; undertakings with

---

November 2020, available at https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.*, p. 49; J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel, p. 55; S. Vezzoso, "Competition Policy in Transition: Exploring Data Portability's Roles", *15th ASCOLA (Virtual) Conference*, June 2020, available at https://ssrn.com/abstract=3634736, p. 20; Stigler Committee on Digital Platforms, "Final Report", September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report, p. 32; Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf, p. 5 and 13; V. Mayer-Schonberger and T. Ramge, *Re-inventing capitalism in the age of big data*, New York, Basic Books, 2018, p. 167-169; Unofficial translation of the Draft Bill for the Reform of the German Competition Act, 24 January 2020, available at https://www.d-kart.de/wp-content/uploads/2020/02/GWB10-Engl-Translation-2020-02-21.pdf, p. 3; European Commission, Inception Impact Assessment: "*Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market*", June 2020, Ares(2020)2836174, p. 3-4; European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 25 and 36.

[2433] See point 382.

[2434] Proposal for a Digital Markets Act.

[2435] See Articles 2.1 and 3 of the Proposal for a Digital Markets Act. For more details on the determination of this threshold, see points 397 and 398.

[2436] For instance, according to Article 6.1.j) of the Proposal for a Digital Markets Act, a gatekeeper shall "provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data". See also Article 6.1.h), presented at point 169, and Article 6.1.i), presented at point 182. See also Recitals 54 to 56.

[2437] Undertakings that are "in a position to exercise market power over a gateway or bottleneck in a digital market, where they control others' market access" (J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit.*, p. 55).

[2438] *Ibidem*. See also Competition and Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, p. 322-323.

[2439] Bottleneck power "describes a situation where consumers primarily single-home and rely upon a single service provider, which makes obtaining access to those consumers for the relevant activity by other service providers prohibitively costly" (Stigler Committee on Digital Platforms, "Final Report*", op. cit.*, p. 32).

[2440] *Ibid.*, p. 100-101.

"strategic market status"; undertakings having "bottleneck power"; undertakings of "paramount significance"[2441]; "unavoidable trading partners"[2442]; "structuring undertakings"[2443]; "large gatekeeper platforms"[2444]; etc.[2445]). As outlined by the European Parliament in its resolution pertaining to the Commission's Digital Services Act Package, such regulatory interventions must contain a set of clear indicators allowing the European Commission to decide whether a large data holder must be considered as a "gatekeeper" or not, such as "whether the undertaking is active to a significant extent on multi-sided markets or has the ability to lock-in users and consumers, the size of its network (number of users), and the presence of network effects; barriers to entry, its financial strength, the ability to access data, the accumulation and the combination of data from different sources; vertical integration and its role as an unavoidable partner and the importance of its activity for third parties' access to supply and markets, etc".[2446] Importantly, this would thus imply that the scope of application of the horizontal *ex ante* legislations should be broad enough in order to cover all types of data holders[2447] that may be considered as such "gatekeepers", even if the concrete obligations contained in the legislations would only have to be respected by those that the European Commission deems to be "gatekeepers", in light of the indicators contained in the legislations.[2448]

397. Regarding the indicators to be used by the European Commission, the proposal for a Digital Markets Act provides that a large data holder offering a "core platform service" will meet the "gatekeeper" threshold if: "(a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future".[2449] These criteria are thus

---

[2441] See the unofficial translation of the Draft Bill for the Reform of the German Competition Act, 24 January 2020, available at https://www.d-kart.de/wp-content/uploads/2020/02/GWB10-Engl-Translation-2020-02-21.pdf, p. 3.

[2442] J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era*", op. cit.,* p. 49.

[2443] Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques", *op. cit.*, p. 5 and 13.

[2444] A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *op. cit.*, p. 4.

[2445] In the same perspective, see the suggestion to create a "progressive data sharing obligation", which would kick in once the market share of a data holder has reached a certain threshold, and according to which the amount of data to be shared by a specific data holder should be function of its market share (V. Mayer-Schonberger and T. Ramge, *Re-inventing capitalism in the age of big data*, *op. cit*., p. 167-169).

[2446] European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 25 and 36. On these indicators, see also European Commission, Inception Impact Assessment: "*Digital Services Act package*", *op. cit.*, p. 2; and A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *op. cit.*, p. 11-12.

[2447] Contrary, for example, to the Platform-to-Business Regulation that only applies to certain types of online intermediation services and to online search engines (Articles 2.2 and 2.5 of the Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019). On this Regulation, see points 180 to 182.

[2448] A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *op. cit.*, p. 10.

[2449] Article 3.1 of the Proposal for a Digital Markets Act. On the different policy options that were considered, see Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for*

cumulative, and three quantitative "presumption thresholds" have been set in order to streamline the assessment of the existence of a "gatekeeper" position.[2450]

First, the significant impact on the internal market will be presumed if the large data holder "achieves an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, or where the average market capitalisation or the equivalent fair market value of the undertaking to which it belongs amounted to at least EUR 65 billion in the last financial year, and it provides a core platform service in at least three Member States".[2451] Second, the fact that the large data holder operates an important gateway for business users to reach end users will be presumed if it provides a core platform service[2452] that "has more than 45 million monthly active end users[2453] established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year".[2454] Third, the large data holder will be presumed to have an entrenched and durable position if the "users threshold" mentioned above were met in each of the last three financial years.[2455]

---

a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)", Brussels, 15 December 2020, SWD(2020) 363 final, p. 46-50, 64-78, 82, 85 and 96-120.

[2450] Article 3.2 of the Proposal for a Digital Markets Act. According to some authors, a fourth "ecosystem criterion" could have been added as well, relating to the fact that the large data holder provides several digital services within its ecosystem (A. de Streel, B. Liebhaberg, A. Fletcher, R. Feasey, J. Krämer and G. Monti, "The European Proposal for a Digital Markets Act: A First Assessment", *CERRE Assessment Paper*, January 2021, available at https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/, p. 6 and 15).

[2451] Article 3.2.a) of the Proposal for a Digital Markets Act. It should be noted that, in order to focus the scope of the Digital Markets Act on a smaller number of undertakings, namely those that play "an unquestionable role as gatekeepers due to their size and their impact on the internal market", the European Parliament's "Draft report" on this Act suggests to raise these thresholds to EUR 10 billion and EUR 100 billion respectively (see Committee on the Internal Market and Consumer Protection of the European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)), 1 June 2021, 2020/0374(COD), available at https://www.europarl.europa.eu/doceo/document/IMCO-PR-692792_EN.pdf, p. 32 and 79).

[2452] It is worth highlighting that the European Parliament's "Draft report" on this Act suggests adding another requirement, namely that the gatekeeper must provide at least two core platform services – each of which having more than 45 million monthly active end users established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year –, in order to take into account the role of "ecosystems of services" more explicitly (Committee on the Internal Market and Consumer Protection of the European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector, *op. cit.*, p. 33 and 79). This echoes a similar call made by some authors and policy makers (see French Ministry of the Economy, Finance and the Recovery, German Federal Ministry for Economic Affairs and Energy and Dutch Ministry of Economic Affairs and Climate Policy, "Strengthening the Digital Markets Act and Its Enforcement", May 2021, available at https://www.economie.gouv.fr/files/2021-05/1055%20-%20Strengthening%20the%20Digital%20Markets%20Act%20and%20Its%20Enforcement.pdf, p. 1; A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *op. cit.*, p. 12).

[2453] "Monthly active end users shall refer to the average number of monthly active end users throughout the largest part of the last financial year" (Article 3.2.b), al.2 of the Proposal for a Digital Markets Act).

[2454] Article 3.2.b), al.1 of the Proposal for a Digital Markets Act. The European Parliament's "Draft report" on this Act suggests to add an Annex containing a list of indicators pertaining to the establishment of the number of monthly active end-users and yearly active business users (Committee on the Internal Market and Consumer Protection of the European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector, *op. cit.*, p. 71-77 and 79).

[2455] Article 3.2.c) of the Proposal for a Digital Markets Act.

Importantly, the European Commission would be empowered to adopt delegated acts to specify the methodology used for assessing whether these three quantitative "presumption thresholds" are met, as well as to adjust them to market and technological developments where necessary.[2456] Such a delegated act, which could take the form of guidelines, would have the merit to enhance legal certainty and predictability on this new issue of "gatekeeper" identification[2457].

If a large data holder meets all of these three quantitative "presumption thresholds", it will have to notify the European Commission thereof[2458], as the latter is in charge of designating those that meet the "gatekeeper" threshold.[2459] However, in its notification, the large data holder can attempt to rebut this "gatekeeper" presumption (i.e. that it does not meet the "gatekeeper" threshold of Article 3.1 even if it meets the three quantitative "presumption thresholds" of Article 3.2) by presenting sufficiently substantiated arguments relying on qualitative indicators such as low entry barriers or the lack of user lock-in due to multi-homing possibilities.[2460] If the large data holder presents sufficiently substantiated arguments to rebut this "gatekeeper" presumption, the European Commission shall rely instead on qualitative indicators to demonstrate that the large data holder meets the "gatekeeper" threshold of Article 3.1.[2461] These are: "(a) the size, including turnover and market capitalisation, operations and position of the provider of core platform services; (b) the number of business users depending on the core platform service to reach end users and the number of end users; (c) entry barriers derived from network effects and data driven advantages, in particular in relation to the provider's access to and collection of personal and non-personal data or analytics capabilities; (d) scale and scope effects the provider benefits from, including with regard to data; (e) business user or end user lock-in; (f) other structural market characteristics".[2462]

Moreover, the European Commission can also decide, on the basis of a market investigation procedure mentioned above[2463], that a large data holder meets the "gatekeeper" threshold even if it does not satisfy each of the three quantitative "presumption thresholds".[2464] In doing so, it should consider the qualitative indicators mentioned above. In conducting this assessment, the Commission should consider foreseeable developments of these elements.[2465]

Finally, as data markets are dynamic and evolutive, the European Commission will have to regularly review, at least every 2 years, whether the "gatekeepers" that it has listed still meet the threshold mentioned above, as well as whether new large data holders have come to meet

---

[2456] Articles 3.5 and 37 of the Proposal for a Digital Markets Act.
[2457] A. de Streel, B. Liebhaberg, A. Fletcher, R. Feasey, J. Krämer and G. Monti, "The European Proposal for a Digital Markets Act: A First Assessment", *op. cit.*, p. 6 and 15.
[2458] Article 3.3 of the Proposal for a Digital Markets Act.
[2459] Article 3.4, al. 1 of the Proposal for a Digital Markets Act.
[2460] Article 3.4, al. 1 of the Proposal for a Digital Markets Act.
[2461] Article 3.4, al. 2 of the Proposal for a Digital Markets Act.
[2462] Article 3.6, al.2 of the Proposal for a Digital Markets Act.
[2463] See point 319. See Article 15 of the Proposal for a Digital Markets Act.
[2464] Article 3.6, al.1 of the Proposal for a Digital Markets Act.
[2465] Article 3.6, al.3 of the Proposal for a Digital Markets Act.

it.[2466] In this regard, the Commission can, upon request or on its own initiative, adapt or repeal a decision following which a large data holder meets the "gatekeeper" threshold if "there has been a substantial change in any of the facts on which the decision was based;" or if "the decision was based on incomplete, incorrect or misleading information provided by the undertakings".[2467]

398. In light of the above, there thus seems to be a strong consensus that horizontal *ex ante* legislations imposing B2B data sharing, whose adoption is justified by economic "specific circumstances", should be asymmetric and limited to a specific sub-set of data holders. In this regard, the determination of whether a data holder falls within the scope of the data sharing obligation could be based on a set of clear quantitative and qualitative indicators contained in the legislations, to be assessed on a case-by-case basis by the controlling authority. Indeed, if other horizontal *ex ante* legislations were to be adopted, for example to impose additional data sharing obligations than those contained in the Digital Markets Act[2468], a semi-flexible approach could be taken, where quantitative indicators (e.g. annual turnover or number of customers) could serve as "rebuttable presumptions" that specific data holders fall within the scope of the initiative. These could be complemented by qualitative indicators (e.g. barriers to entry or user lock-in) that could be used to make other data holders fall within the scope of the initiative, in situations where the presumptions are rebutted or where the quantitative thresholds are not met. This would require a case-by-case analysis, based on the markets and context at hand, as the legislations should merely provide these indicators, while the concrete list of data holders falling within the scope of the initiative will, by nature, be evolutive and dynamic.[2469] Therefore, these indicators must be "sufficiently flexible to adapt to different business models as well as technology and market evolution which evolve rapidly and can be unpredictable in the digital economy (…) [and] should also be sufficiently clear and easy to implement to ensure legal predictability and not be subject to long and complex procedures".[2470] Moreover, the regulatory authority's decisions that certain data holders fall within the scope of the data sharing obligation would have to be re-assessed at regular intervals, in order to take into account the evolution of the market at hand, as the data holders might no longer fulfil these indicators, or as the market failures justifying the intervention might disappear over time.[2471]

[2466] Article 4.2 of the Proposal for a Digital Markets Act. For some authors, this two-years cycle is too short and should be extended to five years, in order to reduce the logistical and fact-finding pressure (A. de Streel, B. Liebhaberg, A. Fletcher, R. Feasey, J. Krämer and G. Monti, "The European Proposal for a Digital Markets Act: A First Assessment", *op. cit.*, p. 15).

[2467] Article 4.1 of the Proposal for a Digital Markets Act.

[2468] This Act indeed only contains a certain number of specific data sharing obligations, to the benefit of third party providers of online search engines (Article 6.1.j) – see point 382), of business users of these gatekeepers' services (Article 6.1.i) – see point 182), and to individuals (Article 6.1.h) – see point 169). However, data sharing obligations could also be created to the benefit of other actors, such as competitors of these gatekeepers or undertakings developing complementary services.

[2469] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 12 and 56-58.

[2470] A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *op. cit.*, p. 11.

[2471] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 83.

Such a limitation of the scope of application of the legislations is justified by the fact that the costs implied by the data sharing obligation on the data holder's business interests should only be imposed to a specific sub-set of data holders, namely those that are considered as playing a central role in the (systemic) market failure(s) that led to the legislative intervention.[2472] Indeed, as the aim of these interventions is to enhance competition by levelling the competitive playing field and by ensuring the contestability of data markets, it is preferable to opt for an asymmetric approach[2473], which would only burden this sub-set of data holders, and not other market actors. This is, according to this thesis, a key difference with empowerment initiatives imposing B2B data sharing.[2474]

2. Who can receive the data?

399. Second, the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes will have to determine whether any recipient whatsoever should be entitled to access the data holder's data, or whether only some of them should be entitled to such access. Indeed, an *erga omnes* entitlement to access the data would potentially maximise the economic benefits pursued by the legislations, in light of the non-rivalrous nature of data. On the other hand, the greater the number of potential recipients, the greater the risks for the data holder's business interests and for the privacy and personal data protection of the multiple individuals whose data would be shared in an aggregated way.[2475] Any horizontal compulsory B2B data sharing legislation would thus have to consider this necessary balance.

400. In this regard, some guidance could be sought in the principles for B2G data sharing outlined above.[2476] Accordingly, the legislations could provide that recipients would have to demonstrate that the purposes they would pursue thanks to the shared data would lead to clear economic benefits. Moreover, the legislations could provide that the sharing with a specific recipient should only be mandated if the costs for data holders and the potential individuals whose data would be shared are reasonable and proportionate to the economic objectives pursued.

In support of such an idea, Drexl argues that the horizontal B2B compulsory data sharing legislations could provide that only the recipients that pursue a legitimate economic interest should benefit from an access to the data.[2477] Naturally, the core issue here would be to determine what these legitimate interests are. Attempting to draft an extensive list of these interests in the legislations might not be the best solution, as it would risk not being exhaustive. Rather, the legislations could list several criteria to be considered in the determination of these legitimate interests (such as the demonstration of a clear economic benefit for society or of a significant contribution to research in a specific field, which would derive from the recipients processing of the data). Then, a specific regulatory body/authority

---

[2472] *Ibid*., p. 58.
[2473] See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf, p. 12.
[2474] See points 211 and 212.
[2475] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 9 and 60.
[2476] See point 392.
[2477] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 164.

could be appointed in order to assess, on a case-by-case basis, the legitimacy of the recipient's economic interests in light of these criteria, and to assess whether this recipient presents sufficient guarantees in terms of privacy and security, in order to protect the rights of the multiple individuals whose data would be transferred in an aggregated way.[2478] In this regard, the European Data Protection Supervisor (EDPS) underlined that some type of formal "vetting" of the data recipients might be warranted to address the risks mentioned above[2479], for example in the form of a Clearinghouse.[2480]

401. Accordingly, the inclusion of a certification/accreditation scheme for data recipients in these horizontal legislations might be justified, as this would generate more trust in the whole sharing process.[2481] In light of the analogous developments made above regarding the relevance to include such schemes in "empowerment" initiatives imposing data sharing[2482], which will not be repeated here, this thesis argues that in order to be entitled to receive the data, the data recipient could be required to notify a description of the specific economic purpose that it intends to pursue to competent authorities to be appointed in each Member State.[2483] These authorities, which could be the same as those created by the Data Governance Act in order to avoid a multiplication of regulatory bodies[2484], could then assess, *ex post*, the legitimacy of the recipients' economic interests and whether they offer sufficient guarantees in terms of privacy and security (in collaboration with the data protection authorities[2485]).[2486] Indeed, as outlined earlier in this thesis, while such a "notification obligation with *ex post* monitoring of the compliance" could be quite cumbersome, it is the most pragmatic solution.[2487]

402. Moreover, the horizontal legislations could impose harmonised obligations on the recipients, to be monitored *ex post* as well, in order to ensure their trustworthiness.[2488] Indeed, as outlined by Feasey and de Streel, such legislations should "devote as much attention to the oversight of those firms that obtain access to the data as to regulating the firms that are obliged to provide access".[2489] This is an advantage of *ex ante* regulatory initiatives over competition law intervention, as the latter is not really suited to impose obligations on the beneficiaries of the intervention.[2490] For instance, one of the guiding principles for B2G data sharing outlined above could be imported in this context[2491], and these legislations could provide that the recipients shall be prevented from re-using the data for other purposes than the economic purpose(s) that they have notified, except for compatible purposes to the extent

---

[2478] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 9.
[2479] See point 399.
[2480] European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, *op. cit*.., p. 13.
[2481] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 59-60.
[2482] See Part II, Chapter 2, Section C, c).
[2483] See, by analogy, Article 17.4.h) of the Proposal for a Data Governance Act.
[2484] See point 218.
[2485] See, by analogy, Recitals 28 and 29 and Article 12.3 of the Proposal for a Data Governance Act.
[2486] See, by analogy, Article 13 of the Proposal for a Data Governance Act. See also point 408.
[2487] See point 219.
[2488] See, by analogy, Recitals 22 to 34 and Articles 9 to 14 of the Proposal for a Data Governance Act.
[2489] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 60.
[2490] *Ibidem*.
[2491] See point 392.

necessary and proportionate[2492], in full compliance with the GDPR where applicable.[2493] The recipient should, however, not be prevented from combining the data with other data sources in order to achieve its initial purpose(s). Another example is that these legislations could provide that it is forbidden for data recipients to re-identify the individuals whose data have been aggregated and pseudonymised in order to enable the sharing.[2494] In case of a breach of an obligation imposed by the legislations, or if the data recipient has provided false information in its notification, the competent national authorities mentioned above could also be empowered to impose fines and/or to request the cessation of the unlawful processing.[2495]

3. To which types of data would this apply?

403. Third, the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes will have to determine the scope of the data to be covered by the sharing obligation. On the one hand, the greater the scope of the data covered, the greater the potential economic benefits for recipients and society. On the other hand, the greater the scope of the data covered, the greater the risks for the data holder's business interests, as data sharing entails (incentive) costs for the holder.[2496] Moreover, the greater the scope of the data covered, the greater the risks for the privacy and personal data protection of the multiple individuals whose data would be shared in an aggregated way. Any horizontal compulsory B2B data sharing legislation would thus have to consider these balancing exercises.

i. Balance with the data holder's business interests

404. If the "specific circumstances" justifying the adoption of these legislations are economic, the determination of the scope of the data to be covered by the legislations can arguably take inspiration from the determination of the scope of the data to be covered by compulsory B2B data sharing competition law remedies.[2497] Based on that reasoning, which will not be repeated here, the scope of *economic initiatives imposing B2B data sharing* should arguably also be limited to actively provided and observed data, excluding inferred/derived data.[2498] Indeed, by analogy with the guiding principles of G2B data sharing[2499], excluding inferred/derived data would amount to excluding the data holder's most commercially sensitive data, and this would address both the data holder's fear of free-riding and the data recipients' potential expectation to free-ride, which are factors that could deter innovation.[2500] Moreover, acquired data should also be excluded from the scope of such legislations, as otherwise this would impose disproportionate and unnecessary costs on the data holders, since this data can be obtained elsewhere through *voluntary* data sharing.[2501]

[2492] See, by analogy, Article 11.1 and 11.2 of the Proposal for a Data Governance Act.
[2493] See Article 6.4 of the GDPR.
[2494] See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 12.
[2495] See point 219. See, by analogy, Article 13.3 to 13.5 of the Proposal for a Data Governance Act.
[2496] See Part I, Chapter 2, Section B, c), 5.
[2497] See Part III, Chapter 1, Section D, b).
[2498] See points 302 to 306.
[2499] See point 387.
[2500] See point 89. R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 62; J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 11.
[2501] See point 301.

405. Furthermore, while the legislations should specify the types of data covered by their scope of application, this does not mean that all of the data holder's data potentially falling within this scope (e.g. all of the data holder's actively provided and observed data) will have to be shared. Rather, by analogy with the principles for B2G data sharing outlined above[2502], only the data that are necessary, relevant and proportionate for the economic objectives pursued by the legislations should be shared. This will have to be determined on a case-by-case basis. If there is a disagreement between the data holder and the data recipient in this regard, this could be settled by a regulatory authority.[2503]

Additionally, and similarly than for G2B data sharing[2504], these legislations could provide that the data holder is compelled to licence, under objective, proportionate and non-discriminatory conditions, any potential database right that it may have on the data.[2505] These legislations could also provide that the conditions of these licences should not restrict competition nor re-use possibilities, but that, in exchange, the data holder should be entitled to a remuneration.[2506]

Finally, in order to be truly efficient and sustainable, the legislations should not only cover the data holder's historical data, but also present and future data.[2507] Indeed, to reach the economic objectives pursued, the imposition of static data sharing might not be sufficient, and dynamic data sharing might be necessary. However, as this would entail more implementation costs for the data holders, such a dynamic real-time data sharing should only be imposed when its benefits trump its costs. Moreover, once again by analogy with G2B data sharing[2508], these legislations could provide that the data holder should not be bound to create, collect or adapt data merely to enable the re-use by data recipients, if this would involve disproportionate efforts. The legislations could also provide that the data holder would not be obliged to further collect and process data that it no longer needs, simply because a recipient relies on it for its activities. In the latter case, these legislations could nevertheless require that the data holder should make such decisions publicly known in a timely fashion.

ii. Compliance with the privacy and personal data protection of the multiple individuals whose data would be shared in an aggregated way

406. Horizontal *ex ante* legislations imposing B2B compulsory data sharing will also have to take the rules of personal data protection into account. Indeed, even if this thesis suggests to follow a common holistic approach for both personal and non-personal data in order to determine the categories of data that should be covered by these legislations[2509], it is

---

[2502] See point 392.
[2503] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 70.
[2504] See point 387.
[2505] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 164.
[2506] On this remuneration, see Part III, Chapter 3, Section B, b), 4.
[2507] Stigler Committee on Digital Platforms, "Final Report*", op. cit*., p. 117.
[2508] See point 387.
[2509] For a call to follow such a holistic approach see I. Graef, R. Gellert and M. Husovec, "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is

nevertheless of paramount importance to take personal data protection considerations into account when relevant.[2510] Yet, as the legislations will likely cover personal data pertaining to multiple individuals, some tensions might emerge with personal data protection law. Accordingly, and as in G2B data sharing legislations[2511], B2B legislations should make it explicit that they shall not affect the individuals' protection of their personal data.[2512]

407. To bypass the application of the GDPR, the aggregated personal data pertaining to multiple individuals could be anonymised (e.g. with a sufficient level of granularity) before sharing it. To encourage such anonymisation, the horizontal data sharing legislations could even provide that if the data holder anonymises the personal data before sharing it, it could charge the marginal costs incurred for the anonymisation to the recipients.[2513] However, as outlined above, what is presented as anonymisation will, in fact be mere pseudonymisation, and the rules of the GDPR will thus have to be applied.[2514]

Accordingly, these legislations should provide that aggregated personal data pertaining to multiple individuals should only be shared to the extent that this complies with the GDPR's principles (lawfulness, fairness and transparency; purpose limitation[2515]; data minimisation; data accuracy; storage limitation; integrity and confidentiality; and accountability)[2516] and that there are lawful basis of processing allowing the sharing.[2517]

408. As far as the data holder is concerned, it should, in principle, be able to argue that the transfer is necessary for the compliance with a legal obligation to which it is subject (i.e. the data sharing obligation contained in the horizontal legislation).[2518] However, Recital 41 of the GDPR provides that this legal obligation must be clear, precise, predictable and accessible.[2519] Therefore, the horizontal legislation imposing the data sharing will have to meet an objective of public interest (*in casu* the economic objective) and be proportionate to the legitimate aim pursued, and it will have to specify the purposes and the recipients of the sharing, as well as the types of data and the data subjects concerned by the data sharing.[2520]

Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, September 2018, available at http://ssrn.com/abstract=3256189, p. 14-18.

[2510] See, for example, Part III, Chapter 2. "Articulation between data protection and competition law".

[2511] See point 388.

[2512] For a "Code of practice" on *voluntary* data sharing, which aims at serving as a guide for businesses wishing to share personal data in a privacy-compliant way, see Information Commissioner's Office, "Data sharing code of practice", 17 December 2020, available at https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/.

[2513] See point 388.

[2514] See point 353.

[2515] See, for instance, Recitals 54 and 55 and Article 6.1.i) of the Proposal for a Digital Markets Act.

[2516] Articles 5 of the GDPR. For a more detailed analysis of this articulation, see, by analogy, Part III, Chapter 2, Section B, b).

[2517] Articles 6 of the GDPR. For a more detailed analysis of this articulation, see, by analogy, Part III, Chapter 2, Section B, a).

[2518] Article 6.1.c) of the GDPR.

[2519] See also R. Ergec, *Protection européenne et internationale des droits de l'homme*, Bruxelles, Larcier, 2014, p. 232.

[2520] See point 358.

Data recipients, on the other hand, could attempt to rely on the explicit freely given, specific, informed and unambiguous consent of the multiple individuals whose data is shared[2521], or could attempt to argue that the re-use is necessary for the purposes of their "legitimate interests", and that these economic interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.[2522] In fact, such a demonstration could be requested in the context of the notification obligation mentioned above.[2523] One way for the recipient to demonstrate that the balance tips in its favour would be to show that it relies on the use of privacy-enhancing technologies in order to limit the risks for the data subjects.[2524] Indeed, if, for instance, the aggregated personal data pertaining to multiple individuals that it receives is pseudonymised, this reduces the risks that the re-use could entail for the data subjects. In fact, this could be combined with a limitation of the risks embedded in the horizontal legislations, if the latter contained a provision forbidding data recipients from re-identifying the multiple individuals whose data have been aggregated and pseudonymised prior to the sharing.[2525]

4. Should this be remunerated?

409. Horizontal *ex ante* legislations imposing B2B data sharing could arguably provide for a remuneration in exchange for the sharing, as this would be a way to protect the data holders' business interests, in return for the expected benefits of these legislations.[2526] This would indeed compensate the data collection costs incurred by the data holder, and would preserve its data collection incentives, as well as those of the recipients.[2527]

As the value of data is difficult to assess, it is advisable for the legislations not to impose a specific price for the sharing, but rather to set a sufficiently precise criteria to determine this price.[2528] One possibility would be to take inspiration from the PSI Directive, as these legislations could provide that the price should cover the costs of data collection, production, reproduction, dissemination and storage incurred by the data holder, as well as a reasonable return on investment for the holder.[2529] While this price calculation method presents the advantage of being relatively simple, it might however not reflect appropriately the value of the data and the incentive costs of the sharing for the holder. Indeed, data will not necessarily be valuable for a data holder because it was expensive to collect or produce, but rather because it is one of the few actors that has collected it (e.g. it is not, as such, expensive for Google to collect search data, but rather the value of search data for Google derives from the fact that most of the users use its search engine, and it is thus able to draw data advantages

---

[2521] Article 6.1.a) of the GDPR. See Part III, Chapter 2, Section B, a), 2, i., for more information on the limits of resorting to this lawful basis.
[2522] Article 6.1.f) of the GDPR. See Part III, Chapter 2, Section B, a), 2, ii., for more information on the possibility, for a recipient, to rely on this lawful basis.
[2523] See point 401.
[2524] See Recital 6 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit*., p. 13.
[2525] See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 12.
[2526] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 11 and 77-80. Some however argue that the data holders should not be entitled to a remuneration: see J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 14.
[2527] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 11 and 77-80.
[2528] *Ibid*., p. 38.
[2529] See, by analogy, Article 6.1 of the Directive 2019/1024.

from this).[2530] This loss of "data power" is important to factor in the sharing price in B2B scenarios, while it is less of a concern in G2B scenarios, where the objective is precisely to break the monopoly that public authorities might have on some data, which are seen as highly valuable resources.[2531] Accordingly, it might not be advisable to import this price calculation method from G2B data sharing to B2B data sharing.

410. Alternatively, the horizontal legislations could provide that this remuneration should be proportionate.[2532] This would imply that the price of sharing should be lower in cases where the incentives costs of sharing are low and where the potential benefits of sharing are high; and that this price should be higher in cases where the incentives costs of sharing are high and where the potential benefits of sharing are low.[2533] Determining such a proportionate remuneration would thus, once again, require a case-by-case analysis. To guide and facilitate this case-by-case assessment of the "proportionality" of the remuneration, the legislations could outline several factors to be taken into consideration. For instance, the remuneration could be function of the volume of data being shared.[2534] Moreover, and to the extent that this would be possible in practice[2535], the price for data generated as a by-product should, arguably, be lower than the price for data generated as the core economic activity of the data holder.[2536] Similarly, the price could be higher if (some of) the shared data is covered by an IP right (for example by a *sui generis* database right).[2537] Furthermore, the price could be higher if the data is shared with a direct competitor, than if the data is shared with a data recipient offering complementary products or services.

411. However, relying on an open formula such as "proportionate remuneration", even if the legislations outline several factors to be taken into consideration, might lead to uncertainties in the determination of the concrete remuneration, as illustrated by the numerous discussions around the notion of FRAND licensing fees for SEPs[2538].[2539] Nevertheless, several authors have suggested that the negotiation framework created by the European Court of Justice in its *Huawei*[2540] judgment could provide inspiration and could assist the parties to reach an

---

[2530] See Part I, Chapter 2, Section B, c).
[2531] See Recitals, 3, 7, and 11 of the Directive 2019/1024.
[2532] See, by analogy, the principles for B2G data sharing outlined above at point 392.
[2533] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 77-80.
[2534] *Ibid*., p. 11.
[2535] See point 305.
[2536] See point 304.
[2537] On this right, see points 58 to 60.
[2538] See, for instance, D. Geradin, A. Layne-Farrar and N. Petit, *EU Competition Law and Economics*, Oxford, Oxford University Press, 2012, p. 457; D. Geradin, "Ten Years of DG Competition Effort to Provide Guidance on the Application of Competition Rules to the Licensing of Standard-Essential Patents: Where Do We Stand?", 21 January 2013, available at https://ssrn.com/abstract=2204359, p. 7-8; C. Graham and J. Morton, "Latest Developments in Standards, Patents and FRAND licensing", *E.I.P.R.*, 2014, Vol. 36, Issue 11, p. 700-706; R. Stern, "What are Reasonable and Non-discriminatory Terms for licensing a Standard-essential Patent?", *E.I.P.R.*, 2015, Vol. 37, Issue 9, p. 549-557; J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975, p. 55; ECJ, *Huawei*, 16 July 2015, C-170/13, EU:C:2015:477.
[2539] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 80.
[2540] ECJ, *Huawei*, 16 July 2015, C-170/13, EU:C:2015:477, §§ 60-69.

agreement on the data sharing price.[2541] If no agreement is reached between the parties on the determination of this "proportional remuneration", the price could be determined by an independent third party. By analogy with what has been outlined above regarding the remuneration of the data holder in the context of a competition data sharing remedy[2542], this thesis argues that this could be done by the national authorities whose appointment is suggested in the European Commission's proposal for a Data Governance Act[2543], with the assistance of the Support Centre for Data Sharing and of the future European Data Innovation Board.[2544]

While this might be perceived by data holders as being a significant intervention by third parties / regulatory authorities in their business activities, this is probably the most pragmatic solution that can be designed. Indeed, while it would be much simpler to set a price in advance in the legislation, this does not appear to be realistic nor appropriate in B2B scenarios.[2545] On the other hand, the alternative of not providing for any remuneration at all is even more undesirable for the interests of the data holders. Moreover, it must be reminded that these economic initiatives imposing B2B data sharing should only be warranted when specific circumstances dictate it. Hence, if the legislator decides to intervene, this means that it has identified a (significant) problem that must be solved, which explains while some constraints could justifiably be imposed on a specific sub-set of data holders, namely those that are considered as playing a central role in the (systemic) market failure(s) that provoked the regulatory intervention.[2546]

To be sure, relying on an open formula such as "proportionate remuneration" and on the above-mentioned negotiation framework would generate a certain amount of red-tape that could delay and complicate the implementation of the data sharing initiative. Indeed, if long negotiations are necessary in order to agree on the determination of what constitutes a "proportionate" price for the data sharing, the implementation of the data sharing initiative might not be as timely as originally desired. To mitigate this risk, the initiative could set binding deadlines for this negotiation period. In this regard, the initiative could, for instance, provide that the data holders and the data recipients have one month to agree on a "proportionate" price, and that if they do not manage to come to an agreement within that period, the parties will have to refer the issue to the designated independent third party, which will itself then have one month to determine the price of the sharing. Moreover, the initiative could provide that the designated independent third party will have to draft guidelines, at regular intervals, aiming at providing more contextual information about the above-mentioned factors that have to be taken into consideration on a case-by-case basis to determine this

---

[2541] See point 308. J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access*", op. cit.*, p. 55. See also H. Richter and P. Slowinski, "The Data Sharing Economy: On the Emergence of New Intermediaries", *IIC*, 2019, Volume 50, Issue 1, p. 4-29.
[2542] See point 309.
[2543] See Recitals 22 to 34 and Articles 13 and 23 to 25 of the Proposal for a Data Governance Act.
[2544] See Recitals 40 and 41 and Articles 26 and 27 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit.*, p. 54.
[2545] See point 409.
[2546] See Part III, Chapter 3, Section B, b), 1.

"proportionate" remuneration (volume of data shared; by-product or not; covered by an IP right or not; sharing with a direct competitor or not).[2547] These guidelines could also suggest the addition of new factors that would be worth taking into consideration. This could then assist future negotiations between data holders and data recipients, especially if these guidelines are illustrated with relevant examples and success cases.

412. Finally, remunerating the data holder could also contribute to the personal data protection of the multiple individuals whose data would be shared. Indeed, as outlined for G2B data sharing, the horizontal *ex ante* legislations could provide that the data holder can charge the marginal costs incurred for the anonymisation of the aggregated data (e.g. the costs incurred in order to reach a sufficient level of granularity) to the data recipients.[2548] This would incentivise the data holders to resort to such anonymisation techniques prior to the sharing, and would thus reduce the risks for the multiple individuals whose data would be shared.[2549]

5. How could this be implemented technically?

413. Another important issue to consider for the horizontal *ex ante* legislations imposing B2B data sharing for economic purposes, is to determine how the data sharing should be implemented technically. Indeed, there are various technical ways in which such sharing could take place[2550], and they each entail their own benefits and costs. As this thesis focusses on legal considerations rather than on technical considerations, it will not delve extensively on this point. Rather, the objective of this sub-section is to point out that determining the appropriate technical approach will require a balancing exercise.

414. An important number of scientific contributions make the argument that, in order for the horizontal *ex ante* legislations imposing B2B data sharing to be truly efficient, they should require the data holders to share their data in (near) real-time and on a constant basis via application programming interfaces ("APIs")[2551], and to ensure the interoperability of their data formats.[2552] Indeed, in certain situations, it might be necessary to consider the imposition

---

[2547] See point 410.
[2548] See point 353.
[2549] See point 388.
[2550] See for instance the various conceptual models of data sharing presented in Part I, Chapter 3, Section A.
[2551] "An application programming interface (API) is an interface or communication protocol between a client and a server intended to simplify the building of client-side software. It has been described as a "contract" between the client and the server, such that if the client makes a request in a specific format, it will always get a response in a specific format or initiate a defined action" (https://en.wikipedia.org/wiki/Application_programming_interface).
[2552] See, for instance, J. Furman, D. Coyle, A. Fletcher, P. Marsden and D. McAuley, "Unlocking digital competition", *op. cit.*, p. 71-74; Stigler Committee on Digital Platforms, "Final Report", *op. cit.*, p. 113 and 117-118; S. Ennis and A. Fletcher, "Developing international perspectives on digital competition policy", 31 March 2020, available at https://ssrn.com/abstract=3565491, p. 7; J. Hoffmann and G. Johannsen, "EU-Merger Control & Big Data: On Data-specific Theories of Harm and Remedies", *Max Planck Institute for Innovation and Competition Research Paper No. 19-05*, 31 May 2019, available at https://ssrn.com/abstract=3364792, p. 64; J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 1; J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", *op. cit.*, p. 71; European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 20 and 36; W. Kerber, "From

of dynamic data sharing obligations in order to reach the economic objectives of the horizontal legislations.

This would however require the adoption of common technical standards for APIs and data interoperability, and would thus entail higher implementation costs for the data holders.[2553] This could have a substantial impact on their business interests. To limit this impact, large data holders could be tempted to influence the standard-setting process with the objective that their own proprietary standard be chosen as the common technical standard.[2554] This, in turn, could entail high costs for the data recipients and could affect their ability to develop their own products/services. As a result, the economic objectives of the horizontal legislations might not be achieved. Accordingly, in order to ensure that the interests of all of the parties are fairly balanced and taken into consideration in the determination of these standards, while ensuring that the process remains manageable, an appropriate representation of all the different interests should be ensured in the standardisation process.[2555]

Yet, the above would entail substantial costs in terms of resources and time for both the data holders and the data recipients. It is thus important to keep in mind that standardisation and interoperability will not always necessarily entail a positive effect on competition and innovation.[2556] Moreover, the direct continuous and interoperable sharing between data holders and data recipients could increase the risks for the individuals' personal data protection, as well as security risks.[2557] Therefore, the European legislator should carefully consider these costs when pondering whether horizontal legislations imposing B2B data sharing should require the adoption of common technical standards for APIs and data interoperability, and should arguably only impose it when the expected economic benefits trump these important costs.

415. It should also be outlined that this technical approach of the direct sharing of the data between the data holders and the recipients, via APIs and common technical standards, is criticised due to its impracticability, as it would require hundreds of holder-recipient relations.[2558] Moreover, the volume of data directly received by the recipients could be overwhelming and many of the (smaller) recipients could have difficulties to store and process such data.[2559] Therefore, Prüfer suggests to rely on trustworthy data intermediaries[2560] (data trustees) rather than on direct sharing between the holders and the recipients.[2561] In this technical approach, the data holder's data would be shared with an intermediary instead of

---

(Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *Joint Discussion Paper Series in Economics No. 40-2020*, 26 August 2020, available at https://ssrn.com/abstract=3681263, p. 28-29.

[2553] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 9 and 71.

[2554] *Ibid*., p. 72.

[2555] *Ibidem*.

[2556] W. Kerber, "From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *op. cit.*, p. 29.

[2557] *Ibid*., p. 29-31.

[2558] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 15.

[2559] R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 69.

[2560] It is interesting to point out that the European Commission's proposal for a Data Governance Act addresses the activities of such "trusted data intermediaries" in the context of *voluntary* B2B data sharing (see Recitals 22 to 34 and Articles 9 to 14 of the Proposal for a Data Governance Act).

[2561] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 12 and 15.

with the recipient, and the latter would only be entitled to execute its algorithms in the intermediary's database, without receiving any of the shared data itself.[2562] As illustrated in the principles for B2G data sharing outlined above[2563], the intermediaries' databases would thus constitute a form of "testing environments ('sandboxes') for pilot testing ('pilots') to help assess the potential value of data for new situations in which a product or service could potentially be used ('use cases')".[2564] As a result, only the trained algorithms, but not the data originally shared by the data holders, would then be transferred by the intermediaries to the recipients.[2565]

The advantage of resorting to such intermediaries is that this could reduce the risks for the multiple individuals whose data could be shared, as these intermediaries could, for instance, ensure the anonymisation of the data before it is accessed by the data recipients to train their algorithms.[2566] Moreover, these risks for the individuals are further reduced if only the algorithms, but not the training data, are transferred to the recipients. On the other hand, this technical approach makes it much more cumbersome for the data recipients to conduct their activities, and it would require an enormous infrastructure for the intermediary, in order to process the data (continuously) in any meaningful way.[2567] As a result, the economic objectives of the horizontal legislations might not be achieved to their full extent.

416. In light of all of the above, it appears that determining how the data sharing should be implemented technically will require to find a balance between the benefits and costs of various technical approaches. As the result of this balance will largely be function of the circumstances of the cases at hand, the horizontal legislations themselves may not be the best place to address this issue. However, it would be advisable for these legislations to charge regulatory bodies to define the technical modalities of the sharing in cases where the data holders and recipients (and potentially the trusted data intermediaries) do not agree on them. In such a case, it will be important for these regulatory bodies to be aware of the potential anti-competitive effects of the data sharing obligation, notably if they envisage to resort to the creation of a data pool for the technical implementation of the data sharing.[2568]

These regulatory bodies could be the national authorities to be appointed in the context of the Data Governance Act.[2569] Indeed, the knowledge of the technical experts that could be appointed within these authorities could be precious to suggest concrete technical sharing means in the absence of an agreement between the data holder and the data recipient, as the

---

[2562] *Ibidem*.
[2563] See point 392.
[2564] High-Level Expert Group on Business-to-Government Data Sharing, "Towards a European strategy on business-to-government data sharing for public interests – Final report", 2020, available at https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more, p. 7.
[2565] J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 12.
[2566] *Ibidem*.
[2567] J. Krämer, D. Schnurr and S. Broughton Micova, "The role of data for digital markets contestability", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/, p. 97.
[2568] On this issue, see Part III, Chapter 1, Section D, d).
[2569] See Recitals 22 to 34 and Articles 13 and 23 to 25 of the Proposal for a Data Governance Act.

technical mechanisms used for *voluntary* data sharing are equally relevant for *compulsory* data sharing imposed by horizontal legislations. These national authorities could be assisted by the future European Data Innovation Board.[2570]

6. How will these legislations be enforced?

417. Finally, it is essential to ensure an appropriate enforcement of the above-mentioned rules, in order for the horizontal *ex ante* legislations imposing compulsory B2B data sharing for economic purposes to be truly efficient and to reach the aims pursued. Indeed, a lack of (timely) enforcement can affect the full deployment of the legal framework's effects. For instance, it has been outlined that the time-consuming process of competition intervention is not aligned with the timing of market evolutions and that, as a result, enforcement might come too late, when the damage is already irreparable.[2571] Moreover, it has been outlined that even if the GDPR has created a strict legal framework for the processing of personal data, the enforcement of the GDPR by data protection authorities is sporadic (largely due to a lack of sufficient resources), leading to negative effects not only on the individuals' right to personal data protection, but also on competition.[2572]

Accordingly, it is fundamental for the horizontal *ex ante* legislations imposing compulsory B2B data sharing to ensure that the rules they enshrine will be respected and adequately enforced. Moreover, as outlined throughout this sub-section, many concrete issues will need to be determined on a case-by-case basis. Therefore, while these horizontal legislations will need to determine the "rules of the game" for compulsory data sharing, one or several regulatory bodies will need to be appointed in order to apply these rules on a case-by-case basis, and to enforce them. In substance, two avenues can be pursued.

418. On the one hand, a (new) regulatory body could be appointed at the European level, in order to ensure a harmonised, consistent and coherent application and enforcement of these horizontal *ex ante* legislations imposing B2B data sharing for economic purposes.[2573] Another advantage of resorting to a single authority appointed at the European level is that it would quickly develop the appropriate expertise, since it would be the sole body to apply the "rules of the game". In this regard, it should be reminded that the proposal for a "Digital Markets Act" provides that the compliance with this legislation should be monitored by the European Commission[2574], and that similar proposals of appointing a single authority have also been made in the UK and in the US.[2575] Interestingly, the European Commission's proposal for a Data Governance Act also considered the creation, at the European level, of a single new

---

[2570] Recitals 40 and 41 and Articles 26 and 27 of the Proposal for a Data Governance Act.
[2571] See Part III, Chapter 1, Section E.
[2572] See Part III, Chapter 2, Section A, c).
[2573] See P. Alexiadis and A. de Streel, "Designing an EU Intervention Standard for Digital Platforms", *Robert Schuman Centre for Advanced Studies Research Paper No. 2020/14*, 26 February 2020, available at https://ssrn.com/abstract=3544694, p. 46-47; A. de Streel, M. Cave, R. Feasey, J. Krämer and G. Monti, "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *CERRE Recommendations Paper*, November 2020, available at https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/, p. 17-19.
[2574] See Articles 3 to 7 and 18 to 33 of the Proposal for a Digital Markets Act.
[2575] See points 396 to 398.

independent structure with legal personality (similar to the European Data Protection Board) to oversee the implementation of this legislation, but this idea was abandoned due to the high costs and the issues of political feasibility that it implied.[2576]

419. On the other hand, instead of appointing a (new) regulatory body at the European level, competent authorities could be appointed in each Member State. In fact, this is the approach that was taken by the European Commission in its proposal for a Data Governance Act.[2577] To ensure an effective enforcement of these legislations, these national authorities will have to cooperate and assist each other where necessary[2578], notably through the exchange of information and best practices.[2579] This should be facilitated by the Support Centre for Data Sharing and the European Data Innovation Board.[2580] Moreover, they will have to be impartial, transparent, consistent and reliable and they will need to intervene in a timely manner.[2581] If this second option is taken, this thesis argues that, in order to avoid an unnecessary multiplication of regulatory bodies, the same authorities should be appointed to monitor the horizontal *ex ante* legislations pertaining to both *voluntary* and *compulsory* data sharing.

420. Independently of the option taken, such authority will have an important role to play. Indeed, it could first be charged with determining whether a (large) data holder falls within the scope of the data sharing obligation.[2582] Secondly, it could be tasked with receiving the compulsory notification of activities from the data recipients[2583], in order to assess the legitimacy of their activities and whether they offer sufficient guarantees, notably in terms of personal data protection[2584], and it could be empowered to impose fines and/or other remedies of this is not the case.[2585] Third, it could be charged with identifying the data that are necessary, relevant, and proportionate for the recipient's purposes, and with determining the "proportionate remuneration" and the technical modalities for the sharing, in the absence of an agreement between the data holders and the data recipients on these matters.[2586]

421. Finally, as the monitoring and enforcement of the *ex ante* legislations would imply a substantial workload, it will have to be ensured that these regulatory authorities have adequate financial and human resources, as well as the necessary technical knowledge and resources, to

---

[2576] Proposal for a Data Governance Act, p. 6. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit*., p. 28-29, 40, 43 and 52-53.
[2577] Articles 13 and 23 to 25 of the Proposal for a Data Governance Act.
[2578] Articles 13.6 and 23.6 of the Proposal for a Data Governance Act.
[2579] See, by analogy, European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html, p. 20.
[2580] See Recitals 40 and 41 and Articles 26 and 27 of the Proposal for a Data Governance Act. See also Commission Staff Working Document, Impact assessment report accompanying the Data Governance Act, *op. cit*., p. 54-55.
[2581] Article 23.2 of the Proposal for a Data Governance Act.
[2582] See point 398.
[2583] See point 401.
[2584] See, by analogy, Article 13 of the Proposal for a Data Governance Act. See also point 408.
[2585] See, by analogy, Article 13.3 to 13.5 of the Proposal for a Data Governance Act.
[2586] See points 405, 411 and 416.

carry out these missions.[2587] Moreover, to ensure an efficient and harmonised enforcement across the Digital Single Market, it will be fundamental for these regulatory authorities to cooperate with, and assist, each other and to be coherent in their decisional practice.[2588] Additionally, they will need to cooperate with the data protection and competition authorities, as well as with other relevant sectoral authorities, as some overlapping issues may have to be tackled by different regulatory authorities.[2589]

To be sure, the multiplication of regulatory authorities can lead to several issues that could hamper the swift enforcement of these compulsory data sharing initiatives. Indeed, if, as suggested, regulatory authorities are appointed in each Member State, there is a risk that this could lead to different degrees of enforcement across the Union, as well as to diverging or even contradicting case law, if there is insufficient cooperation and exchange of information and good practices between the different authorities. The cooperation issues that have become apparent in the context of the enforcement of the GDPR are a clear illustration of this problematic.[2590] Moreover, even if the data sharing initiatives could require from these authorities to cooperate with other types of authorities, such as data protection and competition authorities, one should be aware of the risks of overlapping "enforcement competences", and of the ensuing "regulator wars" that could occur in order to handle specific types of cases that could be dealt with on the basis of different regulatory approaches (compulsory data sharing initiatives, competition law, data protection law, consumer protection law, etc). This could lead to a dilution of the application of these norms, generating significant levels of legal insecurity and thus hampering the accomplishment of the objectives pursued by the data sharing initiatives. Although these "enforcement design" considerations will not be further detailed nor analysed here, as they fall outside of the scope of this thesis, it is important to underline that further research on the matter is indispensable in order to identify concrete proposals that would allow to solve these issues, as without proper and efficient enforcement, it might be missed out on the numerous benefits that should result from these compulsory data sharing initiatives.

* * *

422. To conclude this Chapter, the above-mentioned insights regarding the key elements that horizontal *ex ante* legislations imposing B2B data sharing for economic purposes should consider are summarised in Table 3.

Table 3: Insights on the key elements to consider for horizontal ex ante legislations imposing B2B data sharing for economic purposes

	"Ex ante" legislations imposing B2B data sharing for economic purposes
Data holders subject to the sharing obligation	Asymmetric application to a specific sub-set of data holders.[2591] Determination based on a set of clear quantitative and qualitative indicators contained

[2587] See, by analogy, Article 23.5 of the Proposal for a Data Governance Act.
[2588] Articles 13.6 and 23.6 of the Proposal for a Data Governance Act.
[2589] See Recitals 28 and 29 and Article 12.3 of the Proposal for a Data Governance Act.
[2590] See Part III, Chapter 2, Section A, d).
[2591] See Part III, Chapter 3, Section B, b), 1, i.

	in the legislations, which would allow the regulatory authority to decide, on a case-by-case basis, whether a specific data holder falls within the scope of the initiative.[2592]
Data recipients entitled to benefit from the sharing obligation	Recipient could be required to notify a description of the economic purposes that it intends to pursue.[2593] *Ex post* assessment of the legitimacy of the recipients' interests and of whether they offer sufficient guarantees in terms of privacy and security.[2594] Imposition of harmonised obligations on the recipients for the provision of their products/services, to be monitored *ex post* as well.[2595]
Types of data covered by the sharing obligation	Only actively provided and observed data (not acquired, nor inferred/derived data).[2596] Only the data that are necessary, relevant and proportionate, in terms of detail (e.g. type of data, granularity, quantity, frequency of access).[2597] Not only historical data, but also present and future data.[2598] Personal data should only be shared to the extent that this complies with the GDPR's principles and that there are lawful basis of processing allowing the sharing.[2599] Legislations could contain a provision forbidding data recipients from re-identifying the multiple individuals whose data have been aggregated and pseudonymised prior to the sharing.[2600]
Remuneration of the data holder as compensation for the sharing obligation	Proportionate remuneration (legislations could outline several factors to be taken into consideration: volume of data; by-product v. core economic activity of the data holder; data covered by an IP right or not; data shared with a direct competitor or not).[2601] If the data holder(s) and data recipient(s) fail to agree on the data sharing price, this price could be determined by an independent third party.[2602] To mitigate the risk of lengthy negotiations, the legislations could set binding deadlines to speed up the process. Data holder can charge the marginal costs incurred for the anonymisation of the aggregated data (e.g. the costs incurred in order to reach a sufficient level of granularity) to the data recipients.[2603]
Technical implementation of the sharing obligation	The horizontal legislations themselves may not be the best place to address this issue.[2604] Rather, it would be advisable for these legislations to charge regulatory bodies to define the technical modalities of the sharing in cases where the data holders and recipients do not agree on them.

[2592] See points 396 to 398.
[2593] See Part III, Chapter 3, Section B, b), 2.
[2594] See point 401.
[2595] See point 402.
[2596] See Part III, Chapter 3, Section B, b), 3, i.
[2597] See Part III, Chapter 3, Section B, b), 3, i.
[2598] See point 405.
[2599] See Part III, Chapter 3, Section B, b), 3, ii.
[2600] See point 408. See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 12.
[2601] See Part III, Chapter 3, Section B, b), 4.
[2602] See point 411.
[2603] See point 412.
[2604] See Part III, Chapter 3, Section B, b), 5.

Chapter 4. Societal initiatives imposing B2B data sharing

423. Coincidentally to the creation of economic initiatives imposing B2B data sharing, one could also consider the adoption of compulsory B2B data sharing initiatives pursuing societal objectives. As outlined in the European Commission's *Strategy for data*, "making more data available and improving the way in which data is used is essential for tackling societal, climate and environment-related challenges, contributing to healthier, more prosperous and more sustainable societies".[2605] Indeed, as it is apparent from the numerous examples provided in Part I of this thesis, not only public sector data, but also private sector data, can make a significant contribution to the common good.[2606]

Yet, one must acknowledge that the policy and legislative discussions pertaining to the creation of societal initiatives imposing B2B data sharing are scarce. Indeed, while some societal initiatives pertaining to (compulsory) data sharing are being proposed in the B2G field[2607], the same cannot be said about societal initiatives imposing B2B data sharing. Therefore, this Chapter will aim at developing some prospective reflections on why they might make sense and on how they could be constructed in the future, in the hope to spur further discussions on this topic. The aim is thus not to be exhaustive, but rather to set some foundations on which future research could build.

Section A. Contextualisation

424. Like any other initiative imposing B2B data sharing, societal initiatives will entail balancing exercises. In substance, the broader societal benefits deriving from the wider data sharing that such initiatives would entail[2608] would have to be balanced with the data holder's business interests, as compulsory data sharing might deter the data holder's incentive to further collect data, due to the fear of free-riding.[2609] However, this thesis argues that, in light of the fact that the B2B data sharing initiative would pursue societal objectives, the data holder's costs may weigh less heavily in the balance, as they are opposed to fundamental societal objectives that could be viewed as superseding "mere" economic considerations. Additionally, these horizontal legislations will have to comply with the personal data protection rules.[2610]

425. One way to address these balancing exercises would be to consider, by analogy with what has been said for economic initiatives[2611], that such societal initiatives imposing B2B data sharing should only be created when "specific circumstances" dictate it. Indeed, such

---

[2605] Communication from the Commission, "*A European strategy for data*", *op. cit.*, p. 3. See also J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 6-8; P. Picht, "Towards an Access Regime for Mobility Data", *op. cit.*, p. 942.
[2606] See Part I, Chapter 2, Section C, a); and in particular see point 93.
[2607] See, for instance, Articles 15 to 22 of the Proposal for a Data Governance Act; and European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151, p. 2 and 5.
[2608] See Part I, Chapter 2, Section C, a); and in particular see point 93.
[2609] D. Rubinfeld and M. Gal, "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 374.
[2610] See points 91 and 96 and Part III, Chapter 2 and Chapter 3, Section B, b). See European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, *op. cit.*, p. 8.
[2611] See point 382.

legislations should only be adopted if they are proportional and necessary to address these "specific circumstances", in order to achieve an optimal balance with the data holder's freedom to conduct a business. Accordingly, this would entail that such compulsory data sharing should only be imposed if less stringent alternatives, such as the stimulation of *voluntary* data sharing for societal purposes/the common good[2612], turn out to be insufficient to achieve the desired societal objectives, or if it is highly important and/or urgent to achieve these objectives.

"Specific circumstances" justifying the adoption of a compulsory data sharing legislation could, arguably, be established in situations where a just, fair and equal access to (some) data would be necessary to tackle societal challenges.[2613] For instance, one could consider whether B2B data sharing could be imposed in order to tackle global pandemics, in cases where pharmaceutical companies refuse to share data about their research aiming at developing the appropriate vaccine or medication, thus slowing down the global cure-finding process to the detriment of the general interest. In such a scenario, it might be justified to make it compulsory for pharmaceutical companies to share, with private healthcare and/or research institutions, data pertaining to vaccine/medication trial results, in order to rapidly identify the trials that lead to unsatisfactory results and those that lead to more promising results, in order to address such global healthcare challenges caused by pandemics as fast as possible.

Other important societal objectives such as avoiding food waste or limiting mankind's environmental footprint could also be deemed as justifying compulsory B2B data sharing in "specific circumstances". To illustrate this, it can be reminded that, as mentioned above[2614], farmers increasingly resort to "smart farming", notably in order to monitor of the health of crops and to detect plant diseases at an early stage (crop sensors). As this data is usually collected through sensors integrated in farming equipment sold by specialised manufacturers, it is the latter who often have control on the data, and they might not be eager to share it. Yet, one could reflect on whether it would be justified, in some specific situations, to compel these farming equipment manufacturers to share such data in order to prevent food waste. For instance, these manufacturers could be forced to share data about the apparition of a disease (inferred from the observation of crop sensor data they have received from one/several farms) with farmers active in the same territory on a very short notice, in order to enable the farmers to address the issue rapidly and to limit the loss of crops. In the same vein, these manufacturers could be forced to share data about the efficiency of a certain type of pesticide and the appropriate dose to be sprayed, in order to reduce the environmental damage caused by such products. Indeed, as these manufacturers could financially benefit from "over-spraying" as it implies that they will sell more products, they might not be willing to share such data on a voluntary basis. Yet, this could lead to highly detrimental environmental consequences, and could therefore potentially justify the adoption of compulsory B2B data sharing initiatives.

[2612] See, in this regard, Articles 15 to 22 of the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final.
[2613] J. Shkabatur, "The Global Commons of Data", *Stanford Technology Law Review*, 2019, Vol. 22, p. 401-402. See Part I, Chapter 2, Section C, a).
[2614] See point 93.

Section B. Prospective thoughts on how these societal initiatives imposing B2B data sharing could be constructed

426. Similarly to economic initiatives, societal initiatives imposing B2B data sharing could either be sectoral or a could have a more general horizontal scope. As mentioned above[2615], while sector-specific legislations have the advantage of being much more targeted and adapted to the sector's needs, this must be balanced with the non-rivalrous and general-purpose nature of data, which implies that it could be re-used for completely different purposes in another sector.[2616] In fact, such a sectoral limitation seems especially unwarranted if the data sharing legislation pursues societal objectives, as cross-sectoral re-use could generate significant societal value.[2617] For instance, an energy provider's research data pertaining to its decarbonisation initiatives could also be useful for other actors active in other sectors, such as transport, to reduce their environmental footprint. Similarly, air pollution data collected by sensors located on buses operated by a ride-sharing service provider could be highly useful for farmers that are active in the same territory, as such data about the air quality could enable them to relocate their cattle to less polluted places. Therefore, limiting the scope of the compulsory data sharing legislation to re-uses within a single sector would not enable the generation of such additional societal value. Accordingly, horizontal initiatives imposing B2B data sharing for societal purposes might have to be favoured.

427. Furthermore, even if "specific circumstances" justify the adoption of societal initiatives imposing B2B data sharing, the concrete provisions of such legislations will nevertheless need to find a balance between the societal benefits of the sharing and the costs on the data holder's business interests, and they will need to comply with the individuals' right to privacy and to personal data protection. This will require tackling the same fundamental questions as the ones raised in the analysis pertaining to economic initiatives imposing data sharing[2618], namely: Who will have to share data and who can receive the data? To which types of data would this apply? Should this be remunerated? How could this be implemented technically? How will these legislations be enforced?

Once again, it should be made clear from the outset that there is no "one size fits all" answer to these questions, and that the result of the balancing exercises underlying each of these questions will necessarily be case specific. In this regard, some of the guiding principles identified above in the fields of G2B and B2G data sharing can be useful for societal initiatives as well.[2619]

[2615] See Part III, Chapter 3, Section A.

[2616] See point 52; Deloitte, "Realising the economic potential of machine-generated, non-personal data in the EU", *Report for Vodaphone Group*, July 2018, available at https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf, p. 32. See also Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on European data governance: An enabling framework for common European data spaces (Data Governance Act)*", Brussels, 25 November 2020, SWD(2020) 295 final, p. 15.

[2617] See Part I, Chapter 2, Section C, a).

[2618] See Part III, Chapter 3, Section B, b).

[2619] See Part III, Chapter 3, Section B, a).

As many of the reflections pertaining to these questions are, to a large extent, similar to those developed in the context of the analysis of economic initiatives imposing B2B data sharing, the structure of this Chapter will mirror the structure of Chapter 3, Section B, b), and this thesis will solely focus here on developments that are specifically relevant for societal initiatives, while reverting, for the rest, to the corresponding developments in Chapter 3.

a) Who will have to share data?

428. Because compulsory B2B data sharing entails costs for data holders, it is important to ensure that this obligation will only apply to the data holders whose data is considered as necessary to achieve the societal objectives pursued by the initiative. However, arguably, it could be conceivable to apply the data sharing obligation to a broader amount of data holders if the purpose is societal, rather than economic.[2620] Indeed, by analogy with what has been said above about *"empowerment" initiatives imposing data sharing*, it would make sense to impose such obligations symmetrically.[2621] This is because not only large data holders, but also smaller actors, may hold data that is considered as being valuable in order to fulfil these societal objectives.

Yet, the risk of applying such data sharing obligations symmetrically is that it could disproportionally burden smaller undertakings, and that this could negatively affect competition if it has an impact on their capacity to innovate, notably in a situation where they would have to dedicate an important share of their resources to the compliance with societal initiatives imposing data sharing. Accordingly, to limit this risk, it could be envisaged to include, in such legislations, an exemption for smaller actors that have a limited number of financial and human resources and/or a small turnover, in order to avoid overburdening them.[2622] In this perspective, and as suggested by Mayer-Schonberger and Ramge, the legislations could create "progressive data sharing obligations", which would kick in once the data holder has reached a certain size or turnover, and according to which the amount of data to be shared by a specific data holder should be function of its size / turnover.[2623] The bigger its size or turnover, the more data it has to share. This determination of whether a data holder meets this minimal threshold and of the amount of data to be shared could be made, on a case-by-case basis, by regulatory authorities. In order to avoid an unnecessary multiplication of regulatory authorities, these regulatory authorities could be the same as those that will be created in the context of the Data Governance Act.[2624]

However, it must be considered that such an exemption and progressive sharing mechanism would potentially limit the societal benefits to be expected from the legislations imposing the compulsory data sharing, compared to a situation in which the sharing obligation would apply in full to all data holders. Yet, as these benefits must be balanced with the costs that such a

---

[2620] On this point for economic initiatives imposing B2B data sharing, see Part III, Chapter 3, Section B, b), 1.
[2621] See points 211 and 212.
[2622] See, by analogy, A. Diker Vanberg and M. Ünver, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", *European Journal of Law and Technology*, 2017, Vol. 8, Issue 1, p. 1-22; OECD, *Consumer Data Rights and Competition - Background note*, June 2020, DAF/COMP(2020)1, available at http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm, p. 43.
[2623] V. Mayer-Schonberger and T. Ramge, *Re-inventing capitalism in the age of big data*, *op. cit.*, p. 167-169.
[2624] See Articles 13 and 23 to 25 of the Proposal for a Data Governance Act.

sharing imposes on the data holders, it could be argued that the costs that would be imposed on smaller actors would be too important to justify such an obligation, while they would weigh less heavily in the balance when they are applied to larger data holders, which can absorb them more easily.

b) Who can receive the data?

429. When considering the creation of a societal initiative imposing B2B data sharing, it should also be reflected on whether any recipient whatsoever should be entitled to access the data holder's data, or whether only some of them should be entitled to such access. The former option would potentially maximise the societal benefits pursued by the initiative, in light of the non-rivalrous nature of data. However, the greater the number of potential recipients, the greater the risks for the data holder's business interests and for the privacy and personal data protection of the multiple individuals whose data would be shared in an aggregated way.[2625]

Accordingly, the second option might be preferable, and, by analogy with the principles for B2G data sharing outlined above[2626], the compulsory B2B data sharing initiative could provide that only the recipients that can demonstrate that their re-use will contribute to the societal objective underlying the initiative should benefit from an access to the data.[2627]

By analogy with what has been said in this regard for empowerment initiatives and for economic initiatives[2628], which will not be repeated here, this thesis argues that in order to be entitled to receive the data, the data recipient could be required to notify a description of the specific societal purpose that it intends to pursue to supervisory authorities.[2629] These authorities, which could be the same as those created by the Data Governance Act[2630], could then assess, *ex post*, the legitimacy of the recipients' societal interests and whether they offer sufficient guarantees in terms of privacy and security (in collaboration with the data protection authorities[2631]).[2632] Moreover, harmonised obligations could be imposed on the recipients in order to ensure their trustworthiness, which could be monitored *ex post* as well.[2633]

c) To which types of data would this apply?

430. Societal initiatives imposing B2B data sharing will also have to determine the scope of the data to be covered by the sharing obligation. This implies another key balancing exercise, as opting for a broad scope of data would increase the potential societal benefits for recipients and society, but would imply greater costs for the data holder's business interests, as well as

---

[2625] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit*., p. 9 and 60.
[2626] See point 392.
[2627] J. Drexl, "Data Access and Control in the Era of Connected Devices", *op. cit.*, p. 164.
[2628] See Part II, Chapter 2, Section C, c) ; and Part III, Chapter 3, Section B, b), 2.
[2629] See, by analogy, Article 17.4.h) of the Proposal for a Data Governance Act.
[2630] See point 218.
[2631] See, by analogy, Recitals 28 and 29 and Article 12.3 of the Proposal for a Data Governance Act.
[2632] See, by analogy, Article 13 of the Proposal for a Data Governance Act. See also point 408.
[2633] See, by analogy, Recitals 22 to 34 and Articles 9 to 14 of the Proposal for a Data Governance Act.

greater the risks for the privacy and personal data protection of the multiple individuals whose data would be shared in an aggregated way.

431. By analogy with what has been said above regarding economic initiatives[2634], which will not be repeated here, actively provided and observed data should be included in the scope of societal initiatives imposing B2B data sharing. For instance, car manufacturers, navigation system providers, fleet managers and parking operators could be compelled to share location and parking availability data (i.e. observed data) in order to enable "smart parking" services, which would limit the pollution deriving from CO_2 car emissions and would reduce the number of cars on the network.[2635] Similarly, in the context of a global pandemic, private healthcare institutions could be compelled to share data pertaining to their intensive care units' bed occupation rate (i.e. observed data), in order to better distribute the arrival of new patients and to address sanitary concerns.[2636]

Moreover, in light of the societal objectives pursued by these initiatives, one could reflect on whether the scope of the data covered should also include, in some circumstances, some of the data holder's inferred/derived data, as these could contain highly valuable information. Indeed, if socially valuable inferred/derived data are held (exclusively) by some data holders, including these types of data in the scope of these legislations could generate immense societal benefits.[2637] For instance, coming back to the examples mentioned earlier in this Chapter[2638], it might be justified to make it compulsory for pharmaceutical companies to share, with private healthcare and/or research institutions, inferred/derived data pertaining to vaccine/medication trial results; or to make it compulsory for farming equipment manufacturers to share inferred/derived data about the apparition of a disease with farmers active in the same territory, or inferred/derived data about the efficiency of a certain type of pesticide and the appropriate dose to be sprayed.

Yet, these societal benefits would have to be carefully balanced with the costs that this would warrant for the data holder, notably due to the fact that such derived/inferred data might be covered by IP rights.[2639] This might however be justified in circumstances where it is highly important and/or urgent to achieve these societal objectives. Moreover, if, as suggested above[2640], these legislations pursuing societal objectives are constructed around "progressive data sharing obligations"[2641], data holders having smaller sizes or turnovers could be exempted from the obligation to share inferred/derived data.

432. For the rest, and by analogy with what has been said above regarding economic initiatives[2642], which will not be repeated here, only the data that are necessary, relevant and

---

[2634] See Part III, Chapter 3, Section B, b), 3, i.
[2635] See point 93.
[2636] *Ibidem*.
[2637] J. Shkabatur, "The Global Commons of Data", *Stanford Technology Law Review*, 2019, Vol. 22, p. 383.
[2638] See point 425.
[2639] See Part I, Chapter 2, Section B, b), 1.
[2640] See point 428.
[2641] See V. Mayer-Schonberger and T. Ramge, *Re-inventing capitalism in the age of big data*, *op. cit.*, p. 167-169.
[2642] See Part III, Chapter 3, Section B, b), 3, i.

proportionate for the societal objectives pursued by the initiative should be shared – although this could cover historical, but also present and future data –, and these societal initiatives imposing B2B data sharing could provide that the data holder is compelled to licence, under objective, proportionate and non-discriminatory conditions, any potential database right that it may have on the data.

Finally, these initiatives should provide that aggregated personal data pertaining to multiple individuals should only be shared to the extent that this complies with the GDPR's principles (lawfulness, fairness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; integrity and confidentiality; and accountability)[2643] and that there are lawful basis of processing allowing the sharing.[2644]

d) Should this be remunerated?

433. Similarly than for economic initiatives[2645], societal initiatives imposing B2B data sharing could also provide that the data holder should be remunerated in exchange for the data sharing, as this would be a way to protect his business interests, in return for the expected benefits of these initiatives.[2646]

In this regard, and contrary to what has been said regarding economic initiatives, the price calculation method contained in the PSI Directive might be preferable than an open formula such as a "proportionate remuneration".[2647] Indeed, contrary to economic initiatives, the fact that such a method does not take appropriately into account the loss of "data advantage" or of "data power" for the data holder deriving from the sharing is not as problematic, as in this context the data is shared for societal purposes, and not for economic purposes with competitors. The sharing of the data, in such circumstances, is thus less likely to affect the data holders' "data advantage", especially if the recipients have to demonstrate that their re-use will contribute to the societal objective underlying the initiative.[2648] Moreover, in light of the importance of achieving the societal objectives in a timely manner, using a more concrete price calculation method, such as the one contained in the PSI Directive, would arguably make the process faster, as it will not be hampered by discussions pertaining to what should be considered as a "proportionate remuneration", which is the downside of a more open formula.[2649]

Accordingly, societal initiatives imposing B2B data sharing could provide that the price should cover the costs of data collection, production, reproduction, dissemination and storage

---

[2643] Articles 5 of the GDPR. For a more detailed analysis of this articulation, see, by analogy, Part III, Chapter 2, Section B, b).
[2644] Articles 6 of the GDPR. For a more detailed analysis of this articulation, see, by analogy, Part III, Chapter 2, Section B, a); and Part III, Chapter 3, Section B, b), 3, ii.
[2645] See Part III, Chapter 3, Section B, b), 4.
[2646] See R. Feasey and A. de Streel, "Data Sharing for Digital Market Contestability", *op. cit.*, p. 11 and 77-80. Some however argue that the data holders should not be entitled to a remuneration: see J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 14.
[2647] See points 409 to 411.
[2648] See point 429.
[2649] See point 411.

incurred by the data holder, as well as a reasonable return on investment for the holder.[2650] Indeed, this price calculation method presents the advantage of being relatively simple, especially if the initiatives defines what constitutes a "reasonable" return on investment.[2651] Furthermore, they could provide, as outlined for G2B data sharing, that the data holder can charge the marginal costs incurred for the anonymisation of the aggregated data (e.g. the costs incurred in order to reach a sufficient level of granularity) to the data recipients.[2652]

e) How could this be implemented technically and how will this be enforced?

434. Finally, when reflecting on the creation of a societal initiative imposing B2B data sharing, matters of technical implementation and of enforcement should also be considered. As the above analysis of these matters conducted in the context of economic initiatives is equally applicable to societal initiatives imposing B2B data sharing, they will not be repeated here.[2653] It will simply be reminded that, if a "progressive data sharing obligation" is adopted, supervisory authorities will have an important role to play, as they could be charged with determining whether a small data holder can be exempted from the sharing obligation, or whether it could at least be exempted from sharing its inferred/derived data.[2654]

* * *

435. To conclude this Chapter, the above-mentioned insights regarding the key elements that societal initiatives imposing B2B data sharing should consider are summarised in Table 4.

Table 4: Insights on the key elements to consider for societal initiatives imposing B2B data sharing

	Societal initiatives imposing B2B data sharing
Data holders subject to the sharing obligation	Symmetric application to all data holders but exemption for smaller actors which only have a limited size and/or turnover, in order to avoid overburdening them (consideration of a "progressive data sharing obligation").[2655]
Data recipients entitled to benefit from the sharing obligation	Recipient could be required to notify a description of the societal purposes that it intends to pursue.[2656] *Ex post* assessment of the legitimacy of the recipients' interests and of whether they offer sufficient guarantees in terms of privacy and security.[2657] Imposition of harmonised obligations on the recipients for the provision of their products/services, to be monitored *ex post* as well.[2658]
Types of data covered by the sharing	Actively provided and observed data + potentially inferred/derived data (notably in circumstances where it is highly important and/or urgent to achieve these societal

[2650] See, by analogy, Article 6.1 of the Directive 2019/1024.
[2651] See, by analogy, Article 2.16 of the Directive 2019/1024: "'reasonable return on investment' means a percentage of the overall charge, in addition to that needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the ECB".
[2652] See point 353.
[2653] See Part III, Chapter 3, Section B, b), 5 and 6.
[2654] See points 428 and 431.
[2655] See Part III, Chapter 4, Section B, a).
[2656] See Part III, Chapter 4, Section B, b).
[2657] *Ibidem*.
[2658] *Ibidem*.

obligation	objectives). Could be articulated around a "progressive data sharing obligation": data holders having smaller sizes and/or turnovers could be exempted from the obligation to share inferred/derived data.[2659] Only the data that are necessary, relevant and proportionate, in terms of detail (e.g. type of data, granularity, quantity, frequency of access). Not only historical data, but also present and future data.[2660] Personal data should only be shared to the extent that this complies with the GDPR's principles and that there are lawful basis of processing allowing the sharing.[2661] Legislations could contain a provision forbidding data recipients from re-identifying the multiple individuals whose data have been aggregated and pseudonymised prior to the sharing.[2662]
Remuneration of the data holder as compensation for the sharing obligation	Remuneration covering the costs of data collection, production, reproduction, dissemination and storage incurred by the data holder, as well as a reasonable return on investment for the holder.[2663] Data holder can charge the marginal costs incurred for the anonymisation of the aggregated data (e.g. the costs incurred in order to reach a sufficient level of granularity) to the data recipients.[2664]
Technical implementation of the sharing obligation	The societal initiatives themselves may not be the best place to address this issue. Rather, it would be advisable for these legislations to charge regulatory bodies to define the technical modalities of the sharing in cases where the data holders and recipients do not agree on them.[2665]

[2659] Part III, Chapter 4, Section B, c).
[2660] *Ibidem*.
[2661] *Ibidem*.
[2662] *Ibidem*. See J. Prüfer, "Competition Policy and Data Sharing on Data-driven Markets", *op. cit.*, p. 12.
[2663] Part III, Chapter 4, Section B, d).
[2664] *Ibidem*.
[2665] See Part III, Chapter 4, Section B, e) and Part III, Chapter 3, Section B, b), 5.

Conclusion

436. The aim of this doctoral thesis was to answer the following research question: "**What are the economic and societal balancing exercises underlying compulsory B2B data sharing?**".

To answer this question, the concept of data (What?) was first specified.[2666] In the context of this thesis, data was defined in a broad sense, as any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording.[2667]

While the European legal framework and the legal literature traditionally distinguish personal from non-personal data, this thesis opted to follow a common holistic approach for both categories of data because the boundary between these two concepts is porous and often difficult to establish in practice. Nevertheless, personal data considerations were taken into account when relevant. This led to the establishment of an alternative data typology composed of four categories of data, namely actively provided data, observed data, inferred/derived data and acquired data.[2668] In fact, this typology can be reduced to three broader categories of data, namely i) primary data, ii) inferred/derived data, and iii) acquired data. Indeed, actively provided and observed data can be classified in a common group of primary data. Inferred/derived data are a second generation of data drawn, by the data holder itself, from the analysis of this first generation of primary data. The data holder could also opt not to create/collect primary data or to generate inferred/derived data itself, but rather to acquire data from third parties, such as data brokers.

Although a common holistic approach for both personal and non-personal data was followed, the thesis focussed more on behavioural/consumer data than on non-personal IoT data. This is mainly because the two gaps that this thesis aims to fill through a normative approach precisely pertain to such behavioural/consumer data.[2669] Moreover, most of the European policy discussions pertaining to compulsory B2B data sharing relate to large data actors that draw a "data advantage" from their privileged access to, and control of, consumer/behavioural data.[2670] On the other hand, IoT non-personal data have received much less policy attention, especially since the option to create a "data producers right" on non-personal machine generated data has been abandoned.[2671] While this could change in the future with the growth of the IoT, notably in the context of societal initiatives imposing B2B data sharing[2672], this also explains why the focus of this thesis was mostly set on consumer/behavioural data, rather than on IoT non-personal data.

[2666] See Part I, Chapter 1.
[2667] This definition is based on Article 2.1 of the Proposal for a Data Governance Act; Article 2.19 of the Proposal for a Digital Markets Act.
[2668] See Part I, Chapter 1, Section C.
[2669] See point 5.
[2670] See Part I, Chapter 2, Section B, c); Part II, Chapter I; Part III, Chapters 1 and 3. See, for instance, the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final.
[2671] On this topic, see Part I, Chapter 2, Section B, b), 2.
[2672] See Part I, Chapter 2, Section C, a); and Part III, Chapter 4.

437. Then, a large focus of this thesis was set on the rationale for (data) sharing (Why?).[2673] In order to do so, this thesis first reverted to the more standard discussions on whether a resource should be shared.[2674] Indeed, finding a balance between granting exclusive ownership/property rights to the few, on the one hand, and providing access to and sharing resources with the many, on the other hand, has also always been a challenge, whether this related to tangible or intangible resources. Regarding intangible resources, it was outlined that the free-rider dilemma that underlies the creation of intellectual property rights, which were established in order to avoid an information underproduction problem, is also a key concern in discussions pertaining to whether data sharing should be made compulsory in certain circumstances. Indeed, the prospect of free-riders may discourage the creators/inventors from producing intangible resources, in light of their potential inability to generate returns on investments, and it may also discourage, for the same reasons, data holders from investing in data collection and/or analysis.

In fact, the European Commission itself reflected on whether an "IP-like" right on data should be granted to data producers, in order to stimulate data production, in light of this free-rider dilemma.[2675] However, a large majority of legal scholars argued that there was no economic justification to support such a proposal, as there is no evidence that the absence of such a right creates a lack of incentives for the production, analysis or marketing of data (i.e. there is no data underproduction problem). Moreover, the creation of such a right could have led to disruptive juxtapositions and delimitation problems with existing IP rights, and it could have strengthened entry barriers that, consequently, would have increased the market power of large data holders. Accordingly, the policy debates have moved away from the idea of creating an IP-like right on data, towards legal reflections revolving around data reservation (i.e. the fact that data holders have a *de facto* exclusive control on their data and can decide on whether, and to whom, they provide access to it).[2676] This explains why these intellectual property rights considerations were less relied on in the remainder of the thesis, and that the focus was rather set on competition considerations linked to data control and access.

438. It was, however, outlined that even if the Commission has moved away from (intellectual) property on data towards data reservation, it has not moved away from the dominant approach in our Western societies, namely that exclusive ownership or exclusive property is generally the default model (*in casu* data is exclusively reserved through contractual and technical means), while models based on sharing/access are less common.[2677] Yet, this thesis made the argument that concepts such as property or ownership, and sharing or commons, should not be opposed so strongly. Indeed, commons can be subject to ownership and can thus be subject to a form of appropriation or reservation, but, importantly, this does not lead to the exclusion of others. Rather, commons are a form of ownership that

---

[2673] See Part I, Chapter 2.
[2674] See Part I, Chapter 2, Section A.
[2675] See Part I, Chapter 2, Section B, b), 2.
[2676] See Part I, Chapter 2, Section B, a) and b).
[2677] See Part I, Chapter 2, Section B, b), 3.

organise the collective and shared use of a resource. To some extent, they reflect a form of inclusive property, as opposed to exclusive property. Commons, and other forms of sharing, are thus situated somewhere along a continuum between absolute exclusive property/ownership, on the one hand, and the absence of any form of property/ownership (public good/free-for-all), on the other hand. While a (data) commons approach could be a fertile ground to move away from the traditional conception of exclusive property towards more generative forms of rights, based on collective access and usage rights, this thesis did not further investigate this approach, because it is based on voluntary efforts, within a diffused community of actors, to govern a resource and to share it. It thus relies on *voluntary* (data) sharing in the context of the exercise of collective rights on commons. Yet, this thesis is instead focussed on hypotheses of *compulsory* data sharing, which do not fit in this commons approach.

Indeed, as outlined in the introduction, legal instruments promoting *voluntary* data sharing, tend to focus more on data governance and technical issues (standardisation, interoperability, etc.), in order to create more favourable conditions for the market actors to share data. The underlying idea behind these instruments is that it is preferable to first attempt to create a clear framework to incentivise the market actors to share data on their own initiative, rather than to compel them to do so. Yet, such *voluntary* data sharing initiatives may not always be sufficient, and legislators could be tempted to go a step further, by imposing *compulsory* data sharing. That being said, *voluntary* and *compulsory* data sharing should not be seen as two extremes on the regulatory intervention scale. Rather, there are links to be made between these two approaches, which complement each other. Indeed, if the step has to be taken from *voluntary* to *compulsory* data sharing regulatory initiatives, the latter should build on the former, as the data governance principles and technical provisions contained in the former are equally relevant for the latter. Despite this complementarity, the choice has been made, in this thesis, to focus on *compulsory* B2B data sharing regulatory initiatives, because if the legislator decides to force the sharing, this will require the prior consideration of a certain number of fundamental economic and societal balancing exercises. Highlighting the nature of these balancing exercises was the core objective of this thesis.

439. Building on the above-mentioned discussions, the thesis then delved in the analysis of the rationale for data sharing.[2678] In this regard, it was emphasised that, in light of the data's characteristics, a growing call for compulsory data sharing is being made.[2679] Yet, compulsory B2B data sharing is not a goal in itself, and it should only be used in specific circumstances as a way to achieve determined objectives. In fact, three types of rationale can be called upon to support compulsory B2B data sharing, namely economic, societal, and empowerment considerations.

440. To get a better grasp of the economic rationale for data sharing, the economics of data were presented.[2680] The digital economy is characterised by network effects and by strong economies of scale, scope and speed. Data therefore plays a prominent role and the ability to

[2678] See Part I, Chapter 2, Sections B and C.
[2679] See Part I, Chapter 2, Section B, c).
[2680] *Ibidem*.

use data to develop or improve innovative products or services is a key competitive parameter. Looking at it from the other side of the coin, these characteristics might lead to techno-economic entry barriers (uniqueness of the data collected by the incumbent data holder or unique gateway to it; economies of scale, scope and speed; network effects; lock-in and switching costs). Consequently, several market failures may appear. Firstly, the economics of data favour concentration. Indeed, data driven markets have a natural tendency to tip towards monopolisation as there is a strong first-mover advantage. Due to these first-mover advantage and market tipping dynamics, data concentration might increase entry barriers for new firms and strengthen the market power of data aggregators, leading to diminishing incentives for innovation. Such concentration may also establish long-term competitive advantages and this could endanger the contestability of these data driven markets. Secondly, these network effects and economies of scope, scale and speed may also be leveraged by an incumbent data holder to expand and strengthen its position in adjacent connected markets. Accordingly, there are clear incentives for data driven firms to expand their activities in as many markets as possible and to build conglomerates. In light of the above, compulsory B2B data sharing is increasingly being proposed in order to remedy these market failures.

At present, this is mainly tackled through competition law[2681], with the exception of a sector-specific data sharing legislation in the automotive sector.[2682] However, as competition intervention is a time-consuming process, it is increasingly argued that competition law rules should be adapted to the digital environment (e.g. by adapting the traditional balances to digital markets, or by increasing the use of interim measures or of market investigations) and that they should be complemented by the creation of potential *ex ante* legislations imposing B2B data sharing.[2683]

441. Compulsory B2B data sharing could also be justified by societal objectives.[2684] Indeed, increased data sharing could prove to be essential for tackling societal, environmental, health and mobility challenges.[2685] The underlying idea is that not only public sector data, but also private sector data, can be used to support societal goals. In contrast, this implies that a lack of data sharing, deriving from data concentration and conglomeration, will not only create economic challenges, but also societal challenges. As the societal value of the data held (exclusively) by some incumbent data holders is enormous, allowing (some) third parties to use this data could generate immense scientific benefits and could be used to address these societal challenges.

Yet, this thesis outlined that while the policy and legislative discussions pertaining to the creation of societal initiatives imposing data sharing are emerging in the B2G field, the same cannot be said about societal initiatives imposing B2B data sharing. Accordingly, this thesis developed some prospective reflections on why such initiatives might make sense and on how they could be constructed in the future, in the hope to spur further discussions on this topic.

[2681] See Part III, Chapter 1.
[2682] See Part III, Chapter 3, Section A, a).
[2683] See Part III, Chapter 1, Section E and Chapter III.
[2684] See Part I, Chapter 2, Section C, a).
[2685] See the numerous examples mentioned at point 93; and Part III, Chapter 4.

The aim was thus not to be exhaustive, but rather to set some foundations on which future research could build.

442. Thirdly, data sharing is also increasingly presented as a way to empower individuals, by giving them more control on their data through tools that allow them to decide at a much more granular level what can be done with it.[2686] In fact, this thesis outlined that these empowerment initiatives can pursue two different types of sub-objectives.

On the one hand, empowerment initiatives can pursue the objective of allowing the exercise of fundamental rights, such as the right to personal data protection and informational self-determination.[2687] This "power of control" that data subjects can (re)claim on their data is fundamental as it will facilitate the exercise of their fundamental rights, as increased access to information will improve their decision making and will allow them to take fundamental decisions about all aspects of their life.[2688]

On the other hand, empowerment initiatives can be adopted to address specific market failures.[2689] The underlying idea of these initiatives is that by giving more control to individuals on "their" data, this will allow them to multi-home or to switch more easily between service providers as their searching and switching costs are reduced, and this should reduce the market failures deriving from consumer inertia and lock-in effects.[2690] Indeed, the aim is to give more autonomy to the individuals by allowing them to optimise the use of their resources. In turn, this should facilitate entry and should foster competition on the targeted markets, which should lead to better services, more choice and lower prices for the individuals.

At present, both types of empowerment initiatives imposing data sharing are essentially structured around (some forms of) data portability rights.[2691] However, the effectiveness of these existing initiatives and their ability to truly empower individuals is being criticised and as a result, a growing call for the creation of a continuous portability right has emerged.[2692]

443. These distinct but possibly also complementary objectives[2693] led to the identification of two main categories of *compulsory B2B data sharing initiatives* that guided the analysis carried out in this thesis, namely *empowerment initiatives imposing B2B data sharing*, on the one hand, and *economic or societal initiatives imposing B2B data sharing*, on the other hand.[2694] A core difference between these two categories, other than the types of objectives pursued, is the amount of data transferred. Indeed, in this first category of initiatives, the amount of data transferred is relatively small as it is limited to the data relating to the specific individual at hand. Of course, the framework created as a whole by these initiatives can

---

[2686] See Part I, Chapter 2, Section C, b).
[2687] See Part II, Chapter 1, Section A.
[2688] See point 97.
[2689] See Part II, Chapter 1, Section B.
[2690] See point 97.
[2691] See Part II, Chapter 1, Sections A and B.
[2692] See Part II, Chapter 1, Section C.
[2693] See point 130.
[2694] See Part I, Chapter 3, Section B.

potentially lead to the sharing of data pertaining to a very large number of individuals, but each act of sharing will relate to a specific individual. Accordingly, these empowerment initiatives mostly benefit a specific individual but also have indirect benefits for third parties (such as (potential) competitors of the data holder). On the other hand, what will be shared in the second category of initiatives are larger amounts of (aggregated) personal data pertaining to multiple individuals and/or non-personal data rather than smaller quantities of data linked to a specific individual. These initiatives thus mostly benefit third parties but they also have indirect benefits for the individuals' whose data are shared.

444. An important finding of this thesis is that, independently of the objectives that it pursues, any compulsory B2B data sharing initiative must consider a certain number of fundamental economic and societal balancing exercises. Maximising data sharing should thus not be seen as an objective in its own right and data sharing obligations should only be imposed if the benefits created trump the economic and societal costs. More concretely, this thesis focussed on three balancing exercises[2695], namely the need to balance the benefits stemming from compulsory B2B data sharing initiatives with: i) the economic interests of the data holder; ii) personal data protection considerations; and iii) the long-term and collective costs that (some of) these initiatives could entail in terms of individual autonomy. This focus can be explained by the evolution of the doctoral research, which has paralleled the evolution of the policy discussions on compulsory B2B data sharing since 2016, which marked the beginning of the research.

Indeed, the economic, societal or individual empowerment benefits deriving from data sharing have to be balanced with the data holder's business interests.[2696] This is because data collection and processing and consequently data sharing entails costs for the data holder, as although data use by multiple parties does not affect its existence, it may affect its value. Therefore, data sharing obligations might create disincentives for data collection and processing as sharing could deter innovation by the data holder who might no longer want to invest in data collection if it no longer provides him with a competitive advantage, due to the fear of free-riding that derives from the non-rivalrous nature of data. Moreover, a data sharing obligation might also create reputational costs for the data holder, for instance if it is required to reveal data showing that its activity is highly polluting. If the data sharing initiative pursues economic objectives, it should also be factored that imposing data sharing might also deter innovation by third parties who will no longer see the point in innovating in order to collect the data themselves, as they will receive it from the data holder (expectation to free-ride).[2697] On the other hand, if the data sharing initiative pursues individual empowerment or societal objectives, the data holder's costs may weigh less heavily in the balance, as they are opposed to fundamental societal objectives that could be viewed as superseding mere economic considerations.[2698] In light of the above, the first ambition of this thesis was to adopt an analytical approach, in order to shed more light on how these economic interests of the data

[2695] See point 5 for more details.
[2696] See Part I, Chapter 2, Section B, c), 5; and Part I, Chapter 2, Section C.
[2697] See Part I, Chapter 2, Section B, c), 5.
[2698] See Part I, Chapter 2, Section C.

holders are factored in the existing compulsory B2B data sharing initiatives, and to provide some insights on how these interests could be factored in future initiatives.[2699]

Additionally, whether they pursue economic, societal or empowerment objectives, reaping the potential benefits deriving from these data sharing initiatives will only be acceptable if this is done in compliance with the right to privacy and to personal data protection of the (other) individuals whose data would be shared.[2700] As it quickly appeared that this articulation was insufficiently addressed by legislators and policy-makers, the second ambition of this thesis was to adopt a normative approach in order to fill this gap, by attempting to clarify the core elements that must be factored in this balancing exercise, and by attempting to provide insights on how this delicate articulation can be solved.[2701]

Moreover, *empowerment initiatives imposing B2B data sharing* imply another fundamental balancing exercise, namely that the potential individual short-term gains that are promised to individuals will have to be balanced with the potential long-term costs and collective costs that these initiatives might entail in terms of control, autonomy and self-determination. As this balancing exercise seems to be broadly overlooked by policy-makers and legislators, the third ambition of this thesis was, once again, to adopt a normative approach in order to fill this gap, by attempting to raise awareness about the crucial need to take these risks into consideration, and by attempting to provide insights on how this delicate balance can be addressed.[2702]

Indeed, empowering individuals by offering them more choice will not necessarily increase their control, autonomy and (informational) self-determination. In fact, if these empowerment initiatives are not strictly delineated, they might actually entail a high price and a loss of control for the individuals.[2703] This is because, due to strong asymmetries of information, individuals rarely have a clear understanding of what is done exactly with their data by the data holder, and do not have a clear view on whether the latter processes the data in the way it has announced. They are thus not fully aware of the consequences of sharing and the impact this could have on their privacy. Indeed, this data could be used to influence their future decision-making in covert, subtle and targeted manners, raising concerns in terms of their autonomy and self-determination. As a result, it must be factored that data that has been shared by individuals in exchange for short-term gains might, in the long-term, be broadly disseminated and/or be used against them, potentially leading to a loss of control and autonomy. Furthermore, it is important to acknowledge that an individual's decision to share data will not only have an impact on her own autonomy and self-determination, but also on those of others.[2704] Indeed, data sharing by an individual creates negative externalities, as it also reveals information about other individuals whose information is correlated with those of

---

[2699] See, inter alia, Part I, Chapter 2, Section B, c), 5; Part II, Chapter 2, Section A, a); Part II, Chapter 2, Section C; Part III, Chapter 1; Part III, Chapter 3, Section B; and Part III, Chapter 4, Section A.
[2700] See Part II, Chapter 2, Section A, b); Part III, Chapter 2; Part III, Chapter 3, Section B, b); and Part III, Chapter 4.
[2701] See, inter alia, Part II, Chapter 2, Section A, b); Part II, Chapter 2, Section C; Part III, Chapter 2; Part III, Chapter 3, Section B; and Part III, Chapter 4, Section A.
[2702] See Part I, Chapter 2, Section C, b) and Part II, Chapter 2, Section A, c).
[2703] See point 198.
[2704] See point 199.

others, even if they themselves did not share any data. In light of this relational and collective nature of data, it is also fundamental to balance the individual's potential gains from data sharing with the potential collective costs for other individuals in terms of control, autonomy and self-determination.

In order to assess these long-term and collective costs, this thesis argued that legislators could engage in a case-by-case risk assessment of the "systemic risks" that the empowerment initiatives could entail.[2705] In this context, legislators should consider the economic risks that such data sharing initiatives could entail for (other) individuals, as well as the "surveillance capitalism" risks that might derive from such practices. Moreover, legislators will also have to take into consideration the systemic risks that such data sharing initiatives could have on the exercise of fundamental rights by individuals, such as their possibility to take fundamental decisions about their health, their family life or their professional life. In assessing these risks, particular consideration should be given to the potentially rapid and wide dissemination of the data shared by individuals. On the basis of this risk assessment, legislators should then integrate – in the instrument creating the empowerment initiative –, reasonable, proportionate and effective measures aimed at mitigating the specific long-term and collective risks that will have been identified. Furthermore, the empowerment initiative should also provide that external and independent audits can be conducted in order to verify the compliance with these mitigation measures.

445. Another core finding of this thesis is that there is no one-size fits all answer to how the balancing exercises outlined above should be solved. Rather, the objective pursued by the compulsory data sharing initiative (economic, societal or empowerment) should be a key starting point when addressing these fundamental balancing exercises. It should indeed arguably have an impact on the determination of the *ratione personae* (data holders subject to the sharing obligation and data recipients that can access the data) and *ratione materiae* (types of data covered) scopes of these compulsory data sharing initiatives, as well as on considerations pertaining to the remuneration of the data holder and to the technical implementation of the data sharing initiatives.

In terms of the *ratione personae* scope of the initiatives[2706], this thesis has argued that *empowerment initiatives imposing B2B data sharing* should preferably apply symmetrically to all data holders. Indeed, since the core objective of such initiatives is to empower the individuals whose data is shared, it would make sense to impose them symmetrically so individuals can have more control on all their data, and not just on the data that is held by a limited number of data holders. Arguably, such a symmetric approach could also be adopted for *societal initiatives imposing B2B data sharing*, in order to maximise the potential social benefits, although there could be exemptions for smaller actors which only have a limited number of financial and human resources and/or a small turnover, in order to avoid overburdening them. This could for instance be done through a progressive data sharing obligation. On the other hand, there seems to be a strong consensus that *economic initiatives*

[2705] See points 200 to 202.
[2706] See Part II, Chapter 2, Section C, a), 2.; Part III, Chapter 3, Section B, b), 1; and Part III, Chapter 4, Section B, a).

imposing B2B data sharing should be asymmetric and limited to a specific sub-set of data holders. In this regard, the determination of whether a data holder falls within the scope of the data sharing obligation could be based on a set of clear quantitative and qualitative indicators contained in the legislations, to be assessed on a case-by-case basis by the controlling authority. Arguably, such a limitation of the scope of application of these initiatives is justified by the fact that the costs implied by the data sharing obligation on the data holder's business interests should only be imposed to a specific sub-set of data holders, namely those that are considered as playing a central role in the (systemic) market failure(s) that provoked the regulatory intervention.

Regarding the determination of the data recipients, it has been suggested that for all types of compulsory B2B data sharing initiatives that the recipient could be required to notify a description of the product/service it intends to provide, or of the economic/societal purposes that it intends to pursue.[2707] This would enable an *ex post* assessment of the trustworthiness and legitimacy of the recipients' activities, and of whether they offer sufficient guarantees in terms of privacy and security. While such a "notification obligation with *ex post* monitoring of the compliance" could be perceived, by the data recipients, as being too cumbersome and as delaying the benefits of the data sharing, it is certainly less burdensome than requiring a prior certification for the re-use. On the other hand, the option not to subject the re-use to any prior formality should arguably be excluded, as it is vital to ensure that the data is not shared openly with anyone without any limits, as this could have dramatic consequences in terms of the individuals' personal data protection and informational self-determination.[2708] Additionally, harmonised obligations could also be imposed on these recipients, to be monitored *ex post* as well. In case of a breach of an obligation imposed by the legislations, or if the data recipient has provided false information in its notification, the competent regulatory authorities could also be empowered to impose fines and/or to request the cessation of the unlawful processing.[2709]

Turning to the *ratione materiae* scope of these initiatives[2710], this thesis made the argument that *empowerment initiatives imposing B2B data sharing* should only apply to actively provided and observed data but not to inferred/derived data, which are the most valuable for the data holder, or to acquired data. However, it was emphasised that inferred/derived data can be obtained through the exercise of the GDPR data access right. Moreover, it should be made explicit that data holders have the possibility to keep using the data despite the data sharing obligation, and that such sharing should not adversarily affect other data subjects' right to personal data. The scope of *economic initiatives imposing B2B data sharing* should arguably also be limited to actively provided and observed data, excluding inferred/derived and acquired data. *Societal initiatives imposing B2B data sharing* on the other hand could potentially apply to inferred/derived data as well, notably in circumstances where it is highly

[2707] See Part II, Chapter 2, Section C, c); Part III, Chapter 3, Section B, b), 2; and Part III, Chapter 4, Section B, b).
[2708] See point 219.
[2709] See points 219 and 402.
[2710] See Part II, Chapter 2, Section C, a), 1.; Part III, Chapter 3, Section B, b), 3; and Part III, Chapter 4, Section B, c).

important and/or urgent to achieve these societal objectives. However, if, as outlined above, a progressive data sharing obligation is implemented, smaller data holders could be exempted from having to share such inferred/derived data. Moreover, for both *economic and societal initiatives imposing B2B data sharing*, it was underlined that only the data that are necessary, relevant and proportionate for the fulfilment of these objectives should be shared, although this should not be limited to historical data, but could also include present and future data. Importantly, personal data should only be shared to the extent that this complies with the GDPR's principles and that there are lawful basis of processing allowing the sharing. In this regard, the legislations could contain a provision forbidding data recipients from re-identifying the multiple individuals whose data have been aggregated and pseudonymised prior to the sharing.

Remuneration considerations were also taken into account.[2711] In this regard, this thesis argued that *empowerment initiatives imposing B2B data sharing* should in principle not imply any form of payment, neither from the individual whose data is shared, nor from a potential data recipient. This is because the potential costs that such initiatives might entail on the data holders' incentives to collect and process the data will, in fact, be minimal as the volumes of data that will be transferred through such mechanisms are quite low, as they relate to a specific individual. On the other hand, some form of remuneration could be envisaged for *economic and societal initiatives imposing B2B data sharing*. For *economic initiatives*, it was argued that a "proportionate remuneration" could be imposed, which would have to be determined on a case by-case basis. To facilitate this contextual assessment, the legislations could outline several factors to be taken into consideration, such as: i) the volume of data being shared; ii) whether the shared data has been generated as a by-product or as the core economic activity of the data holder; iii) whether the shared data is covered by an IP right; or iv) whether the data is shared with a direct competitor or not. Additionally, it was highlighted that, if the data holder(s) and data recipient(s) fail to agree on the data sharing price, this price could be determined by an independent third party. To mitigate the risk of lengthy negotiations, the initiative could set binding deadlines for this negotiation period. Moreover, the initiative could provide that the designated independent third party will have to draft guidelines aiming at providing more contextual information about the above-mentioned factors. These guidelines could also suggest the addition of new factors that would be worth taking into consideration. For *societal initiatives*, it was argued that the price should cover the costs of data collection, production, reproduction, dissemination and storage incurred by the data holder, as well as a reasonable return on investment for the holder. Furthermore, for both *economic and societal initiatives imposing B2B data sharing*, this thesis suggests that data holders could charge the marginal costs incurred for the anonymisation of the aggregated data (e.g. the costs incurred in order to reach a sufficient level of granularity) to the data recipients.

[2711] See Part II, Chapter 2, Section C, b); Part III, Chapter 3, Section B, b), 4; and Part III, Chapter 4, Section B, d).

This thesis also addressed the technical implementation of the data sharing initiatives.[2712] Regarding *empowerment initiatives imposing B2B data sharing*, depending on the cases it could be necessary to move beyond (continuous) data sharing, towards more interoperability, in order to truly empower the individuals, as (continuous) data sharing by itself does not remedy the lock-in effects deriving from network effects' coordination problem. Concerning *economic and societal initiatives imposing B2B data sharing*, it was outlined that the legislations themselves may not be the best place to address these technical issues. Rather, it would be advisable for these legislations to ask regulatory bodies to define the technical modalities of the sharing in cases where the data holders and recipients fail to agree on them.

446. Finally, and independently of the objectives pursued by the compulsory B2B data sharing initiatives, this thesis has emphasised that a timely enforcement of these initiatives will be of paramount significance. Indeed, a lack of (timely) enforcement can affect the full deployment of the legal framework's effects. For instance, it has been outlined that the time-consuming process of competition intervention is not aligned with the timing of market evolutions and that, as a result, enforcement might come too late, when the damage is already irreparable.[2713] Moreover, even if the GDPR has created a strict legal framework for the processing of personal data, the enforcement of the GDPR by data protection authorities is sporadic (largely due to a lack of sufficient resources), leading to negative effects not only on the individuals' right to personal data protection, but also on competition.[2714]

Therefore, while these compulsory B2B data sharing initiatives will need to determine very clear rules of the game on how to address the fundamental balancing exercises mentioned above, specific regulatory bodies will need to be appointed to apply and enforce these rules on a case-by-case basis.[2715] As this will imply a substantial workload, they will need adequate financial and human resources, as well as the necessary technical knowledge and resources, to carry out these missions. Furthermore, to ensure an efficient and harmonised enforcement across the Digital Single Market, it will be fundamental for these regulatory authorities to cooperate with, and assist, each other and to be coherent in their decisional practice. Additionally, they will need to cooperate with the data protection and competition authorities, as well as with other relevant sectoral authorities, as some overlapping issues may have to be tackled by different regulatory authorities. To be sure, the multiplication of regulatory authorities can lead to several issues that could hamper the swift enforcement of these compulsory data sharing initiatives (different degrees of enforcement; diverging or even contradicting case law; risks of overlapping "enforcement competences" and of the ensuing "regulator wars"; dilution of the application of the norms; etc).[2716] Accordingly, further research on these "enforcement design" considerations would be highly welcomed in order to identify concrete proposals that would allow to solve these issues, as without proper and

[2712] See Part II, Chapter 2, Section C, d); Part III, Chapter 3, Section B, b), 5; and Part III, Chapter 4, Section B, e).
[2713] See Part III, Chapter 1, Section E.
[2714] See Part III, Chapter 2, Section A, c).
[2715] See Part III, Chapter 3, Section B, b), 6; and Part III, Chapter 4, Section B, e).
[2716] See point 421.

efficient enforcement, it might be missed out on the numerous benefits that should result from these compulsory data sharing initiatives.

447. In conclusion, this thesis aimed to demonstrate that compulsory B2B data sharing initiatives imply fundamental economic and societal balancing exercises, which cannot be solved once and for all in the adoption process of these initiatives. Rather, addressing these balancing exercises will require to formulate the rules of these initiatives in such a way that they allow recurring checks and balances, on a case-by-case basis, in order to factor the impact that the specific circumstances of the case, the passing of time and the development of technological innovations will have on the solution to be given to these balancing exercises. The tale of the economic and societal balances underlying compulsory B2B data sharing initiatives will thus not be a short novel, but rather a continuously evolving story.

Bibliography

Legislation

International

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018, CM/Inf(2018)15-final.

Agreement on Trade-Related Aspects of Intellectual Property Rights, contained in Annex 1C to the Agreement establishing the World Trade Organisation (WTO), Marrakesh, 15 April 1994.

Berne Convention for the Protection of Literary and Artistic Works, 9 September 1886, as amended on 28 September 1979.

International Covenant on Economic, Social and Cultural Rights, 16 December 1966.

Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, securing certain rights and freedoms other than those already included in the Convention and in the first Protocol thereto, as amended by Protocol No. 11, signed in Strasbourg on 16 September 1963.

Protocol n° 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Paris on 20 March 1952.

European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950.

Universal Declaration of Human Rights, signed in Paris on 10 December 1948.

European

Treaty on European Union, *OJ C 326/13*, 26 October 2012.

Treaty on the functioning of the European Union, *OJ C 326/47*, 26 October 2012.

Protocol (No 2) on the application of the principles of subsidiarity and proportionality, *OJ C 326/206*, 26 October 2012.

Charter of Fundamental Rights of the European Union, *OJ C 326/391*, 26 October 2012.

Protocol (No 27) on the internal market and competition annexed to the Treaty on the Functioning of the European Union, *OJ C 115/309*, 9 May 2008.

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303/59*, 28 November 2018.

Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L 151/1*, 14 June 2018. See articles 61 to 66, 86 and annexes X and XI.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), *OJ L 119*, 4 May 2016.

Regulation (EU) 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, *OJ L 171/1*, 29 June 2007, articles 6 and 7.

Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings, *OJ L 24/1*, 29 January 2004.

Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, *OJ L 1/1*, 4 January 2003.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, *OJ L 172/56*, 26 June 2019.

Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, *OJ L 158/125*, 14 June 2019.

Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *OJ L 130/92*, 17 May 2019.

Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, *OJ L 111/59*, 25 April 2019.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *OJ L 321/36*, 17 December 2018.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157*, 15 June 2016.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L 337/35*, 23 December 2015.

Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, *OJ L 175/1*, 27 June 2013.

Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, *OJ L 207/1*, 6 August 2010.

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), *OJ L 108/1*, 25 April 2007.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), *OJ L 149/22*, 11 June 2005.

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ L 345/90*, 31 December 2003.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), *OJ L 108/51*, 24 April 2002.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ L 167/10*, 22 June 2001.

Directive 98/61/EC of the European Parliament and of the Council of 24 September 1998 amending Directive 97/33/EC with regard to operator number portability and carrier pre-selection, *OJ L 268/37*, 3 October 1998.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 77/20*, 27 March 1996.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281*, 23 November 1995.

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ L 122/42*, 15 May 1991.

Commission Delegated Regulation 2018/389 of 27 November 2017 supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, *OJ L 69/23*, 13 March 2018, articles 30 to 36.

Tallinn Declaration on eGovernment, 6 October 2017, available at https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration.

Decision 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector, *OJ L 318/1*, 4 December 2015.

National

Belgium

Civil Code.

Code de droit économique.

Loi du 10 décembre 2020 modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir dans le domaine de l'assurance maladie et de l'assurance individuelle sur la vie une restriction de traitement des données à caractère personnel concernant le mode de vie ou la santé issues des objets connectés, *M.B.*, 15 janvier 2021.

Loi du 4 avril 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *M.B.*, 24 mai 2019.

Loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier, *M.B.*, 4 juin 2014.

Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014.

Loi du 15 janvier 1990 organique de la Banque Carrefour de la sécurité sociale, *M.B.*, 22 février 1990.

France

Code de Commerce.

Loi n° 2016-1321 pour un république numérique du 7 octobre 2016, *J.O.*, 8 octobre 2016.

Germany

"*Gesetz gegen Wettbewerbsbeschränkungen*" (Act against Restraints of Competition, adopted on 26 August 1998 and lastly amended on 19 January 2021).

"*GWB-Digitalisierungsgesetz*" (10th amendment to the Competition Act adopted on 19 January 2021).

Preparatory works

Committee on the Internal Market and Consumer Protection of the European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)), 1 June 2021, 2020/0374(COD), available at https://www.europarl.europa.eu/doceo/document/IMCO-PR-692792_EN.pdf.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21 April 2021, COM(2021) 206 final.

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

Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM(2020) 825 final.

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final.

European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), P9_TA-PROV(2020)0272, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html.

Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast), 30 November 2016, COM/2016/0864 final.

Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/1*, 3 May 2016.

Statement of the Council's reasons: Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ C 159/83*, 3 May 2016.

Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634 final.

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 12 March 2014, *OJ C 378/399*, 9 November 2017.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM/2012/011 final.

Proposal by the Commission of the European Communities for a Council Directive on the legal protection of databases, Brussels, 13 May 1992, COM(92) 24 final.

(Belgium) Proposition de loi du 22 février 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, *Doc*., Ch., 2018-2019, n° 3595/001.

(Germany) Governmental draft bill (*GWB-Digitalisierungsgesetz*) for the 10th amendment to the Competition Act of 9 September 2020: Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen, available at https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/gwb-digitalisierungsgesetz.html.

European communications, guidelines, recommendations and staff working documents

Commission Staff Working Document, Preliminary Report – Sector inquiry into consumer internet of things, Brussels, 9 June 2021, SWD(2021) 144 final.

Commission Staff Working Document, Evaluation of the Horizontal Block Exemption Regulation, Brussels, 6 May 2021, SWD(2021) 103 final.

European Commission, Inception Impact Assessment: "*Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)*", May 2021, Ares (2021)3527151.

Communication from the Commission, Guidance on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases, Brussels, 26 March 2021, C(2021) 1959 final.

Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*", Brussels, 15 December 2020, SWD(2020) 363 final.

European Commission Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council, *OJ C 424/1*, 8 December 2020.

Commission Staff Working Document, Impact assessment report accompanying the document "*Proposal for a Regulation of the European Parliament and of the Council on*

European data governance: An enabling framework for common European data spaces (Data Governance Act)", Brussels, 25 November 2020, SWD(2020) 295 final.

European Commission, Inception Impact Assessment: "*New Competition Tool ('NCT')*", June 2020, Ares(2020)2836004.

European Commission, Inception Impact Assessment: "*Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market*", June 2020, Ares(2020)2836174.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A European strategy for data*", 19 February 2020, COM(2020) 66.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Shaping Europe's digital future*", Brussels, 19 February 2020, COM(2020) 67.

Communication from the Commission to the European Parliament and the Council, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", Brussels, 29 May 2019, COM(2019) 250 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Coordinated Plan on Artificial Intelligence*", Brussels, 7 December 2018, COM(2018) 795 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*On the road to automated mobility: An EU strategy for mobility of the future*", Brussels, 17 May 2018, COM(2018) 283.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Towards a common European data space*", Brussels, 25 April 2018, COM(2018) 232 final.

Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication "*Towards a common European data space*", Brussels, 25 April 2018, SWD(2018) 125 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Building a European Data Economy*", Brussels, 10 January 2017, COM(2017) 9 final.

Commission Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the Communication "*Building a European Data Economy*", Brussels, 10 January 2017, SWD(2017) 2 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*EU eGovernment*

Action Plan 2016-2020 - Accelerating the digital transformation of government", Brussels, 19 April 2016, COM(2016) 179 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A Digital Single Market Strategy for Europe*", Brussels, 6 May 2015, COM(2015) 192 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Towards a thriving data-driven economy*", Brussels, 2 July 2014, COM(2014) 442 final.

Communication from the Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 14 January 2011, 2011/C 11/01.

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010, available at https://rm.coe.int/16807096c3.

Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, *OJ C 45/7*, 24 February 2009.

European Commission Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings, *OJ C 265/6*, 18 October 2008.

Commission Notice on the definition of relevant market for the purposes of Community competition law, *OJ C 372/5*, 9 December 1997.

Case law

European Court of Human Rights

ECtHR, *Youth Initiative for Human Rights v. Serbia*, 25 June 2013, App. No. 48135/06.

ECtHR, *Neij and Kolmisoppi v. Sweden*, 19 February 2013, App. No. 40397/12.

ECtHR, *Ashby Donald and Others v. France*, 10 January 2013, App. No. 36769/08.

ECtHR, *Shimovolos v. Russia*, 21 June 2011, App. No. 30194/09.

ECtHR, *Roche v. United Kingdom*, 19 October 2005, App. No. 32555/96.

ECtHR, *Rotaru v. Romania*, 4 May 2000, App. No. 28341/95.

ECtHR, *McGinley and Egan v. United Kingdom*, 9 June 1998, App. No. 21825/93 and 23414/94.

ECtHR, *Guerra et al. v. Italy*, 19 February 1998, App. No. 14967/89.

ECtHR, *Hüvig v. France*, 24 April 1990, App. No. 11105/84.

ECtHR, *Kruslin v. France*, 24 April 1990, App. No. 11801/85.

ECtHR, *Sunday Times v. United Kingdom*, 26 April 1979, App. No. 6538/74.

European Court of Justice

ECJ, *Facebook v. Gegevensbeschermingsautoriteit*, 15 June 2021, C-645/19, EU:C:2021:483.

ECJ, *CV-Online Latvia*, 3 June 2021, C-762/19, EU:C:2021:434.

ECJ, *Slovak Telekom v. Commission*, 25 March 2021, C-165/19 P, EU:C:2021:239.

ECJ, *Planet 49*, 1 October 2019, C-673/17, EU:C:2019:801.

ECJ, *Peter Nowak v Data Protection Commissioner*, 20 December 2017, C-434/16, EU:C:2017:994.

ECJ, *Verlag Esterbauer*, 29 October 2015, C-490/14, EU:C:2015:735.

ECJ, *Huawei*, 16 July 2015, C-170/13, EU:C:2015:477.

ECJ, *Ryanair*, 15 January 2015, C-30/14, EU:C:2015:10.

ECJ, *Google Spain and Google*, 13 May 2014, case C-131/12, EU:C:2014:317.

ECJ, *Innoweb*, 19 December 2013, C-202/12, EU:C:2013:850.

ECJ, *AstraZeneca v Commission*, 6 December 2012, C-457/10 P, EU:C:2012:770.

ECJ, *Football Dataco e.a.*, 1 March 2012, C-604/10, EU:C:2012:115.

ECJ, *Konkurrensverket v TeliaSonera Sverige AB*, 17 February 2011, C-52/09, EU:C:2011:83.

ECJ, *Der Grüne Punkt – Duales System Deutschland v Commission*, 16 July 2009, C-385/07 P, EU:C:2009:456.

ECJ, *Directmedia Publishing*, 9 October 2008, C-304/07, EU:C:2008:552.

ECJ, *Asnef Equifax and Administración des Estado*, 23 November 2006, C-238/05, EU:C:2006:734.

ECJ, *The British Horseracing Board e.a.*, 9 November 2004, C-203/02, EU:C:2004:695.

ECJ, *IMS Health*, 29 April 2004, C-418/01, EU:C:2004:257.

ECJ, *Bronner*, 26 November 1998, C-7/97, EU:C:1998:569.

ECJ, *Tetra Pak International SA v Commission of the European Communities*, 14 November 1996, C-333/94 P, EU:C:1996:436.

ECJ, *RTE and ITP v. Commission*, 6 April 1995, joined cases C-241/91 and C-242/91, EU:C:1995:98.

ECJ, *Hilti AG v. Commission of the European Communities*, 2 March 1994, C-53/92 P, EU:C:1994:77.

ECJ, *AB Volvo v Erik Veng (UK) Ltd*, 5 October 1988, C-238/87, EU:C:1988:477.

ECJ, *Hoffmann-Laroche v. Commission*, 13 February 1979, C-85/76, EU:C:1979:36.

ECJ, *United Brands Company and United Brands Continentaal BV v. Commission*, 14 February 1978, C-27/76, EU:C:1978:22, §65

ECJ, *BRT and SABAM*, 21 March 1974, C-127/73, EU:C:1974:25.

ECJ, *Istituto Chemioterapico Italiano and Commercial Solvents v Commission*, 6 March 1974, joined cases C-6/73 and C-7/73, EU:C:1974:18.

ECJ, *Europemballage Corporation and Continental Can Company v. Commission*, 21 February 1973, C-6/72, EU:C:1973:22.

GC, *Slovak Telekom v. Commission*, 13 December 2018, T-851/14, EU:T:2018:929.

CFI, *Microsoft v. Commission*, 17 September 2007, T-201/04, EU:T:2007:289.

CFI, *IMS Health, Inc. v Commission*, 10 March 2005, T-184/01, EU:T:2005:95.

CFI, *Bayer v Commission*, 26 October 2000, T-41/96, EU:T:2000:242.

CFI, *Tetra Pak International SA v Commission of the European Communities*, 6 October 1994, T-83/91, EU:T:1994:246.

CFI, *Hilti AG v. Commission of the European Communities*, 12 December 1991, T-30/89, EU:T:1991:70.

Opinion of Advocate General Bobek in *Facebook v. Gegevensbeschermingsautoriteit* (ECJ), C-645/19, delivered on 13 January 2021, EU:C:2021:5.

Opinion of Advocate General Jacobs in *Bronner* (ECJ), C-7/97, delivered on 28 May 1998, EU:C:1998:264.

European Commission decisions

European Commission, *Google/Fitbit*, 17 December 2020, case M.9660.

European Commission, *Broadcom*, 16 October 2019, AT.40608.

European Commission, *Apple/Shazam*, 6 September 2018, case M.8788.

European Commission, *Google Android*, 18 July 2018, AT.40099.

European Commission, *Google/DoubleClick*, 11 March 2018, case M.4731.

European Commission, *Google Search (Shopping)*, 27 June 2017, AT.39740.

European Commission, *Microsoft/LinkedIn*, 6 December 2016, case M.8124.

European Commission, *Slovak Telekom*, 15 October 2014, case AT.39523.

European Commission, *Facebook/WhatsApp*, 3 October 2014, case M.7217.

European Commission, *TomTom/TeleAtlas*, 14 May 2008, case M.4854.

European Commission, *Thomson Corporation/Reuters Group*, 19 February 2008, case M.4726.

European Commission, *NDC Health/IMS Health: Interim measures*, 3 July 2001, COMP D3/38.044, *OJ L 59/18*.

European Data Protection board decisions

Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, 9 November 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf.

National decisions

Belgium

Comm. Gand (réf.), 28 octobre 2020, inéd., R.G. n°A/20/02490, commented in B. Gielen and C. Verdonck, "First Belgian ruling on abuse of economic dependence", 3 December 2020, available at https://www.lexology.com.

Autorité de Protection des Données, *X c/ Google*, 14 July 2020, decision no. 37/2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf.

Belgian Competition Authority, Decision n°BMA-2015-P/K-27-AUD, 22 September 2015, available at https://www.abc-bma.be/sites/default/files/content/download/files/2015pk27-aud-bma-pub.pdf.

France

French Cour de Cassation, case n° 02-14529, 3 March 2004.

French Cour de Cassation, cases n° 91-16988 and 91-17090, 12 October 1993.

Conseil d'État, *Société Google LLC*, 19 June 2020, case no. 430810, available at https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042040546/.

Autorité de la concurrence, Decision n°20-MC-01 (*Syndicat des éditeurs de presse v. Google*), 9 April 2020.

Autorité de la concurrence, Decision n°20-D-04, 16 March 2020.

Autorité de la concurrence, Decision n°15-A-06, 31 March 2015.

Autorité de la concurrence, Decision n°14-MC-02 (*GDF Suez*), 9 September 2014.

Autorité de la concurrence, Decision n°10-D-08, 3 March 2010.

Autorité de la concurrence, Decision n°03-D-11, 23 February 2003.

Autorité de la concurrence, Decision n°01-D-49, 31 August 2001.

Autorité de la concurrence, Decision n°99-D-54, 29 September 1999.

Autorité de la concurrence, Decision n°98-D-32, 26 May 1998.

Autorité de la concurrence, Decision n°96-D-44, 18 June 1996.

Autorité de la concurrence, Decision n°94-D-60, 13 December 1994.

Autorité de la concurrence, Decision n° 93-D-48, 9 November 1993.

Autorité de la concurrence, Decision n°91-D-51, 19 November 1991.

Autorité de la concurrence, Decision n°90-D-42, 6 November 1990.

Autorité de la concurrence, Decision n°89-D-39, 13 December 1989.

Autorité de la concurrence, Decision n°89-D-16, 30 May 1989.

Autorité de la concurrence, Decision n°87-MC-02, 25 March 1987.

Commission Nationale de l'Informatique et des Libertés, *Amazon Europe Core*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-013, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729.

Commission Nationale de l'Informatique et des Libertés, *Google LLC and Google Ireland Limited*, 7 December 2020, Deliberation of the Restricted Committee SAN-2020-012, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706.

Commission Nationale de l'Informatique et des Libertés, *Google*, 21 January 2019, Deliberation of the Restricted Committee SAN-2019-001, available at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf.

Germany

German Federal Constitutional Court, *Volkszählungsurteil*, 15 December 1983, 1 BvR 209/83 et al., 65 BVerfGE 1.

BGH, *Facebook*, 23 June 2020, KVR 69/19, no. 080/2020.

BGH, *Konditionenanpassung*, 24 September 2002, WuW/DE-R 948.

BGH, *Designer Polstermöbel*, 9 May 2000, WuW/DE-R 481.

BGH, *Depotkosmetik*, 15 May 1998, WuW/DE-R 206.

BGH, *Kfz-Vertragshändler*, 21 February 1995, WuW/E BGH 2983.

BGH, *Herstellerleasing*, 19 January 1993, WuW/E BGH 2875.

BGH, *Reparaturbetrieb*, 23 February 1988, WuW/E BGH 2479.

BGH, *Opel Blitz*, 23 February 1988, WuW/E BGH 2491.

BGH, *Cartier*, 10 November 1987, WuW/E BGH 2451.

BGH, *Adidas*, 30 June 1981, WuW/E BGH 1885.

BGH, *Sehhilfen*, 12 May 1976, WuW/E BGH 1423.

BGH, *Rossignol*, 20 November 1975, WuW/E BGH 1391.

BGH, *Kraftwagenleasing*, 30 September 1971, WuW/E BGH 1211.

Berlin Court of Appeal, *Agip II*, 7 June 1974 and 4 July 1974, WuW/E OLG 1497 and 1499.

Dusseldorf Higher Regional Court, *Facebook/Bunderskartellamt*, 26 August 2019, VI-Kart 1/19.

Bundeskartellamt (6th Division), *Facebook*, 6 February 2019, B6-22/16, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf.

Ireland

Data Protection Commission, *Twitter International Company*, 9 December 2020, decision no. IN-19-1-1, available at https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf.

Italy

Garante per la protezione dei dati personali, *Facebook*, 14 June 2019, decision no. 9121486, available at https://perma.cc/LHV7-2THY.

Autorità Garante della Concorrenza e del Mercato, *Facebook*, 29 November 2018, decision no. 27432 available at https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

Netherlands

Autoriteit Persoonsgegevens, *TikTok Inc.*, 9 April 2021, (confidential reference), available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf.

Norway

Norwegian Data Protection Authority, *Grindr LLC* (Advance notification), 24 January 2021, decision no. 20/02136-5, available at https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf.

Sweden

Datainspektionen, *Google LLC*, 10 March 2020, decision no. DI-2018-9274, available at https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf.

United Kingdom

Information Commissioner's Office, *Facebook Ireland and Facebook Inc*, 24 October 2018, available at https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf.

United States of America

Supreme Court of the United States, *Verizon Communications v Law Offices of Curtis V. Trinko*, 2004, *LLP*, 540 US 398.

Supreme Court of the United States, *United States v Terminal Railroad Association of St. Louis*, 1912, 224 US 383.

United States Court of Appeals for the Ninth Circuit, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-16783, WL 4251889, 9 September 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html.

United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, case No. 17-CV-03301-EMC, 2020 WL 5408210, 9 September 2020.

United States District Court, Northern District of California, *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-cv-03301-EMC, 14 August 2017, available at https://epic.org/amicus/cfaa/linkedin/2017-08-15-PI-Order.pdf.

Superior Court of the State of California, *PeopleBrowsr, Inc. et al. v. Twitter, Inc. (PeopleBrowsr)*, No. C-12-6120 EMC, 2013 WL 843032, N. D. Cal., 6 March 2013.

References

Books

Adler, M.J., *A Guidebook to Learning: For a Lifelong Pursuit of Wisdom*, London, Macmillan, 1986.

Benkler, Y., *The Wealth of Networks. How Social Production transforms Markets and Freedom*, New Haven, Yale University Press, 2003.

Blackstone, W., *Commentaries on the Laws of England*, Book 2, Chapter 1, Oxford, Oxford University Press, 1771, available at https://avalon.law.yale.edu/18th_century/blackstone_bk2ch1.asp.

Bollier, D. and Helfrich, S., *Free, Fair and Alive. The Insurgent Power of the Commons*, Gabriola Island, New Society Publishers, 2019.

Bonnecase, J., *Précis de droit civil*, 2e éd., Paris, Rousseau, 1938, t. I.

Buydens, M., *Droits des brevets d'invention*, 2e éd., Bruxelles, Larcier, 2020.

Catala, P., *Le droit à l'épreuve du numérique. Jus ex machina*, Paris, PUF, 1998.

Christensen, C., *The Innovator's Dilemma. When New Technologies Cause Great Firms to Fail*, Boston, Harvard Business School Press, 1997.

Christensen, C. and Raynor, M., *The Innovator's Solution: Creating and Sustaining Successful Growth*, Boston, Harvard Business School Press, 2003.

De Boüard, F., *La dépendance économique née d'un contrat*, Paris, LGDJ, 2007.

De Visscher, F. et Michaux, B., *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000.

Degrave, E., *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier - Collection du CRIDS, 2014.

Drahos, P., *Intellectual Property, Indigenous People and their Knowledge*, Cambridge University Press, 2014.

Dubuisson, F., *Existe-t-il un principe general d'appriopriation de l'information?*, Thèse de doctorat, Université Libre de Bruxelles, 2005.

Durant I., *Droit des biens*, Bruxelles, Larcier, 2017.

Dworkin, G., *The Theory and Practice of Autonomy*, Cambridge, Cambridge University Press, 1988.

Ehrlich, P., *The Population Bomb*, New York, Ballantine Books, 1968.

Elhauge, E. and Geradin, D., *Global Antitrust Law and Economics*, Third Edition, St. Paul, Foundation Press, 2018.

Elkin-Koren, N. and Salzberger, E., *The Law and Economics of Intellectual Property in the Digital Age: The limits of the analysis*, London, Routledge, 2013.

Ergec, R., *Protection européenne et internationale des droits de l'homme*, Bruxelles, Larcier, 2014.

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union, 2018.

Feteira, L., *The Interplay between European and National Competition Law after Regulation 1/2003*, Alphen aan den Rijn, Kluwer, 2016.

Fisher, M., *Fundamentals of Patent Law: Interpretation and Scope of Protection*, Oxford, Hart Publishing, 2007.

Floridi, L., *Information: A Very Short Guide*, Oxford, Oxford University Press, 2010.

Frischmann, B., *Infrastructure: The Social Value of Shared Resources*, Oxford, Oxford University Press, 2012.

Gansey, P., *Thinking About Property: From Antiquity to the Age of Revolution*, Cambridge, Cambridge University Press, 2007.

Geradin, D., Layne-Farrar, A. and Petit, N., *EU Competition Law and Economics*, Oxford, Oxford University Press, 2012.

Graef, I. *EU competition law, data protection and online platforms: data as essential facility*, Alphen aan den Rijn, Kluwer, 2016.

Grotius, H., *De Iure Belli ac Pacis*, 1625.

Halbert, D., *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*, Westport, Quorum books, 1999.

Hobbes, T., *Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil*, 1651.

Jones, A. and Sufrin, B., *EU Competition Law. Text, Cases, and Materials*, 4th ed., Oxford, Oxford University Press, 2011.

Kitchin, R., *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, London, Sage Publications, 2014.

Kohn, A., *Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, A's, Praise, and Other Bribes*, Boston, Houghton Mifflin, 1999.

Kramer, M., *John Locke and the Origins of Private Property*, Cambridge, Cambridge University Press, 1997.

Locke, J., *Two Treatises of Government: In the Former, The False Principles, and Foundation of Sir Robert Filmer, and His Followers, Are Detected and Overthrown. The Latter Is an Essay Concerning The True Original, Extent, and End of Civil Government*, London, Awnsham Churchill, 1690.

Mattei, U. and Quarta, A., *The Turning Point in Private Law. Ecology, Technology and the Commons*, Cheltenham, Edward Elgar, 2019.

Mattei, U., Reviglio, E. and Rodotà, S. (eds.), *I beni pubblici. Dal governo democratico dell'economia alla riforma del codice civile*, Rome, Accademia Nazionale dei Lincei, 2010.

Mattei, U., Reviglio, E. and Rodotà, S. (eds.), *Invertire la rotta. Idee per una riforma della proprietà pubblica*, Bologna, Il Mulino, 2007.

Mayer-Schonberger, V. and Ramge, T., *Re-inventing capitalism in the age of big data*, New York, Basic Books, 2018.

OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019, available at https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.

OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications, Paris, 2015, available at https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm.

Olson, M., *The Logic of Collective Action: Public Goods and the Theory of Groups*, Harvard University Press, 1965.

Ostrom, E., *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge, Cambridge University Press, 1990.

Pasquale, F., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, Harvard University Press, 2015.

Posner, R., *Economic Analysis of Law*, Boston, Little Brown, 1973.

Schlatter, R., *Private Property: the History of an Idea*, New Brunswick, Rutgers University Press, 1951.

Schumpeter, J., *The Theory of Economic Development: an Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*, Harvard University Press, 1932.

Smith, A., *An Inquiry into the Nature and Causes of the Wealth of Nations*, London, 1776.

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

Sulija, G., *Standard Contract Terms in Cross-Border Business Transactions – A Comparative Study from the Perspective of European Union Law*, Frankfurt am Main, Peter Lang, 2011.

Sunstein, C., *Why Societies Need Dissent*, Cambridge, Harvard University Press, 2003.

Turow, J., *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, New Haven, Yale University Press, 2017.

von Baeyer, H., *Information: The New Language of Science*, Canbridge, Harvard University Press, 2003.

Weinberger, D., *Too Big to Know*, New York, Basic Books, 2011.

Whish, R. and Bailey, D., *Competition Law*, 7th ed., Oxford, Oxford University Press, 2012.

Windscheid, B., *Lehrbuch des Pandektenrechts*, 3 volumes, Frankfurt am Mein, Rutten & Loening, 1891.

Zuboff, S., *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, New York, PublicAffairs, 2019.

Book Chapters

Aplin, T., "Subject matter", *Research Handbook on the Future of EU Copyright*, E. Derclaye (ed.), Cheltenham, Edward Elgar, 2009, p. 49-76.

Arrow, K., "Economic Welfare and the Allocation of Resources for Invention", *The Rate and Direction of Inventive Activity: Economic and Social Factors*, National Bureau of Economic Research (ed.), 1962, p. 609-626.

Bart, J., "Res communes omnium, res nullius, res publicae, res universatis", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 1052-1054.

Boy, L., "Abuse of market power: controlling dominance or protecting competition?", *The Evolution of European Competition Law: whose Regulation, which Competition?*, H. Ullrich (ed.), Cheltenham and Northampton, Edward Elgar, 2006, p. 201-223.

Burrel, R. and Coleman, A., *Copyright Exceptions: The Digital Impact*, Cambridge, Cambridge University Press, 2005.

Bygrave, L. and Tosoni, L., "Article 4(11). Consent", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 174-187.

Carrier, M.A., "Limiting copyright through property", *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 185-204.

Chaigneau, A., "Propriété collective", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 954-957.

Chrocziel, P. and Prinz zu Waldeck und Pyrmont, W., "Introduction", *Intellectual Property and Competition Law*, P. Chrocziel, M. Lorenz and W. Prinz zu Waldeck und Pyrmont (ed.), Alphen aan den Rijn, Kluwer, 2016, p. 1-32.

Cortese, F., "What are common goods (beni comuni)? Pictures from the Italian debate", *Revista da Faculdade de Direito da UFMG – N° Especial 2nd Conference Brazil-Italy*, 2017, p. 121 – 146.

De Hert, P., "Artikel 8. Recht op privacy", *Handboek EVRM, Deel 2. Artikelsgewijze commentaar*, J. Vande Lanotte and Y. Haeck (ed.), Antwerp, Intersentia, 2004, p. 705-788.

de Terwangne, C., "Article 5. Principles relating to processing of personal data", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 309-320.

de Terwangne, C., “Droit à la vie privée: un droit sur l'information et un droit à l'information”, *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 555-579.

de Terwangne, C., “Définitions clés et champ d’application du RGPD”, *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 59-84.

de Terwangne, C., “Les principes relatifs au traitement des données à caractère personnel et à sa licéité”, *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 87-142.

de Terwangne, C., “La réforme de la Convention 108 du Conseil de l’Europe pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel”, *Quelle protection des données personnelles en Europe?*, C. Castets-Renard (dir.), Bruxelles, Larcier, 2015, p. 81-120.

Derclaye, E., “Introduction”, *Research Handbook on the Future of EU Copyright*, E. Derclaye (ed.), Cheltenham, Edward Elgar, 2009, p. 1-11.

Dreier, T., “How much “property” is there in intellectual property? The German civil law perspective”, *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 116-136.

Dusollier, S., “Du commun de l’intelligence artificielle”, *Penser le droit de la pensée. Mélanges en l’honneur de Michel Vivant*, Paris, Dalloz, 2020, p. 107-120.

Dusollier, S. et Rochfeld, J., “Propriété inclusive ou inclusivité”, *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 983-987.

Dusollier, S., “The commons as a reverse intellectual property - from exclusivity to inclusivity”, *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 258-281.

Emerich, Y., “Propriété exclusive ou exclusivité”, *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 979-983.

Evans, D. and Schmalensee, R., “Some Economic Aspects of Antitrust Analysis in Dynamically Competitive Industries”, *Innovation Policy and the Economy*, Volume 2, A. Jaffe, J. Lerner and S. Stern (eds.), Cambridge, MIT Press, 2002, p. 1-49.

Flanagan, A. and Montagnani, M., “Intellectual property law: economic and social justice perspectives: introduction”, *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. x-xviii.

Gutwirth, S. et Gonzalez Fuster, G., “L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre”, *Law, norms and freedom in cyberspace – Liber Amicorum Yves*

Poullet, E. Degrave, C. de Terwangne, S. Dusollier and R. Queck (ed.), Bruxelles, Larcier, 2018, p. 117-140.

Haucap, J., "A German approach to antitrust for digital platforms", *Digital Platforms and Concentration, Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (ed.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 8-13.

Helfer, L., "Mapping the interface between human rights and intellectual property", *Research Handbook on Human Rights and Intellectual Property*, C. Geiger (ed.), Cheltenham, Edward Elgar, 2015, p. 6-15.

Hugenholtz, B., "Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 75-99

Kerber, W., "Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective", *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (ed.), Baden-Baden, Nomos, 2017, p. 109-133.

Khan, L., "What makes tech platforms so powerful?", *Digital Platforms and Concentration, Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (ed.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 14-17.

Knockaert, M. and Tombal, T., "Quels droits sur les données?", *Actualites en droit du numerique*, H. Jacquemin and B. Michaux (ed.), Limal, Anthémis, 2019, p. 53-97.

Kosta, E., "Article 7. Conditions for consent", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 345-354.

Kotschy, W., "Article 6. Lawfulness of processing", *The EU General Data Protection Regulation (GDPR): A Commentary*, C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 321-344.

Lametti, D., "The Concept of the Anticommons: Useful, or Ubiquitous and Unnecessary?", *Concepts of Property in Intellectual Property Law*, H.R. Howe and J. Griffiths (ed.), Cambridge, Cambridge University Press, 2013, p. 232-257.

Leclercq, P., "Essai sur le statut juridique des informations", *Les flux transfrontières de données: vers une économie internationale de l'information?*, A. Madec (ed.), Paris, La Documentation française, 1982, p. 119-150.

Lomfeld, B., "Fondements de la propriété (Théories de la propriété)", *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 566-569.

Martinelli, S., “Sharing data and privacy in the platform economy: the right to data portability and “porting rights””, *Regulating New Technologies in Uncertain Times*, L. Reins (ed.), The Hague, T.M.C. Asser Press, 2019, p. 133-152.

Michaux, B., “Diffusion du savoir: droit d'auteur et Internet”, *L'Europe des droits de l'homme à l'heure d'Internet,* Q. Van Enis et C. de Terwangne (dir.), Bruxelles, Larcier, 2019, p. 491-526.

Morando, F., “Copyright default rule: reconciling efficiency and fairness”, *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. 24-43.

Polčák, R., “Article 12. Transparent information, communication and modalities for the exercice of the rights of the data subject”, *The EU General Data Protection Regulation (GDPR): A Commentary,* C. Kuner, L. Bygrave and C. Docksey (eds.), Oxford, Oxford University Press, 2020, p. 398-412.

Pothier, R.J., “Traité de la propriété”, *Œuvres de R.-J. Pothier*, D. Ainé (ed.), tome V, Bruxelles, Tarlier, 1831.

Quaedvlieg, A., “Overlap/relationships between copyright and other intellectual property rights”, *Research Handbook on the Future of EU Copyright*, E. Derclaye (ed.), Cheltenham, Edward Elgar, 2009, p. 480-516.

Ramello, G., “Intellectual property, social justice and economic efficiency: insights from law and economics”, *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. 1-23.

Régibeau, P. and Rockett, K., “The relationship between intellectual property law and competition law: an economic approach”, *The Interface between Intellectual Property Rights and Competition Policy*, S. Anderman (ed.), Cambridge, Cambridge University Press, 2007, p. 505-552.

Rouvroy, A., “*Homo juridicus* est-il soluble dans les données ?”, *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), Bruxelles, Larcier, 2018, p. 417-444.

Rouvroy, A. and Poullet, Y., “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy”, *Reinventing Data Protection: Proceedings of the International Conference (Brussels, 12-13 October 2007)*, Dordrecht, Springer, 2009, p. 45-76.

Salord, G., “Propriété commune”, *Dictionnaire des biens communs*, M. Cornu, F. Orsi et J. Rochfeld (dir.), Paris, Presses universitaires de France, 2017, p. 960-964.

Sandeen, S., “The value of irrationality in the IP equation”, *Intellectual Property Law: Economic and Social Justice Perspectives*, A. Flanagan and M. Montagnani (ed.), Cheltenham, Edward Elgar, 2010, p. 44-65.

Strowel, A., “Big Data and Data Appropriation in the EU”, *Research Handbook on Intellectual Property and Digital Technologies*, T. Aplin (ed.), Camberley, Edward Elgar, 2020, p. 107-135.

Tombal, T., "The GDPR: A Shield to a Competition Authority's Data Sharing Remedy?", *Deep Diving into Data Protection*, J. Herveg (coord.), Bruxelles, Larcier, 2021, p. 67-94.

Tombal, T., “Les droits de la personne concernée dans le RGPD”, *Le Règlement general sur la protection des données (RGPD / GDPR) – Analyse approfondie*, C. De Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 407-558.

Van Overwalle, G., “Inventing Inclusive Patents: From Old to New Open Innovation”, *Kritika: Essays on Intellectual Property*, P. Drahos, G. Ghidini and H. Ullrich (ed.), Vol. 1, Cheltenham, Edward Elgar, 2015, p. 206-277.

Voorhoof, D., “Freedom of expression and the right to information: Implications for copyright”, *Research Handbook on Human Rights and Intellectual Property*, C. Geiger (ed.), Cheltenham, Edward Elgar, 2015, p. 331-353.

Wendehorst, C., “Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy”, *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer, (ed.), Baden-Baden, Nomos, 2017, p. 327-355.

Zech, H., “Data as tradeable commodity”, *European Contract Law and the Digital Single Market*, A. De Franceschi (ed.), Cambridge, Intersentia, 2016, p. 51-79.

Papers in scientific journals

Abrahamson, Z., “Essential Data”, *The Yale Law Journal*, 2014, vol. 124, n° 3, p. 867-881.

C. Ahlborn, C. and D. Evans, “The Microsoft Judgment and its Implications for Competition Policy Towards Dominant Firms in Europe”, *Antitrust Law Journal*, 2009, Volume 75, Issue 3, p. 887-932.

Albors-Llorens, A., “The "Essential Facilities" Doctrine in EC Competition Law”, *The Cambridge Law Journal*, 1999, p. 490-492.

Argenton, C. and Prüfer, J., “Search engine competition with network externalities”, *Journal of Competition Law and Economics*, 2012, Vol. 8(1), p. 73-105.

Auf’mkolk, H., “The “Feedback Effect” of Applying EU Competition Law to Regulated Industries: Doctrinal Contamination in the Case of Margin Squeeze”, *Journal of European Competition Law & Practice*, 2012, Vol. 3, Issue 2, p. 149-162.

Azzopardi, A., “No abuse is an island: the case of margin squeeze”, *European Competition Journal*, 2017, Vol. 13, Issue 2-3, p. 228-248.

Bagnoli, V., “Digital Platforms as Public Utilities”, *IIC*, 2020, Volume 51, Issue 8, p. 903-905.

Ben-Shahar, O., “Data pollution”, *Journal of Legal Analysis*, 2019, Volume 11, p. 104-159.

Bergman, M., “The Bronner Case - A Turning Point for the Essential Facilities Doctrine?”, *European Competition Law Review*, 2000, p. 59-63.

Besen, S. and Verveer, P., “Competition and data: Potential remedies”, *Wake Forest Journal of Business and Intellectual Property Law*, 2021, Volume 21, Number 2, p. 103-143.

Botta, M. and Wiedemann K., “The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey”, *Antitrust Bulletin,* vol. 64, issue 3, 2019, p. 428-446.

Bower J. and Christensen, C., “Disruptive Technologies: Catching the Wave”, *Harvard Business Review*, 1995, Volume 73, Issue 1, p. 43-53.

Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T. and Van Alstyne, M., “The EU Digital Markets Act: A Report from a Panel of Economic Experts”, *EU Science Hub*, 2021, available at https://ec.europa.eu/jrc/en/publication/eu-digital-markets-act.

Calo, R., “Digital market manipulation”, *George Washington Law Review*, 2014, Volume 82, Issue 4, p. 995-1051.

Calvet, H. et Desurmont, T., “L’arrêt Magill: Une decision d’espèce?”, *R.I.D.A.*, 1996, n° 167, p. 3-67.

Campbell, J., Goldfarb, A. and Tucker, C. “Privacy Regulation and Market Structure”, *Journal of Economics & Management Strategy*, vol. 24, issue 1, 2015, p. 47-73.

Carbonell, I., “The ethics of big data in big agriculture”, *Internet Policy Review*, 2016, Issue 5(1), p. 1-13, available at https://policyreview.info/articles/analysis/ethics-big-data-big-agriculture.

Colangelo, G. and Maggiolino, M., “Big data as misleading facilities”, *European Competition Journal*, 2017, Issue 13, Vol. 2-3, p. 249-281.

Crowther, P., “Compulsory Licensing of Intellectual Property Rights”, *European Law Review*, 1995, p. 521-528.

Dawes, R.M., “The commons dilemma game: An N-person mixed motive game with a dominating strategy for defection”, *Organ. Res. Inst. Res. Bull*., 13(2), 1973, p. 1-12.

De Bot, D., “De uitvoering van de algemene verordening gegevensbescherming – enkele bemerkingen bij de Belgische context”, *T.V.W.*, 2016/3, p. 218-234.

De Bure, F. and Bary, L., “Disruptive Innovation and Merger Remedies: How to Predict the Unpredictable?”, *Concurrence*, September 2017, N° 3-2017, Art. N° 84407.

de la Mano, M. and Padilla, J., “Big Tech Banking”, *Journal of Competition Law & Economics*, 2018, Issue 14(4), p. 494–526.

de Montjoye, Y.-A., Gambs, S., Blondel, V., Canright, G., de Cordes, N., Deletaille, S., Engø-Monsen, K., Garcia-Herranz, M., Kendall, J., Kerry, C., Krings, G., Letouzé, E., Luengo-Oroz, M., Oliver, N., Rocher, L., Rutherford, A., Smoreda, Z., Steele, J., Wetter, E., Pentland,

A. and Bengtsson, L., “Comment: On the privacy-conscientious use of mobile phone data”, *Scientific Data*, 2018, Issue 5, available at https://www.nature.com/articles/sdata2018286.

de Streel, A. and Larouche, P., “The European Digital Markets Act proposal: How to improve a regulatory revolution”, *Concurrences*, 2021, N° 2, p. 46-63.

Deci, E., Koestner, R. and Ryan, R., “A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation”, *Psychological Bulletin*, 1999, Volume 125, Issue 6, p. 627–668.

Delacroix, S. and Lawrence, N., “Bottom-Up Data Trusts: Disturbing the ‘One Size Fits All’ Approach to Data Governance”, *International Data Privacy Law*, November 2019, Volume 9, Issue 4, p. 236-252.

Derclaye, E., “The IMS Health decision and the Reconciliation of Copyright and Competition”, *European Law Review*, 2004, Volume 29, Issue 5, p. 687-697.

Derclaye, E., “Databases sui generis right: should I adopt the spin off theory?”, *E.I.P.R.*, 2004, Issue 26(9), p. 402-413.

Detroux, G. et George, F., “La protection des données à caractère personnel dans le cadre d’une faillite”, *J.T.*, 2019, n°6783, p. 577-592.

Diker Vanberg, A. and Ünver, M., “The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?”, *European Journal of Law and Technology*, 2017, Vol. 8, Issue 1, p. 1-22.

Drexl, J., “IMS Health and Trinko - Antitrust Placebo for Consumers Instead of Sound Economics in Refusal-to-Deal Cases”, *International Review of Industrial Property and Copyright Law*, 2004, p. 788-808.

Ducuing, C., “Data as infrastructure? A study of data sharing legal regimes”, *Competition and Regulation in Network Industries*, Vol. 21, Issue 2, 2020, p. 124–142.

Eisenmann, T., Parker, G. and Van Alstyne, M., “Platform Envelopment”, *Strategic Management Journal*, 2011, Vol. 32(12), p. 1270–1285.

Engels, B., “Data portability among online platforms”, *Internet Policy Review*, 2016, Vol. 5, Issue 2, available at https://policyreview.info/articles/analysis/data-portability-among-online-platforms.

Ezrachi, A. and Robertson, V., “Competition, Market Power and Third-Party Tracking”, *World Competition: Law and Economics Review*, 2019, Vol. 42, No. 1, p. 5-19.

Fairfield, J.A. and Engel, C., “Privacy as a public good”, *Duke Law Journal*, 2015, Volume 65, Issue 3, p. 385-457.

Feeny, D., Berkes, F., McCay, B. and Acheson, J., “The Tragedy of the Commons. Twenty-Two Years Later”, *Human Ecology*, 1990, Volume 18, Issue 1, p. 1-19.

Frischmann, B., Marciano, A. and Ramello, G., “Retrospectives: Tragedy of the Commons After 50 Years”, *Journal of Economic Perspectives*, 2019, Volume 33, Issue 4, p. 211-228.

Gal, M. and Aviv, O., "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*, September 2020, Volume 16, Issue 3, p. 349-391.

Gal, M. and Rubinfeld, D. "Data Standardization", *New York University Law Review*, 2019, Vol. 94, Number 4, p. 737-770.

Gaullier, F., "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *Communication commerce électronique*, 2018/4, p. 45-52.

Graef, I., "Paving the Way Forward for Data Governance: a Story of Checks and Balances", *Technology and Regulation*, Special issue: Governing Data as a Resource, 2020, p. 24-28.

Graef, I., "Rethinking the Essential Facilities Doctrine for the EU Digital Economy", *RJTUM*, 2019, Vol. 53, p. 33-72.

Graef, I., "Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence", *Yearbook of European Law*, 2019, p. 1-52.

Graef, I., "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition Law and Economics Review*, 2015, Vol. 38, Issue 4, p. 473–506.

Graef, I., "Tailoring the Essential Facilities Doctrine to the IT Sector: Compulsory Licensing of Intellectual Property Rights after Microsoft", *Cambridge Student Law Review*, 2011, Volume 7, Issue 1, p. 1-20.

Graef, I. and Van Berlo, S., "Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility", *European Journal of Risk Regulation*, November 2020, available at https://doi.org/10.1017/err.2020.92.

Graef, I., Husovec, M. and Purtova, N., "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *German Law Journal*, 2018, Issue 19(6), p. 1359-1398.

Graef, I., Wahyuningtyas, S. and Valcke, P., "Assessing data access issues in online platforms", *Telecommunications Policy*, 2015, Vol. 39, p. 375-387.

Graham, C. and Morton, J., "Latest Developments in Standards, Patents and FRAND licensing", *E.I.P.R.*, 2014, Vol. 36, Issue 11, p. 700-706.

Gutwirth, S. et Stengers, I., "Le droit à l'épreuve de la résurgence des *commons*", *Revue Juridique de l'environnement*, 2016/2, Vol. 41, p. 306-343.

Hahn, I., "Purpose Limitation in the time of Data Power: Is there a way forward?", *European Data Protection Law Review*, 2021, Volume 7, Issue 1, p. 31-44.

Hardin, G., "The Tragedy of the Commons", *Science*, December 1968, Vol. 162, Issue 3859, p. 1243-1248.

Heller, M., "The Tragedy of the Anticommons: Property in the Transition from Marx to Markets", *Harvard Law Review*, January 1998, Vol. 111, n° 3, p. 621-688.

Hoeren, T., "A New Approach to Data Property?", *A.M.I.*, 2018/2, p. 58-60.

Hoeren, T. and Bitter, P., “Data ownership is dead: long live data ownership”, *E.I.P.R.*, 2018, 40(6), p. 347-348.

Howarth, D. and McMahon, K., “"Windows has Performed an Illegal Operation": the Court of First Instance's Judgment in Microsoft v Commission”, *European Competition Law Review*, 2008, p. 117-134.

Këllezi, P., “Data protection and competition law: non-compliance as abuse of dominant position”, *Sui-generis*, 2019, p. 343-359.

Kerber, W., “Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data”, *JIPITEC*, 2018, Issue 9, p. 310-331.

Kerber, W., “Governance of Data: Exclusive Property vs. Access”, *IIC*, 2016, Volume 47, Issue 7, p. 759-762.

Kerber, W. and Gill, D., “Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation”, *JIPITEC*, 2019, Issue 10, p. 244-256.

Khan, L., “Amazon’s Antitrust Paradox”, *Yale Law Journal*, 2017, Volume 126, Number 3, p. 710-805.

Kim, D., “No one’s ownership as the status quo and a possible way forward: A note on the public consultation on Building a European Data Economy”, *Journal of Intellectual Property Law & Practice*, 2018, Volume 13(2), p. 154-165.

Kosta, E., “Construing the Meaning of 'Opt-Out': An Analysis of the European, U.K. and German Data Protection Legislation”, *European Data Protection Law Review*, 2015, Vol. 1, p. 16-31.

Krämer, J., Schnurr, D. and Wohlfarth, M., “Winners, losers, and facebook: The role of social logins in the online advertising ecosystem”, *Management Science*, 2019, Vol. 65(4), p. 1678-1699.

Langer, J., “The Court of First Instance's Microsoft Decision: Just an Orthodox Ruling in an On-Orthodox Case”, *Legal Issues of Economic Integration*, 2008, p. 183-195.

Larouche, P., “The European Microsoft case at the crossroads of competition policy and innovation”, *Antitrust Law Journal*, 2008, n° 75, p. 933-963.

Ledger, M. et Tombal, T., "Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ?", *R.D.T.I.*, 2018/3, n°72, p. 25-44.

Lundqvist, B., “Competition and Data Pools”, *Journal of European Consumer and Market Law*, 2018, p. 146-154.

MacCarthy, M., “New directions in privacy: Disclosure, unfairness and externalities”, *Journal of Law and Policy for the Information Society*, 2011, Volume 6, p. 425–512.

Madison, M., “Tools for Data Governance”, *Technology and Regulation*, 2020, p. 29-43.

Martens, B., de Streel, A., Graef, I., Tombal, T. and Duch-Brown, N., “Business to business data sharing: an economic and legal analysis”, *EU Science Hub*, 2020, available at https://ssrn.com/abstract=3658100.

Masson, A., “Creation of database or creation of data: crucial choices in the matter of database protection”, *E.I.P.R.*., 2006, Volume 28, Issue 5, p. 261-267.

Mayer-Schönberger, V. and Padova, Y., “Regime change? Enabling Big Data through Europe’s new Data Protection Regulation”, C*olumbia Science & Technology Law Review*, Vol. XVII, 2016, p. 315-335.

Meinberg, H., “From Magill to IMS Health: the new product requirement and the diversity of intellectual property rights”, *E.I.P.R.*, 2006, Volume 28, Issue 7, p. 398-403.

Merrill, T., “Property and the Right to Exclude”, *Nebraska Law Review*, Volume 77, Issue 4, 1998, p. 730-755.

Michaux, B., “La Cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ?”, note sous C.J.U.E., 29 octobre 2015, C-490/14, *Auteurs et Média*, 2017, Issue 1, p. 28-34.

Miller, A. and Tucker, C., “Health information exchange, system size and information silos”, *Journal of Health Economics*, Vol. 33(2), 2014, p. 28-42.

Moldén, R., “Mandatory Supply of Interoperability Information: The Microsoft Judgment”, *European Business Organization Law Review*, 2008, p. 305-334.

Mousseron, J.-M. et Vivant, M., “Les mécanismes de réservation et leur dalectique: Le «terrain» occupé par le droit”, *Semaine Juridique, Cahiers de Droit de l'Entreprise,*1989/1, p. 2-4.

Ohm, P., “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization”, *UCLA Law Review*, Volume 57, 2010, p. 1701-1777.

Ong, B., “Anti-competitive refusals to grant Copyright Licences : reflections on the IMS Saga”, *E.I.P.R.*, 2004, Volume 26, Issue 11, p. 505-514.

Petit, N., “L’arrêt Microsoft. Abus de position dominante, refus de licence et vente liée...-l’article 82 sans code source”, *Journal de droit européen*, 2008, p. 8-12.

Picht, P., “Towards an Access Regime for Mobility Data”, *IIC*, 2020, Volume 51, Issue 8, p. 940-976.

Pielaet, P.-O., “La *privacy by design* à l’épreuve des « dark patterns »”, *R.D.T.I.*, 2020, Issue 3, p. 33-45.

Purtova, N., “The law of everything. Broad concept of personal data and future of EU data protection law”, *Law, Innovation and Technology*, 2018, Vol. 10, Issue 1, p. 40-81.

Richter, H. and Slowinski, P. “The Data Sharing Economy: On the Emergence of New Intermediaries”, *IIC*, 2019, Volume 50, Issue 1, p. 4-29.

Robertson, A., “The Existence and Exercise of Copyright: Can it Bear the Abuse?”, *The Law Quarterly Review*, 1995, p. 588-591.

Robertson, V., “Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data”, *Common Market Law Review*, 2020, Vol. 57, p. 161–189.

Rocher, L., Hendrickx, J. and de Montjoye, Y.-A., "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, 2019, Vol. 10, n°3069, available at https://www.nature.com/articles/s41467-019-10933-3.

Rouvroy, A. and Stiegler, B., "The Digital Regime of Truth: From Algorithmic Governmentality to a New Rule of Law", *Online Journal of Philosophy*, 2016, Number 3, p. 6-29.

Rouvroy, A. et Berns, T., "Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?", *Réseaux*, 2013, Volume 177, Issue 1, p. 163-196.

Rubinfeld, D. and Gal, M., "Access Barriers to Big Data", *Arizona Law Review*, 2017, vol. 59, p. 339-381.

Sanfilippo, M., Frischmann, B. and Standburg, K., "Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework", *Journal of Information Policy*, 2018, Vol. 8, p. 116-166.

Shkabatur, J., "The Global Commons of Data", *Stanford Technology Law Review*, 2019, Vol. 22, p. 354-411.

Spina Ali, G., "Intellectual Property and Human Rights: A Taxonomy of Their Interactions", *IIC*, 2020, Volume 51, Issue 4, p. 411–445.

Somaini, L., "Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability", *EDPL*, 2020/1, p. 84-93.

Somaini, L., "The right to data portability and user control: ambitions and limitations", *MediaLaws – Rivista dir. media*, 2018/3, p. 164-190.

Stern, R., "What are Reasonable and Non-discriminatory Terms for licensing a Standard-essential Patent?", *E.I.P.R.*, 2015, Vol. 37, Issue 9, p. 549-557.

Stothers, C., "IMS Health and its implications for Compulsory Licensing in Europe", *E.I.P.R.*, 2004, Volume 26, Issue 10, p. 467-472.

Sweeney, L., "Weaving Technology and Policy Together to Maintain Confidentiality", *Journal of Law, Medicine & Ethics*, 1997, Vol. 25, Issues 2 & 3, p. 98-110.

Swire, P. and Lagos, Y., "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique", *Maryland Law Review*, 2013, Vol. 72/3, p. 335-380.

Taylor, S., "Copyright versus Right to Compete - The Judgment of the ECJ in Magill", *Computer and Telecommunications Law Review*, 1995, p. 99-102.

Thomas, L. and Leiponen, A., "Big Data Commercialization", *IEEE Engineering Management Review*, 2016, Volume 44(2), p. 74-90.

Treacy, P., "Essential Facilities - Is the Tide Turning?", *European Competition Law Review*, 1998, p. 501-505.

Tombal, T., "Economic dependence and data access", *IIC*, 2020, Volume 51, Issue 1, p. 70-98.

Van der Wal, G., "Article 86 EC: The Limits of Compulsory Licensing", *European Competition Law Review*, 1994, p. 230-235.

Vinje, T., "The final word on Magill: the judgement of the E.C.J.", *E.I.P.R.*, 1995, Volume 17, Issue 6, p. 297-303.

Waldron, J., "From Authors to Copiers: Individual Rights and Social Values in Intellectual Property", *Chi.-Kent L. Rev.*, 1993, Vol. 68, p. 841-887.

Weibe, A., "Protection of industrial data - a new property right for the digital economy?", *Journal of Intellectual Property Law & Practice*, 2017, Vol. 12, n° 1, p. 62-71.

Wiedemann, K., "A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)", *IIC*, 2020, Volume 51, Issue 9, p. 1168-1181.

Wils, W., "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt", *Concurrences*, 2019, issue 3, p. 58-66.

Wooldridge, F., "The Essential Facilities Doctrine and Magill II: The Decision of the ECJ in Oscar Bronner", *Intellectual Property Quarterly*, 1999, p. 256-264.

Zarsky, T., "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review*, 2017, Vol. 47, No. 4(2), p. 995-1020.

Zarsky, T., "The Privacy–Innovation Conundrum", *Lewis & Clark Law Review*, 2015, Vol. 19, No. 1, p. 115-168.

Zelany, M., "Management support systems: towards integrated knowledge management", *Human Systems Management*, 1987, Volume 7, p. 59-70.

Conference papers

Hugenholtz, B., "Program Schedules, Event Data and Telephone Subscriber Listings under the Database Directive--The 'Spin-Off' Doctrine in the Netherlands and elsewhere in Europe", *Paper presented at 11th Annual Conference on International Intellectual Property Law and Policy, Fordham University School of Law, New York, April 14-25*, 2003, available at https://www.ivir.nl/publicaties/download/spinofffordham.pdf.

Lee, S. and Schißler, J., "Platform Dependence and Exploitation", *Paper presented at the 14th ASCOLA Conference*, June 2019, available at https://ssrn.com/abstract=3403002.

Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L., "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", *CHI Conference on Human Factors in Computing Systems*, April 2020, available at https://arxiv.org/abs/2001.02479.

Okoyomon, E., Samarin, N., Wijesekera, P., Elazari Bar On, A., Vallina-Rodriguez, N., Reyes, I., Feal, A. and Egelman, S., "On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies", *The Workshop on Technology and Consumer*

Protection, 2019, available at https://blues.cs.berkeley.edu/blog/2019/05/10/on-the-ridiculousness-of-notice-and-consent-contradictions-in-app-privacy-policies-conpro-19/.

Vezzoso, S., "Competition Policy in Transition: Exploring Data Portability's Roles", *15th ASCOLA (Virtual) Conference*, June 2020, available at https://ssrn.com/abstract=3634736.

Research papers

Acemoğlu, D., Makhdoumi, A., Malekian, A. and Ozdaglar, A., "Too much data: prices and inefficiencies in data markets", *NBER Working Paper No. 26296*, 2019, available at https://www.nber.org/system/files/working_papers/w26296/w26296.pdf.

Acquisti, A., Taylor, C. and Wagman, L., "The Economics of Privacy", *Sloan Foundation Economics Research Paper No. 2580411*, 8 March 2016, available at https://ssrn.com/abstract=2580411.

Alexiadis, P. and de Streel, A., "Designing an EU Intervention Standard for Digital Platforms", *Robert Schuman Centre for Advanced Studies Research Paper No. 2020/14*, 26 February 2020, available at https://ssrn.com/abstract=3544694.

Bakhoum, M., "Abuse without Dominance in Competition Law: Abuse of Economic Dependence and its Interface with Abuse of Dominance", *Max Planck Institute for Innovation & Competition Research Paper No. 15-15*, 2015, available at https://ssrn.com/abstract=2703809.

Borgogno, O. and Colangelo, G., "Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking", 3 January 2020, available at SSRN: https://ssrn.com/abstract=3513514.

Bougette, P., Budzinski, O. and Marty, F., "Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?", *Ilmenau Economics Discussion Papers No. 119*, 2018, available at http://hdl.handle.net/10419/191022.

Clifford, D., Graef, I. and Valcke, P. "Pre-formulated declarations of data subject consent – Citizen-consumer empowerment and the alignment of data, consumer and competition law protections", *CiTiP Working Paper 33/2017*, February 2018, available at https://ssrn.com/abstract=3126706.

Colangelo, G. and Borgogno, O. "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule", *Stanford-Vienna European Union Law Working Paper No. 35*, 2018, available at https://law.stanford.edu/publications/no-35-data-innovation-and-transatlantic-competition-in-finance-the-case-of-the-access-to-account-rule/.

Colangelo, G. and Maggiolino, M., "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *Bocconi Legal Studies Research Paper No. 2945085*, 2 April 2017, available at https://ssrn.com/abstract=2945085.

Condorelli, D. and Padilla, J., "Harnessing Platform Envelopment Through Privacy Policy Tying", December 2019, available at https://ssrn.com/abstract=3504025.

de Streel, A. “Online Intermediation Platforms and Fairness: An assessment of the recent Commission Proposal”, September 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248723.

de Streel, A. and Larouche, P., “Disruptive innovation and competition policy enforcement”, *OECD Working Paper DAF/COMP/GF(2015)7*, 2015, available at https://ssrn.com/abstract=2678890.

Di Porto, F. and Ghidini, G., “'I Access Your Data You Access Mine'. Setting a Reciprocity Clause for the ‘Access to Account Rule’ in the Payment Services Market”, 2019, available at https://ssrn.com/abstract=3407294.

Drexl, J., “Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy”, *Max Planck Institute for Innovation & Competition Research Paper No. 18-23*, 31 October 2018, available at https://ssrn.com/abstract=3274519.

Drexl, J., Hilty, R., Globocnik, J., Greiner, F., Kim, D., Richter, H., Slowinski, P., Surblytė, G., Walz, A. and Wiedemann, K., “Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission’s “Public consultation on Building the European Data Economy””, *Max Planck Institute for Innovation and Competition Research Paper No. 17-08*, 2017, available at https://ssrn.com/abstract=2959924.

Drexl, J., “Designing Competitive Markets for Industrial Data - Between Propertisation and Access*”, Max Planck Institute for Innovation & Competition Research Paper No. 16-13*, 31 October 2016, available at https://ssrn.com/abstract=2862975.

Duch-Brown, N., Martens, B. and Mueller-Langer, F., “The economics of ownership, access and trade in digital data”, *Digital Economy Working Paper 2016-10*, JRC Technical Reports, 2016, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914144.

Ennis, S. and Fletcher, A., “Developing international perspectives on digital competition policy”, 31 March 2020, available at https://ssrn.com/abstract=3565491.

Fast, F., Schnurr, D. and Wohlfarth, M., "Data-Driven Market Power: An Overview of Economic Benefits and Competitive Advantages from Big Data Use”, July 2019, available at https://ssrn.com/abstract=3427087.

Geradin, D., “Access to In-Vehicle Data by Third-Party Service Providers: Is there a Market Failure and, if so, How Should it be Addressed?”, January 2020, available at https://ssrn.com/abstract=3545817.

Geradin, D., “Ten Years of DG Competition Effort to Provide Guidance on the Application of Competition Rules to the Licensing of Standard-Essential Patents: Where Do We Stand?”, 21 January 2013, available at https://ssrn.com/abstract=2204359.

Geradin, D., “Refusal to Supply and Margin Squeeze: A Discussion of Why the “Telefonica Exceptions” are Wrong”, *TILEC Discussion Paper No. 2011-009*, 2011, available at https://ssrn.com/abstract=1762687.

Geradin, D., Karanikioti, T. and Katsifis, D., "GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech", *TILEC Discussion Paper DP 2020-012*, May 2020, available at https://ssrn.com/abstract=3598130.

Graef, I., Tombal, T. and de Streel, A., "Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper DP 2019-005*, November 2019, available at https://ssrn.com/abstract=2956308.

Graef, I., Husovec, M. and van den Boom, J., "Spill-overs in data governance: the relationship between the GDPR's right to data portability and EU sector-specific data access regimes", *TILEC Discussion Paper DP 2019-024*, 8 April 2019, available at https://ssrn.com/abstract=3369509.

Graef, I., Gellert, R. and Husovec, M., "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, 27 September 2018, available at http://ssrn.com/abstract=3256189.

Hoffmann, J. and Johannsen, G., "EU-Merger Control & Big Data: On Data-specific Theories of Harm and Remedies", *Max Planck Institute for Innovation and Competition Research Paper No. 19-05*, 31 May 2019, available at https://ssrn.com/abstract=3364792.

Ibáñez Colomo, P., "Indispensability and Abuse of Dominance: From Commercial Solvents to Slovak Telekom and Google Shopping", 11 December 2019, available at https://ssrn.com/abstract=3502519.

Jia, J., Zhe Jin, G. and Wagman, L., "The Short-Run Effects of GDPR on Technology Venture Investment", November 2019, available at https://papers.ssrn.com/abstract=32789128.

Johnson, G. and Shriver, S., "Privacy & market concentration: Intended & unintended consequences of the GDPR", March 2020, available at https://ssrn.com/abstract=3477686.

Kathuria, V. and Globocnik, J., "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *Max Planck Institute for Innovation and Competition Research Paper No. 19-04*, 2019, available at https://ssrn.com/abstract=3337524.

Kerber, W., "From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems", *Joint Discussion Paper Series in Economics No. 40-2020*, 26 August 2020, available at https://ssrn.com/abstract=3681263.

Kerber, W., "Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia", September 2019, available at https://ssrn.com/abstract=3469624.

Kerber, W., "Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars", 26 August 2019, available at https://ssrn.com/abstract=3445422.

Kerber, W., “Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection”, *MAGKS Joint Discussion Paper Series in Economics No. 14-2016*, February 2016, available at https://www.econstor.eu/bitstream/10419/144679/1/850599016.pdf.

Kerber, W. and Frank, J., “Data Governance Regimes in the Digital Economy: The Example of Connected Cars”, 3 November 2017, available at https://ssrn.com/abstract=3064794.

Lerner, A., “The Role of 'Big Data' in Online Platform Competition”, 26 August 2014, available at SSRN http://dx.doi.org/10.2139/ssrn.2482780.Lundqvist, B., “Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law”, *Stockholm Faculty of Law Research Paper Series n° 54*, 2018, available at https://ssrn.com/abstract=3103870.

Madison, M., Strandburg, K. and Frischmann, B., “Knowledge Commons”, *Legal Studies Research Paper Series: Working Paper No. 2018-39*, December 2018, available at http://ssrn.com/abstract=3300348.

Martens, B., “An economic perspective on data and platform market power”, *JRC Digital Economy Working Paper 2020-09*, February 2021, available at https://www.researchgate.net/publication/349179464.

Muralidhar, K., Sarathy, R. and Li, H., “'To Share or Not to Share. That is Not the Question' - A Privacy Preserving Procedure for Sharing Linked Data”, 3 July 2014, https://ssrn.com/abstract=2462152.

Nicholas, G., “Taking It With You: Platform Barriers to Entry and the Limits of Data Portability”, 6 March 2020, available at https://ssrn.com/abstract=3550870.

Nicholas, G. and Weinberg, M., “Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?”, 2019, available at https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition.

Parker, G., Petropoulos, G. and Van Alstyne, M., “Digital Platforms and Antitrust”, May 2020, available at https://ssrn.com/abstract=3608397.

Priego, L., Osimo, D. and Wareham, J., “Data sharing practices in Big Data ecosystems”, *ESADE Working Paper 273*, 2019, available at https://ssrn.com/abstract=3355696.

Prüfer, J. and Schottmüller, C., “Competing with Big Data”, *TILEC Discussion Paper No. 2017-006 and CentER Discussion Paper No. 2017-007*, February 2017, available at https://pure.uvt.nl/ws/portalfiles/portal/15514029/2017_007.pdf.

Ranchordás, S. and De Gregorio, G., “Breaking Down Information Silos with Big Data: A Legal Analysis of Data Sharing”, *University of Groningen Faculty of Law Research Paper Series No. 44/2019*, September 2019, available at https://ssrn.com/abstract=3466313.

Richter, H., “The Law and Policy of Government Access to Private Sector Data (‘B2G Data Sharing’)”, *Max Planck Institute for Innovation and Competition Research Paper No. 20-06*, 2020, available at: https://ssrn.com/abstract=3594109.

Richter, H., "Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing", *Max Planck Institute for Innovation and Competition Research Paper No. 20-03*, 2020, available at: https://ssrn.com/abstract=3565762.

Taylor, L., "Hacking a path through the Personal Data Ecosystem", December 2013, available at https://linnettaylor.wordpress.com/2013/12/12/hacking-a-path-through-the-personal-data-ecosystem/.

Tirole, J., "Federal Reserve Bank of Richmond: Econ Focus", Fourth Quarter 2017, available at www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2017/q4/interview.pdf.

Vezzoso, S., "Fintech, Access to Data, and the Role of Competition Policy", 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106594.

Guidelines and Opinions

Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251 rev.01, 6 February 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP 260 rev.01, 11 April 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Article 29 Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

Article 29 Working Party, *Guidelines on the right to data portability*, WP 242, 13 December 2016, available at https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, WP 223, 16 September 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP 216, 10 April 2014, available at https://www.pdpjournals.com/docs/88197.pdf.

Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

Bundeskartellamt and Bundeswettbewerbsbehörde, "Guidance on Transaction Value Thresholds for Mandatory Pre-Merger Notification (Section 35 (1a) GWB and Section 9 (4) KartG)", July 2018, available at

https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitfaden/Leitfaden_Transaktionsschwelle.pdf?__blob=publicationFile&v=2.

European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 March 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_fr.

European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 1.0, 2 September 2020, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, May 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf.

European Data Protection Supervisor, *Opinion 8/2018 on the legislative package "A New Deal for Consumers",* 5 October 2018, available at https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf.

European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017, available at https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf.

Reports, position papers and studies

Access Now, "Three years under the EU GDPR: An implementation progress report", 2021, available at https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf.

Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques*"*, 19 February 2020, available at https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.19_contribution_adlc_enjeux_numeriques_vf.pdf.

Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data*"*, 10 May 2016, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

Australian Competition and Consumer Commission, "Digital Platforms Inquiry – Final Report", 26 July 2019, available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

Barbero, M., Cocoru, D. , Graux, H., Hillebrand, A., Linz, F., Osimo, D., Siede, A. and Wauters, P., "Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability", 25 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and.

Bourreau, M. and de Streel, A., "Digital Conglomerates and EU Competition Policy", *CERRE Report*, March 2019, available at http://www.crid.be/pdf/public/8377.pdf.

Bourreau, M., de Streel, A. and Graef, I., "Big Data and Competition Policy: Market power, personalised pricing and advertising", *CERRE Report*, 2017, available at http://www.cerre.eu/publications/big-data-and-competition-policy.

Brave, "Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities", April 2020, available at https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf.

College of Europe, "Study on the impact of national rules on unilateral conduct that diverge from Article 102 of the Treaty on the Functioning of the European Union (TFEU) – Final Report", 21 November 2012, available at https://ec.europa.eu/competition/calls/tenders_closed.html.

Competition and Markets Authority, "Online platforms and digital advertising: Market study final report", 1 July 2020, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Competition and Markets Authority, "Final Approved Roadmap for Open Banking", 14 May 2020, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885537/Notice_of_proposed_changes_to_the_open_banking_roadmap_-_web_publication_-_cma_gov_uk_---_May_2020_-.pdf.

Competition and Markets Authority, "Online platforms and digital advertising: Market study interim report – Appendix L: Potential approaches to improving personal data mobility", 18 December 2019, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Competition and Markets Authority, "The Retail Banking Market Investigation Order 2017", 2017, available at https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-bankingmarketinvestigationor der-2017.pdf.

Competition and Markets Authority, "Making Banks Work Harder for You", 9 August 2016, available at http://www.agefi.fr/sites/agefi.fr/files/fichiers/2016/08/cma_overview-of-the-banking-retail-market_9_aout .pdf.

Competition and Markets Authority, "Retail Banking Market Investigation – Final Report", 26 February 2016, available at https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk.

Competition and Markets Authority and Information Commissioner's Office, "Competition and data protection in digital markets: a joint statement between the CMA and the ICO", 19 May 2021, available at https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf.

Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *Council of Europe Treaty Series n° 223*, Strasbourg, 10 October 2018, available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

Crémer, J., de Montjoye, Y.-A. and Schweitzer, H., "Competition Policy for the digital era – Final report", 2019, available at http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

CtrlShift, "Data mobility: The personal data portability growth opportunity for the UK economy", 2018, available at https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf.

(Irish) Data Protection Commission, "Annual Report: 1 January – 31 December 2019", 2020, available at https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf.

(Irish) Data Protection Commission, "Annual Report: 25 May – 31 December 2018", 2019, available at https://www.dataprotection.ie/sites/default/files/uploads/2019-02/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf.

Data Transfer Project, "White Paper: Data Transfer Project Overview and Fundamentals", 20 July 2018, available at https://datatransferproject.dev/dtp-overview.pdf.

de Streel, A., Liebhaberg, B., Fletcher, A., Feasey, R., Krämer, J. and Monti, G., "The European Proposal for a Digital Markets Act: A First Assessment", *CERRE Assessment Paper*, January 2021, available at https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/.

de Streel, A., Cave, M., Feasey, R., Krämer, J. and Monti, G., "Digital Markets Act: Making economic regulation of platforms fit for the digital age", *CERRE Recommendations Paper*, November 2020, available at https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/.

de Terwangne, C., Moiny, J.-P., Poullet, Y. et Van Gyzeghem, J.-M., "Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)", *Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD)*, T-PD-BUR(2010)09 (II) FINAL, Conseil de l'Europe, Strasbourg, 3 novembre 2010.

Deloitte, "Realising the economic potential of machine-generated, non-personal data in the EU", *Report for Vodaphone Group*, July 2018, available at

https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf.

Drexl, J., "Data Access and Control in the Era of Connected Devices", *Study on Behalf of the European Consumer Organisation (BEUC)*, 2019, available at https://www.beuc.eu/publications/beuc-x-2018_121_data_access_and_control_in_the_area_of_connected_devices.pdf.

Egan, E., "Data Portability and Privacy", *Facebook White Paper*, September 2019, available at https://iapp.org/media/pdf/fb_whitepaper_sep_2019.pdf.

European Commission, "Consultation on PSI Directive review – Synopsis report", 25 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-revision-directive-reuse-public-sector-information.

Everis, "Study on data sharing between companies in Europe – Final report", *Study for the European Commission*, 2018, available at https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

Everis, "Study on data sharing between companies in Europe – Case studies", *Study for the European Commission*, 2018, available at https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

Expert Group for the Observatory on the Online Platform Economy, "Work stream on Data: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports.

Expert Group for the Observatory on the Online Platform Economy, "Measurement & Economic Indicators: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports.

Expert Group for the Observatory on the Online Platform Economy, "Work stream on Differentiated Treatment: Final Report", 26 February 2021, available at https://ec.europa.eu/digital-single-market/en/news/expert-group-eu-observatory-online-platform-economy-final-reports.

Feasey, R. and de Streel, A., "Data Sharing for Digital Market Contestability: Towards a Governance Framework", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/.

French Ministry of the Economy, Finance and the Recovery, German Federal Ministry for Economic Affairs and Energy and Dutch Ministry of Economic Affairs and Climate Policy, "Strengthening the Digital Markets Act and Its Enforcement", May 2021, available at https://www.economie.gouv.fr/files/2021-05/1055%20-%20Strengthening%20the%20Digital%20Markets%20Act%20and%20Its%20Enforcement.pdf.

Freshfields Bruckhaus Deringer, "New Competition Tool: Observations in the context of the Commission's Public Consultation", 8 September 2020, available at https://passle-

net.s3.amazonaws.com/Passle/5832ca6d3d94760e8057a1b6/MediaLibrary/Document/2020-09-09-14-52-58-669-FreshfieldsSubmissionNewCT.pdf.

Furman, J., Coyle, D., Fletcher, A., Marsden, P. and McAuley, D., "Unlocking digital competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, 2019, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel.

German Federal Ministry for Economic Affairs and Energy, "A New Competition Framework for the Digital Economy: Report by the Commission "Competition Law 4.0" – Executive Summary", 9 September 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competition-framework.pdf?__blob=publicationFile&v=2.

High-Level Expert Group on Business-to-Government Data Sharing, "Towards a European strategy on business-to-government data sharing for public interests – Final report", 2020, available at https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more.

HM Government, "Smart Data: Putting consumers in control of their data and enabling innovation", June 2019, available at https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation.

Information Commissioner's Office, "Data sharing code of practice", 17 December 2020, available at https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/.

Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection", 4 September 2017, available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

International Data Corporation and the Lisbon Council, "The European Data Market Study Monitoring Tool – Final Study Report", June 2020, SMART 2016/0063, available at http://datalandscape.eu/.

Jiip, Technopolis, Bently, L. and Derclaye, E., "Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases – Final report", 2018, available at, https://ec.europa.eu/digital-single-market/en/news/study-support-evaluation-database-directive.

Kemp, R., "Legal Aspects of Managing Data (White Paper)", October 2019, available at http://www.kempitlaw.com/legal-aspects-of-managing-data/.

Krämer, J., Schnurr, D. and Broughton Micova, S., "The role of data for digital markets contestability: case studies and data access remedies", *CERRE Report*, September 2020, available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/.

Krämer, J., Senellart, P. and de Streel, A., "Making data portability more effective for the digital economy", *CERRE Report*, 2020, available at

https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy.

Langford, J., Poikola, A., Janssen, W., Lähteenoja, V. and Rikken, M. (eds.), "Understanding MyData Operators", *MyData Global Report*, 29 April 2020, available at https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf.

Lear, "Ex-post Assessment of Merger Control Decisions in Digital Markets – Final Report", 9 May 2019, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803576/CMA_past_digital_mergers_GOV.UK_version.pdf.

Netherlands Authority for Consumers and Markets, "Big Techs in the payment system", 16 November 2020, available at https://www.acm.nl/en/publications/acm-study-big-techs-dutch-payment-system.

OECD, *Consumer Data Rights and Competition - Background note*, June 2020, DAF/COMP(2020)1, available at http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm.

OECD, "Lines of Business Restrictions – Background note", 8 June 2020, DAF/COMP/WP2(2020)1, available at https://one.oecd.org/document/DAF/COMP/WP2(2020)1/en/pdf.

Ofcom, "Update on Open Communications: Enabling people to share data with innovative services", 7 July 2021, available at https://www.ofcom.org.uk/consultations-and-statements/category-1/open-communications.

Open Data Institute, "Sharing data to create value in the private sector", 2020, available at https://theodi.org/article/report-sharing-data-to-create-value-in-the-private-sector/.

Open Data Institute, "Data trusts: lessons from three pilots", 2019, available at https://theodi.org/article/odi-data-trusts-report/.

Open Data Institute and Fingleton, "Open Banking, Preparing for lift off: Purpose Progress and Potential", 16 July 2019, available at https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf.

Poullet, Y., Dinant, J.-M., de Terwangne, C. et Perez-Asinari, M.-V., "L'autodétermination informationnelle à l'ère de l'internet", *Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD)*, Conseil de l'Europe, Strasbourg, 18 novembre 2004.

Prüfer, J., "Competition Policy and Data Sharing on Data-driven Markets", *Report for the Friedrich-Ebert-Stiftung*, 2020, available at http://library.fes.de/pdf-files/fes/15999.pdf.

Reed, C., BPE Solicitors and Pinsent Masons, "Data trusts: legal and governance considerations", 2019, available at https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf.

Renda, A., Cafaggi, F., Pelkmans, J., Iamiceli, P., Correia de Brito, A., Mustilli, F., Bebber, L., Clavel, S., Ignacio Ruiz Peris, J. and Estevan, C., "Study on the legal framework covering business-to-business unfair trading practices in the retail supply chain – Final report", DG MARKT/2012/049/E, 26 February 2014, available at https://op.europa.eu/en/publication-detail/-/publication/c82dc8c6-ec15-11e5-8a81-01aa75ed71a1/language-en.

Rouvroy, A., ""Of Data and Men": Fundamental Rights and Liberties in a World of Big Data", *Report for the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)*, T-PD-BUR(2015)09REV, Council of Europe, Strasbourg, 11 January 2016.

Samson, R., Gibbon, K. and Scott, A., "About data about us," September 2019, available at https://www.thersa.org/globalassets/pdfs/reports/data-about-us-final-report.pdf.

Schweitzer, H., Schalbruch, M., Wambach, A., Kirchhoff, W., Langeheine, D., Schneider, J.-P., Schnitzer, M., Seeliger, D., Wagner, G., Durz, H., Heider, M. and Mohrs, F., "A New Competition Framework for the Digital Economy", *Report by the Commission "Competition Law 4.0" for the German Federal Ministry for Economic Affairs and Energy*, 2019, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competition-framework.pdf?__blob=publicationFile&v=2.

Schweitzer, H., Haucap, J., Kerber, W. and Welker, R., *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, Baden-Baden, Nomos, 2018 (also available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtigeunternehmen.html (an executive summary in English is available at https://ssrn.com/abstract=3250742)).

Schweitzer, H., Haucap, J., Kerber, W. and Welker, R., "Modernising the law on abuse of market power: Executive Summary", *Report for the German Federal Ministry for Economic Affairs and Energy*, 29 August 2018, available at https://ssrn.com/abstract=3250742.

Steenbergen, J., Snoep, M. and Barthelmé, P., "Joint memorandum of the Belgian, Dutch and Luxembourg competition authorities on challenges faced by competition authorities in a digital world", 2 October 2019, available at https://www.belgiancompetition.be/en/about-us/publications/joint-memorandum-belgian-dutch-and-luxembourg-competition-authorities.

Stigler Committee on Digital Platforms, "Final Report", September 2019, available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report.

Support Centre for Data Sharing, "B.2 – Analytical report on EU law applicable to sharing of non-personal data", SMART 2018/2019, 24 January 2020, available at https://eudatasharing.eu/fr/legal-aspects.

Support Centre for Data Sharing, "B.1 – Report on collected model contract terms", SMART 2018/2019, 26 July 2019, available at https://eudatasharing.eu/fr/legal-aspects.

TRL, "Access to In-Vehicule Data and Resources – Final Report", *Study for the European Commission*, May 2017, available at https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf.

United States House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets – Majority Staff Report and Recommendations", 2020, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

Van Asbroeck, B., Debussche, J. and César, J., "White Paper – Data ownership in the context of the European data economy: proposal for a new right", 2017, available at https://www.twobirds.com/en/news/articles/2017/global/data-ownership-in-the-context-of-the-european-data-economy.

Blogs, news and press releases

Acemoğlu, D., Makhdoumi, A., Malekian, A. and Ozdaglar, A., "Can we have too much data?", 18 November 2019, available at https://voxeu.org/article/can-we-have-too-much-data.

Adam, L., "RGPD : Amazon écope d'une amende record à 746 millions d'euros", 30 July 2021, available at https://www.zdnet.fr/actualites/rgpd-amazon-ecope-d-une-amende-record-a-746-millions-d-euros-39926965.htm.

Aszendorf, Z. and Pratt, G., "CJEU narrows protection afforded to database right in the EU", 9 June 2021, available at https://www.lexology.com/library/detail.aspx?g=f399c5bb-58ac-4162-b2c8-b8a53297f800&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2021-06-11&utm_term=.

Barbaro, M. and Zeller, T., "A Face is exposed for AOL searcher no. 4417749", *The New York Times*, 9 August 2006, available at https://www.nytimes.com/2006/08/09/technology/09aol.html.

Bertuzzi, L., "Irish watchdog given one month to finalise Whatsapp privacy ruling", 29 July 2021, available at https://www.euractiv.com/section/data-protection/news/irish-watchdog-given-one-month-to-finalise-whatsapp-privacy-ruling/.

Bodoni, S., "Amazon Gets Record $888 Million EU Fine Over Data Violations", 30 July 2021, available at https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach.

Bodoni, S., "Facebook Targeted in the U.K. Legal Action Over Cambridge Analytica", *Bloomberg*, 28 October 2020, available at https://www.bloomberg.com/news/articles/2020-10-28/facebook-targeted-in-u-k-legal-action-over-cambridge-analytica.

Brave, "Inside the Black Box: A Glimpse of Google's Internal Data Free-for-All", 2020, available at https://brave.com/wp-content/uploads/2020/03/Inside-the-Black-Box.pdf.

Brennan, C., Mantine, M., Stegmaier, G. and Vose, G., "hiQ Labs, Inc. v. LinkedIn Corp.: federal judge dismisses antitrust claims regarding access to data", 1 October 2020, available at https://www.reedsmith.com/en/perspectives/2020/10/hiq-labs-inc-v-linkedin-corp-federal-judge-dismisses-antitrust-claims.

Bundesgerichtshof, “Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook,” 23 June 2020, available at https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html.

Bundeskartellamt, “Amendment of the German Act against Restraints of Competition (Press release)”, 19 January 2021, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html.

Bundeskartellamt, “Bundeskartellamt prohibits Facebook from combining user data from different sources”, 7 February 2019, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

Chang, A., “The Facebook and Cambridge Analytica scandal, explained with a simple diagram”, 2 May 2018, available at https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

Competition and Markets Authority, “CMA to investigate Google’s ‘Privacy Sandbox’ browser changes”, 8 January 2021, available at https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes.

European Commission, “Antitrust: Commission sends Statement of Objections to Insurance Ireland”, *Press release n° IP/21/3081*, 18 June 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3081.

European Commission, “Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions”, *Press release n° IP/20/2484*, 17 December 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2484.

European Commission, “Questions and Answers – Establishing a fair, trusted and innovation driven ecosystem in the Online Platform Economy”, 9 July 2020, available at https://ec.europa.eu/digital-single-market/en/business-business-trading-practices.

European Data Protection Board, “EDPB adopts Art. 65 decision regarding WhatsApp Ireland”, 28 July 2021, available at https://edpb.europa.eu/news/news/2021/edpb-adopts-art-65-decision-regarding-whatsapp-ireland_en.

Gielen, B. and Verdonck, C., “First Belgian ruling on abuse of economic dependence”, 3 December 2020, available at https://www.lexology.com.

Granville, K., “Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens”, *New York Times*, 19 March 2018, available at https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Guillaud, H., “L’emploi à l’épreuve des algorithmes”, *InternetActu*, 3 May 2013, available at http://www.internetactu.net/2013/05/03/lemploi-a-lepreuve-des-algorithmes/.

Lyons, D., "GDPR: Privacy as Europe's tariff by other means?", 3 July 2018, available at https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/.

Manancourt, V., "Irish data regulator pulls out of 'perverse' MEP hearing as tensions boil over", 18 March 2021, available at https://pro.politico.eu/news/irish-data-regulator-pulls-out-of-perverse-mep-hearing-as-tensions-boil-over.

Mattioli, D., "Amazon scooped up data from its own sellers to launch competing products", *The Wall Street Journal,* 23 April 2020.

McCandless, D., "Data, information, knowledge, wisdom", 29 November 2010, available at http://www.informationisbeautiful.net/2010/data-information-knowledge-wisdom/.

McClelland, J., Grimes, S. and Murphy, S., "EU Trade Secrets Directive: What Are "Reasonable Steps"?", 7 February 2019, available at https://www.lexology.com/library/detail.aspx?g=b59572d9-5e29-44e4-b4fe-67c5559bcf32&filterId=c6af7021-82de-49f8-96af-884381b2f7d6.

Meyer, D., "European Commission experts uneasy over WP29 data portability interpretation*"*, 25 April 2017, available at https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/.

Open Data Institute, "Data Access Map", available at https://theodi.org/project/the-data-access-map/#1565707571855-6d70b0a0-3243.

Pearson, J., "Yahoo's Gigantic 'Anonymized' User Dataset Isn't All That Anonymous", 14 January 2016, available at https://www.vice.com/en/article/yp3d8v/yahoos-gigantic-anonymized-user-dataset-isnt-all-that-anonymous.

Privacy International, "Ad Tech GDPR complaint is extended to four more European regulators", 20 May 2019, available at https://privacyinternational.org/examples/2992/ad-tech-gdpr-complaint-extended-four-more-european-regulators.

Privacy International, "Panoptykon Foundation files complaint against Google and other "ad tech" companies with the with the Polish Data Protection Authority", 28 January 2019, available at https://privacyinternational.org/examples/2982/panoptykon-foundation-files-complaint-against-googleand-other-ad-tech-companies.

Privacy International, "Regulatory complaint against Google and other "ad tech" companies under Europe's GDPR by Johnny Ryan, Jim Killock, and Michael Veale", 12 September 2018, available at https://privacyinternational.org/examples/2983/regulatory-complaint-against-google-and-other-ad-tech-companies-under-europes-gdpr.

Ryan, J., "Formal GDPR complaint against Google's internal data free-for-all", 16 March 2020, available at https://brave.com/google-internal-data-free-for-all/.

Satariano, A., "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates", *The New York Times*, 27 April 2020, available at https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.

Stolton, S., “MEPs rue lack of GDPR sanctions issued by Irish data authority”, 26 March 2021, available at https://www.euractiv.com/section/data-protection/news/meps-rue-lack-of-gdpr-sanctions-issued-by-irish-data-authority/.

Stolton, S., “German legal dispute over Facebook data use sent to European Court of Justice”, 24 March 2021, available at https://www.euractiv.com/section/data-protection/news/german-legal-dispute-over-facebook-data-use-sent-to-european-court-of-justice/.

Stolton, S., “Blacklist prohibitions to be ‘very limited’ to large platforms, Commission says”, 9 December 2020, available at https://www.euractiv.com/section/digital/news/blacklist-prohibitions-to-be-very-limited-to-large-platforms-commission-says/.

Vinocur, N., “‘We have a huge problem’: European tech regulator despairs over lack of enforcement”, *Politico*, 27 December 2019, available at https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.