Journal of Competition Law & Economics, 2025, **00**, 1–52
https://doi.org/10.1093/joclec/nhaf016
Article

OXFORD

ACCESS TO HEALTH DATA, COMPETITION, AND REGULATORY ALTERNATIVES: THREE DIMENSIONS OF FAIRNESS

Ioannis Lianos*

ABSTRACT

The EU legal framework for data access and portability has undergone significant evolution, particularly in the realm of health data, with recent initiatives like the European Health Data Space (EHDS) and competition law enforcement expanding data-sharing obligations across various economic actors. This evolution reflects a shift from an initial emphasis on individuals' fundamental rights to access and port their health data—rooted in privacy protection, personal data rights, and digital sovereignty—towards a more utilitarian perspective. This newer approach extends data-sharing obligations to cover co-generated data involving end-users, business users, and complementors within digital health ecosystems, promoting a concept of data co-use or co-ownership rather than private ownership. Furthermore, the regulatory framework has proactively established 'data commons' to foster cumulative innovation and broader industry transformation. The increasing prominence of a fairness rhetoric in EU regulatory and competition law underscores a transformational intent, aiming not only to acknowledge stakeholders' contributions to data generation but also to ensure equal economic opportunities within the digital health space and facilitate the EU's digital transition. This study adopts a law and political economy perspective to examine the competition-related bottleneck issues specific to health data, considering the economic structure of its generation, capture, and exploitation. It then analyses the distributive implications of current regulations (including the DMA, Data Act, EHDS, Digital Governance Act, and Competition Law) by exploring relationships between key economic players: digital platforms and end users, platforms and their ecosystem complementors, and external third-party businesses interacting with the digital health ecosystem.

JEL: K21, L4, L44, I11, I18

* Professor of Global Competition Law and Public Policy and co-Director Centre for Law, Economics and Society, UCL Faculty of Laws; Member of the UK Competition Appeal Tribunal; Senior Fellow, CEBIL, University of Copenhagen. The research for this work was supported, in part, by a Novo Nordisk Foundation Grant for a scientifically independent International Collaborative Bioscience Innovation & Law Programme (Inter-CeBIL programme—grant no. NNF23SA0087056). The author has no conflict of interest to declare. All views expressed are strictly personal to the author and should not be taken in any way to represent the views of the Tribunal. The author would like to thank my colleagues at UCL Orla Lynskey, Deni Mantzari and the participants to a workshop at Koguan Law School, Shanghai Jiao Tong University, organized by professors Wang Xianlin and Liyang Hou and those at a workshop at the Japanese Fair Trade Commission (JFTC) for helpful feedback. Many thanks to Aadam Choudhary and Athina Stavrou for excellent editorial assistance.

Received: October 14, 2024. **Revised:** April 3, 2025. **Accepted:** May 28, 2025

I. INTRODUCTION

Data has consistently played a crucial role in competition discourse, with the traditional oligopolistic model depicting market actors positioning themselves based on customer preferences and competitors' actions, inherently relying on data-driven insights.[1] However, the recent emphasis on data as a key competitive parameter stems from the transformative effects of digitalisation and the ensuing 'data explosion'.[2] This technological revolution has dramatically reduced the costs associated with data collection and analysis while simultaneously expanding their application across diverse economic and social sectors. The pervasiveness of data-driven decision-making, enabled by these advancements, has fundamentally altered the competitive landscape, making data a more central and accessible resource for businesses across industries. This shift has not only intensified the importance of data in strategic positioning but has also highlighted the importance of have access to sophisticated data analytics (knowledge). Democratizing access to both (data and data analytics knowledge) would potentially level the competitive playing field while simultaneously creating new challenges and opportunities for innovative product and services, particularly in areas such as digital health.[3]

The concept of data as 'the new oil[4]'has become a cornerstone in discussions surrounding digital economy regulation, underscoring its indispensable role in modern productive activities. This analogy highlights data's transformative potential and its status as a critical resource, driving innovation, efficiency, and competitive advantage across sectors. Consequently, the issue of data access has emerged as a central focus in regulatory debates concerning the digital economy.[5] This prominence reflects growing recognition of data's pivotal role in shaping market dynamics, fostering innovation, and potentially creating or reinforcing market power. The regulatory discourse increasingly grapples with balancing the need for open data access to promote competition and innovation against concerns over privacy, security, and the protection of legitimate

1 H.C. White, Where do Markets Come From?, (1981) 87(3) American Journal of Sociology 517.

2 P. Overberg & K. Hand, How to Understand the Data Explosion (December 8th, 2021), available at https://www.wsj.com/articles/how-to-understand-the-data-explosion-11638979214; D.E. Holmes, The data explosion in Big Data: A Very Short Introduction (Oxford, 2017; online edn, Oxford Academic, 23 Nov. 2017), https://doi.org/10.1093/actrade/9780198779575.003.0001, accessed 4 Aug. 2024. There are different categories of digital data, that is information captured on a digital form (N Purtova G. van Maanen, Data as an economic good, data as a commons, and data governance, (2024) 16(1) Law, Innovation and Technology 1, 6). We focus here on 'health data', that is, metadata, raw or processed data, synthetic or 'real', personal or non-personal data capturing individual or social behaviour regarding health conditions, and quality of life, including epidemiological information or 'omics'-based datasets, such as genomics, proteomics, metabolomics, metagenomics, phenomics, transcriptomics, but also data from health and fitness devices.

3 See, Y. Wang, B. Blobel, B. Yang, Reinforcing Health Data Sharing through Data Democratization, (2022) 12(9) J Pers Med 1380, doi: 10.3390/jpm12091380 (on the importance of data sharing infrastructures for the development of democratic health data sharing ecosystems that would respond to the different concerns of the ecosystem stakeholders/parties towards sharing health data). On the conception of ecosystems as public/private governance regimes co-creating social value see, I. Lianos, K. H. Eller & T. Kleinschmitt, Tobias, Towards a Legal Theory of Digital Ecosystems (May 27, 2024). Faculty of Laws University College London Law Research Paper No. 16/2024, Amsterdam Law School Research Paper No. 2024–22, Amsterdam Centre for Transformative private law Working Paper No. 2024–01, Available at SSRN: https://ssrn.com/abstract=4849340.

4 This is credited to mathematician Clive Humby: N. Talagala, Data as the New Oil is not Enough: Four Principles for Avoiding Data Fires, Forbes (March 4, 2022), available at ttps://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires.

5 See, among others, I. Graef, S.Y. Wahyuningtyas & P. Valcke, Assessing data access issues in online platforms, (2015) 39(5) Telecommunications Policy 375; W. Kerber, Data Sharing in IoT Ecosystems and Competition Law: The Example of Connected Cars, (2019) 15(4) Journal of Competition Law and Economics 381; T. Tombal, Economic Dependence and Data Access, (2020) 51(1) IIC—International Review of Intellectual Property and Competition Law 70; B. Martens, F. Mueller-Langer, Access to Digital Car Data and Competition in Aftermarket Maintenance Services< (2020) 16(1) Journal of Competition Law and Economics 116; J. Krämer, D. Schnurr, Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies, (2022) 18(2) Journal of Competition Law and Economics 255; P. Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, Further EU Digital Regulations Acts, and Competition Law, (2023) 14(2) Journal of European Competition Law and Practice 67; H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337; B. Lundqvist, An access and transfer right to data—from a competition law perspective, (2023) 11 Journal of Antitrust Enforcement 157.

business interests, making data access policies a complex and crucial aspect of digital economy governance.[6]

With the development of digital health as 'digital business', the issue of data access could not but take centre-stage in efforts to regulate competition in this area.[7] Because of their sensitive nature, as healthcare services and health data are linked to personhood and raise important ethical and legal concerns,[8] and given the constitutional protection of the right to health perceived as a fundamental right,[9] access to health data presents unique challenges for competition law and regulation. It requires a careful analysis of the, sometimes conflictual, relation between the goals pursued by the different types of regulation that intersect in this area, such as fairness, contestability and innovation. This study aims to uncover the rise of different rhetorics (discourses)[10] or legal narratives[11] that may put forward unifying theoretical constructs that impact the development of operational legal doctrines regulating access to health data.

In analysing the legal rules governing access to health data, present in competition law and other related regulatory alternatives, this study may contribute to the understanding of the justifications put forward, not only for constituting more or less open access regimes, but also for the differentiated levels of access provided, depending on who asks for it. Indeed, 'fair' access has different dimensions: different rules and distributional impact considerations kick in if access is requested by end-users than if access is sought by business users participating to digital health ecosystems and which have contributed to the harvesting of this data and to the generation of surplus value from it. Similarly, a different approach may be taken if access is sought by third parties that aim to take advantage of the economic opportunities of digital health as a business, without however contributing to the specific digital health ecosystem.

This study examines the landscape of differential access in the digital health economy, arguing that the EU regulatory and competition law framework has shifted toward a fairness-based rhetoric. This represents a departure from approaches grounded in economic theory-inspired property rights or even 'dignitary' conceptions of data relations. This shift in rhetoric reflects the intention of the EU regulatory system to recognize the contributions of various stakeholders in data value generation, as well as to ensure equal economic opportunities and the advancement of innovation and of the economy through its digital transition.

The study highlights the critical importance of health data access while also acknowledging that mere data possession is insufficient for generating significant value in the digital health economy. To achieve the full value potential of data, one should take a more holistic approach, termed 'data access plus', which encompasses not only access to health data but also to the computational infrastructure and learning required to fully leverage this data.[12] This holistic vision underscores the interdependence between data and the technological capabilities and

[6] These concerns are also present in other sectors of the digital economy than digital health. For instance, the paradigm of 'Open Finance' includes at its core a requirement for open access to data or data sharing. See, A. Lehmann, M. J. Scott, *Open Finance* (European Parliament. Directorate-General for Internal Policies of the Union, 2023).

[7] L. Savage, M. Gaynor, J. Adler-Milstein, Digital Health Data and Information Sharing: A New Frontier for Healthcare Competition, (2019) 82(2) Antitrust Law Journal 593; G. Schneider, *Health Data Pools under European Data Protection and Competition Law: Health as a Digital Business* (Springer, 2022).

[8] A. Didier, A. Nathaniel, H. Scott, S. Look, L. Benaroyo, M. Zumstein-Shaha, Protecting Personhood: A Classic Grounded Theory, (2023) 33(13) Qual Health Res. 1177.

[9] Art. 35 EU Charter of Fundamental Rights.

[10] See, for instance, the interesting discussion in economics about the role of 'rhetoric': U. Mäki, How to Combine Rhetoric and Realism in the Methodology of Economics, (1988) 4(1) Journal of Economics and Philosophy 89; U. Mäki, Two Philosophies of the Rhetoric of Economics, in W. Henderson, T. Dudley-Evans, and R. Backhouse (eds) *Economics and Language*, (Routledge, 1993), 23; D. McCloskey, *The Rhetoric of Economics*, (University of Wisconsin Press, 1998);

[11] N. McCormick, *Rhetoric and the Rule of Law: A Theory of Legal Reasoning* (OUP, 2005), Chapter 11 on 'legal narratives'.

[12] H. Hallock et al., Federated Networks for Distributed Analysis of Health Data, (2021) 9 Frontiers in Public Health, https://doi.org/10.3389/fpubh.2021.712569.

infrastructure needed to process, analyse, and derive insights from it, and highlights how computational resources are essential for extracting maximum economic and societal value from health data. The study positions this broader framework of access rules as crucial for fostering innovation, improving healthcare outcomes, and driving economic growth in the digital health sector. Linking data access with computational capabilities sets the stage for a more nuanced understanding of the requirements for effective data utilisation in healthcare, pointing towards the need for policies and regulations that address both aspects simultaneously to unlock the full potential of health data in the digital age. This broader framework of access rules is explored in a distinct study.[13]

Section I examines the rise of different rhetorics concerning access to data (in general), and how these may operate as priors in any discussion on the definition of the access-related 'problems' requiring some public intervention through competition law and/or regulatory alternatives. This more 'foundational' section provides the framework to reflect on the issue of 'fair' access to data. It concludes on the dominance of the fairness rhetoric, although it is noted that this has included over time different dimensions. Taking a law and political economy perspective, Section II briefly explores the specific competition related bottleneck issues raised by health data as these manifest and relate to the overall economic structure of their generation, capture, and exploitation. As the institutional framework (or legal code) regulating access to data will play an important role in these competitive interactions, the following three sections highlight the distributive implications of the current regulatory framework, by exploring three sets of relations between groups of economic players using this data. Particularly it examines the relation between the digital platform/orchestrator and end users (Section III), then, that between the digital platform and its complementors in the context of an ecosystem (Section IV), and finally the interactions between third-party business users external to the ecosystem and the actors within the business ecosystem (Section V).[14] The concluding section of the study broadens the discussion on public governance's role in the context of health data and puts forward a dual approach to fostering fairness in health data markets. It argues that public intervention should extend beyond merely regulating relations between economic actors to prevent perceived unfairness and instead advocates for a more proactive stance where public governance may directly intervene with the aim to generate 'fair' outcomes in these markets. By exploring the possibilities of direct intervention, the study implies that achieving truly equitable and efficient health data markets may require governmental bodies to actively participate in market design, data sharing initiatives, or even in creating public data infrastructures. This approach aims to balance various stakeholders' interests, promote innovation, ensure equitable access to health data resources, and ultimately optimize societal benefits derived from health data utilisation in the digital economy.

[13] I. Lianos, Regulating access to data and computational infrastructure in digital health: the need for a holistic approach, in D. Mantzari & M. Ioannidou (eds.), *Research Handbook on Competition Law and Data Privacy* (forth. Edward Elgar, 2025), Chapter 1.

[14] An ecosystem 'orchestrator' is often (but now always) a 'hub' firm that engages in 'a set of deliberate and purposeful actions' 'to encourage voluntary, value co-creating inputs and effect coordination among hierarchically independent' firms (the complementors and business partners): E. Autio, Orchestrating ecosystems: a multi-layered framework, (2021) 24(1) *Innovation*, 96 (fn. 1). A 'business partner' 'fulfil(s) specific end-user needs from core business' by differentiating its products, services and brand from the orchestrator and 'securing its own end-user contact point'. In contrast, 'complementors' contribute 'to the fulfillment of a specific end-user need related to core business with a component', with its product easily integrated by different orchestrators and business partners: M. Jacobides, How to Compete When Industries Digitize and Collide: An Ecosystem Development Framework, (2022) 64(3) California Management Review, 99, 113.

II. AFTER THE 'DATA EXPLOSION': THREE RHETORICS ON THE REGULATION OF ACCESS TO DATA

The EU legal system's initial response to the new phenomenon of 'data explosion' was to adopt a 'Schumpeterian' permissionless innovation approach, except in the area of data protection law.[15] The dominant narrative was that this process of technological, economic and social transformation had to unveil its full potential, before any effort of regulatory intervention, as it produced enormous wealth and economic dynamism, and promised a technological leap forward not seen in a generation. We knew and understood too little as to how to intervene and with which tools.

The 2000s and more so the 2010s may be characterized as a period marked by the 'silence of the law' (albeit with the exception of the GDPR and linked developments regarding fundamental rights protection in the EU).[16] It is not only the *active* contribution of the legal system in recognizing and implementing rights and liabilities that is of importance, but also the lack of such, or, more generally, the *silence of the law* which also plays an important role in shaping the balance of power in these competitive struggles. Legal institutionalists often highlight the constitutive role of law in empowering or taming economic actors, and hence, the development of the GDPR highlights the influence the law may have on the distribution of power (and rents) in the economy. However, inversely, the fact that the legal system did not specifically address data access challenges by adapting its existing scope or expanding it accordingly to deal with the data phenomenon cannot be conceptualized as embracing neutrality or passivity. The non-interventionist stance adopted by states may have contributed to effectively transferring governance to private power structures, replacing the state's traditional monopoly on force.

This laissez-faire approach, characterized as 'permissionless innovation' in the Schumpeterian tradition, has had profound consequences on the digital landscape. It represents a tacit endorsement of the overly concentrated economic structure that has emerged over the past three decades (certainly more ostensibly since the 2010s), marked by the unprecedented dominance of a handful of digital platforms. These entities have amassed market values that surpass historical precedents, fundamentally altering the distribution of economic power and influence. This passive policy response has allowed for the rapid development of digital technologies and business models, but it has also led to the concentration of data, wealth, and market control in the hands of a few corporate giants, mostly situated outside the EU, despite the EU regulatory framework's otherwise central role in the governance of global value chains. The resulting digital economy structure raises critical questions about competition, innovation, and the equitable distribution of productive assets (such as data), highlighting the far-reaching implications of governmental non-intervention in shaping the digital realm.[17]

For instance, the possession of data (personal or non-personal)[18] in the digital economy does not rely on a properly defined property regime to the extent that possession and property rights are distinct concepts.[19] Instead, it relies on the control by digital platforms of important

[15] On the different types of relation between innovation and precautionary principle-based interventions, see T.A. Hemphill, The innovation governance dilemma: Alternatives to the precautionary principle, (2020) 63 Technology in Society 101381.

[16] I. Lianos, Value extraction and institutions in digital capitalism: Towards a law and political economy synthesis for competition law, (2022) 1(4) European Law Open 852.

[17] See, https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/.

[18] Personal data may be defined as any data that enable the identification of a person directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Art. 4(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119 (hereinafter GDPR).

[19] Some data may benefit from protection as a trade secret. The databases directive does not protect data as such but the content and the structure of a database.

technological bottlenecks in the way final consumers and business users access the Internet and the various services this may provide to them.

The GDPR restricts the processing of personal data, but as it is inspired by 'Kantian dignitary conceptions of data as an expression of the self, and thus subject to deontological requirements of human dignity', it does not integrate a 'propertarian' logic that would have 'coded' personal data as a form of quasi-capital, which can be exchanged in data markets and 'serve to create wealth for its holders'.[20] Although the GDPR recognizes some property rights-like entitlements on personal data, such as data portability, or the right to be forgotten, it does not put into place a proper property rights regime.[21] This would have granted formal rights over the economic value of the data whose violation would be sanctioned by a public authority and would have also delimited the boundaries of these rights or put in place a system to adjudicate disputes as to the ownership of these rights.[22] EU law includes the protection of personal data as a fundamental right,[23] implemented by the GDPR, which is itself inspired by the principle of data minimisation, the data harvesting being limited to what is directly relevant and necessary (or more broadly proportional) to accomplish a specific purpose to which the data subject has consented.[24] However, even if it predominately follows a 'dignitary' approach, the GDPR does not object to an economic logic of data exchange and governance. The GDPR restrictions on data processing cannot qualify as an inalienability rule,[25] as data commodification and transactions on data are permitted in the presence of the data subjects' informed 'consent',[26] or some other legal basis of the General Data Protection Regulation (GDPR).[27]

[20] S. Viljoen, A Relational Theory of Data Governance, (2021) 131(2) The Yale Law Journal 573, 617–628.

[21] In the absence of a property regime, as some authors have argued, 'personal data will be appropriated in proportion to the de facto power of the data market participants to exclude others': N. Purtova, The illusion of personal data as no one's property, (2013) 7(1) Law, Innovation and Technology 83. See also, N. Economides, I. Lianos, Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective, (2021) 17(4) Journal of Competition Law & Economics, 765.

[22] This is not a normative statement but a description of the state of legal thinking in the GDPR. GDPR, Recital 7 only refers to the fact that 'Natural persons should have control of their own personal data' but does not institute a property right. See also, I. Stepanov, Introducing a property right over data in the EU: the data producer's right—an evaluation, (2020) 34(1) International Review of Law, Computers & Technology, 65, 70.

[23] GDPR, Recital 1; Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).

[24] GDPR, Art. 5(1)(c).

[25] The lack of full market inalienability may be justified by the fact that the data has been harvested and already provides economic benefits to data holders. Such data holders may be, in the context of digital health, natural persons or undertakings active in the healthcare or care sectors, or developing products or services intended for the health, healthcare, or care sectors (including wellness applications): see Art. 2(2) point (t) EHDS Regulation. By allowing commodification (as data is transacted with monetary value at least between the digital platform and advertisers) and alienability (through consent) in practice the situation may be compared to that of 'market pluralism', as the alienability of personal data is legitimized but there may be some limited market inalienabilities justified by the need to protect and foster personhood. The advantages and disadvantages of this institutional setting for various societal groups, particularly the most vulnerable economically will not be discussed here. However, one may agree with M.J. Radin, Market-Inalienability, (1987) 100(8) Harvard Law Review 1849, when she explains that 'market inalienability must be judged against a background of unequal power. In that world it may sometimes be better to commodify incompletely than not to commodify at all. Market inalienability may be ideally justified in light of an appropriate conception of human flourishing, and yet sometimes be unjustifiable because of our nonideal circumstances'.

[26] Article 6 and Recital 40 GDPR. On a recent discussion of the different modes of expressing informed consent, particularly for the re-use of personal health data, such as broad consent (which allow agreement to unknown future applications), dynamic consent, and so forth, see, M. Christofidou, T.N. Arvanitis, D. Kalra, N. Lea, M. Shabani P. Coorevits, Data altruism and the "consent" question: a study into the "consent" models used under the GDPR and how the data altruism mechanism can act as a potential solution for the research community in the reuse of health data, (2025) *Front. Med.* 11:1489925, doi: 10.3389/fmed.2024.1489925.

[27] Article 6 of the GDPR also lists five other legal bases (justifications) for processing of personal data to be lawful: processing is necessary (i) to satisfy a contract to which the data subject is a party, (ii) to comply with a legal obligation, (iii) to protect the vital interests of the data subject or of another natural person, (iv) for the performance of a task carried out in the public interest or in the exercise of official authority, (v) for legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Article 89 GDPR includes derogations in favour of the re-use of personal data on the basis of a one-time consent for statistical, historical and scientific purposes without being

The tension between the 'dignitary' aspirations of the GDPR with regard to personal data and the economic reality of (personal) data markets, particularly following the rise of online advertising based business models in the digital economy,[28] has not stopped discussions about the creation of a 'data producer right' for non-personal or anonymized data with the objective of enhancing their 'tradability' as 'an economic good',[29] marking the ascendancy of the 'propertarian' logic for non-personal data. This concept proposed conferring a property right *in rem*, or at least a set of defensive rights, to data 'producers' or 'harvesters' in case the digital data in question involved the harvesting and organisation of raw data in datasets. This approach was designed to empower the *de facto* data holder—typically the manufacturer of sensor-equipped machines, tools, or devices generating the data, who had invested in their development and market commercialisation—providing them with legal recourse against third parties in cases of 'illicit misappropriation' of data. The primary aim of this 'property rights' rhetoric was to protect the *de facto* possession of data, essentially creating a legal framework that would reinforce the existing power dynamics in data ownership and control. This proposition reflected an early attempt to address the complex issues of data rights and ownership in the digital economy, focusing on safeguarding the interests of those who invest in data-generating technologies. However, the approach also raised questions about the balance between protecting investment and fostering innovation, as well as concerns about data accessibility and the potential for data monopolies. The debate surrounding this concept underscores the challenges in developing legal frameworks that can adequately address the unique characteristics of data as an economic asset and the multiple economic (including distributional) effects they may have, highlighting the tension between protecting proprietary interests and promoting broader access and utilisation of data for societal benefit.[30] These proposals were therefore criticized, and ultimately abandoned, at least in this form.

As explained above, the lack of a property regime for data has enabled digital transaction or innovation platforms, sometimes acting in intermediation markets between end-users and business partners/complementors, to harvest this valuable material, without any corresponding protection of the economic interests of the users, relying instead on their consent to their terms and conditions to get access to products or online services, the latter often provided for 'free'. Owning or having a property right on an asset gives the owner the residual rights of control, that it to use and manage the property, the right to receive an income from it, the right to use it as capital to produce income, the right to physically occupy (possess) it, the right to borrow against it, and any other right not specifically excluded. Property rights are usually understood *in rem* (against objects) and *erga omnes* (absolute rights vis-à-vis anyone).[31] This broader perspective on property rights brings to the fore the issue of appropriate governance design principles if one focuses on establishing data governance regimes for the public good.

able to fully identify the purpose of personal data processing at the time of data collection, particularly as future research purposes are difficult to predict at that time (Recital 33 GDPR).

[28] D.S. Evans, The Economics of the Online Advertising Industry, (2008) 7(3) Review of Network Economics, 359.

[29] See, *inter alia*, W. Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, (2016) 11 GRUR Int 989; J. Drexl, R.M. Hilty, L. Desaunettes, F. Greiner, D. Kim, H. Richter, G. Surblyte, & K. Wiedemann. Data Ownership and Access to Data—Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165; N. Duch-Brown, B. Martens, F. Müller-Langer, The economics of ownership, access and trade in digital data, JRC Digital Economy Working Paper, No. 2017–01, available at https://joint-research-centre.ec.europa.eu/document/download/6819ebb1-d65c-4691-ac14-d140a8d6de40_en.

[30] See, European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final, at 33. This right would have covered only the syntactical level of information (code level), not the semantic level (ideas or information), although as it has been noted by some commentators, there are circumstances in which the two are blurred, particularly if data is created through standardized computational operations: I. Stepanov, Introducing a property right over data in the EU: the data producer's right—an evaluation, (2020) 34(1) International Review of Law, Computers & Technology, 65, 80.

[31] As opposed to *in personam* rights which are rights against or in respect of a specific person (e.g. contract law).

Deciding about governance design principles has in economic theory been linked to the 'type' of the 'good' in question.[32] Ownership of a 'good' can be private, public or communal.[33] It is communal if the 'good' in question is subject to rivalrous consumption (high substractability of use) and it is difficult to exclude potential beneficiaries (high non-excludability) from its use.[34] In this case it will be open access for anyone to use (common pool resources). A low non-excludability (having the capacity to exclude non-beneficiaries) combined with high substractability of use qualifies the situation as a club good, with the result that access will only be open to a defined group of users. In contrast, public goods are subject to low substractability of use and high non-excludability.[35] Turning to data, although information has usually been characterized as a public good (low substractability of use and high non-excludability), the digitalisation process with the development of technical tools to harvest the data and enable, or restrict others' access to it, and the regulatory obligations imposed to share data with some categories of users (for example, GDPR), transforms data to a club good, to the extent that non-excludability may be high due to these technical and legal interventions.[36] Note also that although certain goods have characteristics that would situate them high or low in the substractability axis, the definition of the type of good depends, ultimately, on the type of governance regime, and not only on the 'intrinsic' characteristics of the good.[37] It follows from the above that focusing on appropriate data governance regimes for (personal and non-personal) data flows becomes essential.

The governance of data transactions presents a spectrum of legal approaches, ranging from inalienability to various forms of protection for data entitlements. When legal systems opt against making data completely inalienable, they typically employ either property rules or liability rules, often complemented by regulatory frameworks, to manage data rights and transactions.[38] If liability rules apply, the violation of a specific entitlement to privacy without an agreement (consent or some other form of legal justification) should result in compensation being paid to the victim for the damages/loss incurred. Property rights provide their holder with the right to legally bar, by injunctive relief, anyone who violates or is likely to violate their entitlement without their consent. The underlying concept is that any property violation is severely punished by injunctive relief, which in and of itself is costly; this serves to deter the violation of any entitlement in the first place and therefore avoid future harm. Liability rules are more retrospective—they provide for compensation through damages for any harm incurred. Property rules facilitate the possibility of bargaining and thus facilitate transactions in the context of the digital economy. However, they may also lead to inefficiencies, such as data

[32] E. Ostrom, Beyond Markets and States: Polycentric Governance of Complex Economic Systems, (2010) 100 American Economic Review 645.

[33] There are various economic theories of property rights, a common feature of which is of providing incentives to the owner to achieve a greater internalization of (positive or negative) externalities, thus adopting a welfare-maximization perspective. See, inter alia, H. Demsetz, Towards a Theory of Property Rights, (1967) 57(2) The American Economic Review 347; Y. Barzel, *An Economic Analysis of Property Rights* (Cambridge University Press, 2009, 2nd ed.).

[34] Pure private goods are characterized by high substractability and low non-excludability.

[35] E. Ostrom, *Understanding Institutional Diversity* (Princeton University Press, 2005), 24.

[36] For a discussion, see N Purtova G. van Maanen, Data as an economic good, data as a commons, and data governance, (2024) 16(1) Law, Innovation and Technology 1, 12–17.

[37] T. De Moor, From common pastures to global commons: A historical perspective on interdisciplinary approaches to commons, (2011) 19(4) Natures Sciences Sociétés 422.

[38] See, *inter alia*, G. Calabresi & A. D. Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, (1972) 85 Harvard Law Rev. 1089. Direct regulation (e.g. a prohibition) can be considered as a form of property rule (providing injunctive relief), with the difference being that enforcement of a property rule is done by private parties at their option, whereas regulation is enforced by government. However, other forms of regulation (e.g. a FRAND obligation) may be considered as a form of liability rule, again with the difference being the implementation of the regulation at the formal initiative of a government institution which exercises its discretion. Hence, regulation in this context also exhibits similar features in terms of approximating harm as a liability rule L. Kaplow & S. Shavell, Property Rules Versus Liability Rules (1996). Available at SSRN: https://ssrn.com/abstract=56405, 41.

ownership fragmentation (increasing transaction costs) and risks of strategic anticompetitive behaviour by data holders.[39]

The rhetoric of property rights on data was linked to the realisation that the possession and harvesting of data confer important competitive advantages in the digital era. Data constitutes an asset greatly valued by financial markets and thus provides an intangible boost to the market value of Big Tech companies.[40] This non-interventionist approach to data and digital platform regulation was primarily justified by arguments of superior economic efficiency, with the enormous profits generated by these platforms seen as evidence of their competitive prowess. It was also motivated by the assumption that this 'wealth' would trickle down to the users in data markets (business or end-users) and society overall. For instance, Big Tech economic consultants completed research focusing on the time the users were spending on these platforms to assess the value provided by the Internet to consumers. Concerning business users, in a widely publicized presentation in 2011 the chief economist of Google, Hal Varian, indicated that advertisers on Google were getting back about seven times what they spent in value of ad clicks and could benefit from clicks coming out of organic (non-ad funded) search.[41] Varian also emphasized the benefits going to the users of Google's search engine in terms of time 'saved', estimating that this amounted to an annual value of $120 billion in 2011, based on the value of time savings to average users. Hence, the argument was made that, in this 'brave new world'. everyone was getting their fair share of the pie!

This consensus was challenged from other social sciences than (competition) economics with a new rhetoric slowly emerging regarding the manipulative dimension of targeted advertising and the exploitative potential of digital platforms. To the rhetoric of Varian, one may oppose that of Shoshana Zuboff, who argued that digital platforms are harvesting a considerable amount of data, not always to recycle this for the benefit of their users with service improvements, but to constitute what Zuboff calls 'behavioral surplus'.[42] This is presented as the equivalent of industrial waste and the necessary leftover from the production process, that for efficiency purposes should not be left into the 'atmosphere' but captured to be recycled into 'useful data'.[43] Digital platforms share these 'surveillance assets' with their partners in their ecosystems or commercialize them to gather 'surveillance revenues' that are then accumulated in 'surveillance capital'.[44] The data is also used to develop the digital platforms' evolving AI capabilities. These enable them to make better predictions about the individuals' future behaviour and to develop specific prediction products, offered into new kinds of markets trading exclusively in future behaviour (what she called 'behavioral futures markets').[45]

This research directly focused on issues of exploitation and fairness at a relational level between the data controller and the data subject, rather than at a (eco)system or industry level, between a specific digital platform processing this data and its business or end-users, as well as among the different users. The narrowness of these relational approaches becomes clear if one focuses on wider 'population-based' impacts of data processing. Data exchanges result from and impact on different social relations: vertical ones between the data controller and the data

[39] See, N. Duch-Brown, B. Martens, F. Müller-Langer, The economics of ownership, access and trade in digital data, JRC Digital Economy Working Paper, No. 2017–01, 29–35.

[40] L. Taylor, H. Mukri-Smith, T. Petroçnik, L. Savolainen & A. Martin, (Re)making data markets: an exploration of the regulatory challenges, (2022) 14(2) Law, Innovation and Technology, 355.

[41] See, H. Varian, Economic Value of Google (2011), available at http://assets.en.oreilly.com/1/event/57/The%20Economic%20Impact%20of%20Google%20Presentation.pdf; E. Brynjolfsson & J. Hee Oh, The Attention Economy: Measuring the Value of Free Digital Services on the Internet, (2012) available at https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1045&context = icis2012

[42] S. Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019), 81.

[43] Ibid., 112

[44] Ibid., 94

[45] Ibid., 96.

subject, but also horizontal data relations which are not 'one to one' but involve 'population-based relations' between the different data subjects or types of data subjects, to the extent that 'informational infrastructures' have the capacity to 'make sense of data subjects via group classification' (for example, making inferences or predictions about patterns of behaviour) and 'operationalize' these classifications 'to act back on subjects'.[46] As is explained by Viljoen, as 'data becomes an essential component of informational capital', one needs to think of 'collective modes of ordering this productive activity' and develop 'institutional responses necessary to represent (and adjudicate among) the relevant population-level interests at stake in data production'.[47]

Some recent work has therefore added a third dimension to this discussion, completing this three-dimensional picture of the 'fairness', or fairness as distributive justice now, rhetoric.[48] O'Reilly, Strauss and Mazzucatto explored the creation of rents in the digital economy emphasising that 'algorithmic systems by which platforms allocate user attention affect not only users but an entire ecosystem of third-party suppliers (such as websites, content creators, or app developers), as well as advertisers'.[49] Taking a (eco)system or industry, rather than a bilateral or even trilateral (ecosystem orchestrator, business and end-users) relational, perspective, Lianos[50] and Jacobides and Lianos[51] have highlighted the contribution to the co-creation of the value and innovation of several stakeholders (business partners (for example, suppliers of inputs), labour, consumers, but also the local community and citizens) forming part of the broader business ecosystems[52] that power the global digital economy.[53] So everyone contributing to value co-creation has a stake. This value predominately benefits the shareholders of the large digital platforms, through the distribution of dividends and buybacks.[54] Doctorow has also challenged the commonly held idea that platfoms are focused on providing a good end-user experience, showing that they are in reality re-prioritizing their focus on attracting users at the money side (advertisers), reducing the quality of the experience of end-users at the subsidized side of the digital platform, finally focusing on maximising profits for their shareholders (a process he has named 'enshittification').[55]

One may think of additional justifications to this variety of 'fairness' arguments than the superior competitive advantage/acumen of Big Tech digital platforms or the fact that a large group of stakeholders has contributed to the value generation process,[56] the essential common

[46] S. Viljoen, A Relational Theory of Data Governance, (2021) 131(2) The Yale Law Journal 573, 607–608.

[47] Ibid., 577 & 579.

[48] By focusing on a broader system's level rather than the bilateral relation between the digital platform and its user, the third dimension integrates a distributive justice perspective to the extent that it focuses on the 'right' distribution of benefits and burdens of economic activity among all the actors involved in the production and use of data (here in the digital health economy space), to develop the appropriate data governance regime not just from an economic efficiency perspective but also other outcomes-based goals, such as distributive justice (fairness) if this is the normative choice of the specific social contract.

[49] T. O' Reilly, I. Straus, M. Mazzucato, Algorithmic Attention Rents: A theory of digital platform market power, Institute for Innovation and Public Purpose (Working paper 2023/10), 2.

[50] I. Lianos, Value extraction and institutions in digital capitalism: Towards a law and political economy synthesis for competition law, (2022) 1(4) European Law Open 852; I. Lianos, Competition Law for the Digital Era: A Complex Systems' Perspective (August 30, 2019). available at SSRN: https://ssrn.com/abstract=3492730.

[51] M. G Jacobides & I. Lianos, Regulating platforms and ecosystems: an introduction, (2021) 30(5) Industrial and Corporate Change, 1131.

[52] Ecosystems have been defined as 'groups of firms that must deal with either unique or supermodular complementarities that are nongeneric, requiring the creation of a specific structure of relationships and alignment to create value': MJ. Jacobides, C. Cennamo & A. Gawer, Towards a Theory of Ecosystems, (2018) 39(8) Strategic Management Journal 2255.

[53] On the role of complementors in 'augmenting' the focal value proposition of digital ecosystems, see, A.E. Carst & Y. Hu, Complementors as Ecosystem Actors: A Systematic Review, (2023) Management Review Quarterly https://doi.org/10.1007/s11301-023-00368-y.

[54] I. Lianos & A. McLean, Competition Law, Big Tech and Financialisation—The Dark Side of the Moon, in > Corradi & J. Nowag (eds.), *Intersections between Corporate and Antitrust Law* (CUP, 2023), 319.

[55] C. Doctorow, 'Enshittification' is coming for absolutely everything, FT magazine (February 8th, 2024), available at https://www.ft.com/content/6fb1602d-a08b-4a8c-bac0-047b7d64aba5.

point being that the division of rents resulting from the use of the data 'assets' disproportionately benefits the Big Tech digital platforms. A more encompassing view of fairness would aim to guarantee equality of opportunity, or equalized odds (or chances) to achieve success in competition, conditioned on each economic actor's true condition/size/capabilities, but also a broader conception of the common good, such as favouring the constitution of health 'data commons'[57] to enable a wider distribution of the (economic) benefits and opportunities of data production,[58] eventually through the exercise of 'data altruism',[59] a mechanism of 'data solidarity' or 'data philanthropy',[60] particularly for health data,[61] so that data is used and benefits the wider public and future generations,[62] or even through the constitution of negative data flow spaces (narrowly circumscribed spaces of data inalienability) through opt out mechanisms, if the risk of the development of exploitative relations is very high, particularly for vulnerable groups of users.[63] By enabling the reuse of public sector data and promoting the concept of 'data altruism', individuals and companies give their consent or permission to make available data that they generate—voluntarily and without reward—to be used in the public interest. The Data Governance Act exemplifies this effort to change the economic paradigm and escape the competition bottlenecks that may result from private control of data resources.[64] It precisely aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU, an ambition which is implemented in the digital health area by the European Health Data Space Regulation (EHDS),[65] which from this perspective, may be considered as a *lex specialis* to the Data Governance Act.[66]

The aim of these initiatives would be to take bolder action to establish data governance regimes that limit (or tame) situations of structural inequality and entrenched domination.

[56] One may indeed take a Rawlsian or Binmorian social contract perspective to arrive to the same conclusion as to the inadequacy in terms of 'fairness' of the current allocation of rents.

[57] The concept of data commons may give rise to different conceptions. It may refer in the sense used by E. Ostrom, *Governing the commons: The evolution of institutions for collective action* (Cambridge university press, 1990) to resources which can be jointly appropriated by a group, or to resources that are characterised by an open access regime in the sense of G. Hardin, The tragedy of the commons, (1968) 162 *Science* 1243 (that is resources owned by no one), or finally to resources to which everyone has access. See, S. Moroni, S. Untangling the commons: three different forms of commonality, (2024) *Review of Austrian Econ*omics https://doi.org/10.1007/s11138-024-00639-1.

[58] Data commons may result from a 'cloud-based data platform with a governance structure that allows a community to manage, analyze and share its data': R.L. Grossman, Ten lessons for data sharing with a data commons, (2023) 10 *Scientific Data* 120. Examples in the health data space include the NCI Genomic Data Commons: A.P. Heath, *et al*. The NCI Genomic Data Commons, (2021) 53 Nature genetics 257.

[59] Art. 2(16) of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), (2022) OJ L 152/1 (hereinafter Data Governance Act), which defines 'data altruism' as 'the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable' with healthcare mentioned as one of the areas.

[60] For a discussion, see M. Christofidou, T.N. Arvanitis, D. Kalra, N. Lea, M. Shabani & P. Coorevits, Data altruism and the 'consent' question: a study into the 'consent' models used under the GDPR and how the data altruism mechanism can act as a potential solution for the research community in the reuse of health data, (2025) 11 *Front. Med.* 1,489,925, doi: 10.3389/fmed.2024.1489925.

[61] B. Prainsack & A. Buyx A, *Solidarity in Biomedicine and Beyond* (Cambridge University Press, 2016).

[62] Data altruism may be inspired by an outcome-based ethical framework drawing on social welfare (also of future generations) and/or by a duty/rule-based or a value ethics perspective.

[63] See, for instance, the development for individuals of mechanisms to opt out and to object to the use of their data discussed in the last Section of this paper. Opt out regimes are intrinsically linked to the consent model used by the GDPR as the primary legal basis for data processing.

[64] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), (2022) OJ L 152/1.

[65] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, OJ L, 2025/327, 5.3.2025 (hereinafter EHDS Regulation).

[66] European Parliament, The European Health Data Space (2022), op.cit.,13.

With the establishment of an overarching regulatory framework dealing with the market failures of the digital economy, and including horizontal and sector-specific initiatives to promote data access and portability,[67] the European Union (EU) seems to have been increasingly influenced by the power and fairness-minded rhetorics taking into account also the interests of end-users, complementors and third party challengers and not only focusing on the innovation incentives of digital platforms.[68] The recent adoption of the Data Act has re-opened the discussion about property rights on data, as a response to a perceived lack of 'fairness' in the way the economic rents of digital innovation are divided.[69] Relying on the economic theory of property rights, some authors have criticized the property-like effects of the implicit acceptance by the Data Act of the exclusive *de facto* control position of data holders,[70] and suggested institutional alternatives, such as the co-ownership of this data, and the subsequent enjoyment of a bundle of rights, by all those that contribute to unlocking is economic value, allowing for a 'market-driven solution' to the problem.[71] Other suggestions depart from this emphasis on property rights and argue for a more regulatory-focused solution by providing direct access and transfer right to data that would benefit business users,[72] or the institution of a 'data sharing obligation' that may be imposed in certain economic circumstances to avoid market tipping,[73]

[67] Among the horizontal initiatives, we can refer to the GDPR (data portability rules), the Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act, OJ L, 2023/2854), the Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (DMA), OJ L 265, 12.10.2022/1), the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (DSA), OJ L 277, 27.10.2022/1), the Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022/1). Sector-specific initiatives to promote data access include the European Health Data Space (Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final), the Payment System Directive (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, 23.12.2015,/35), and to a certain extent the EU Right of Repair Directive (Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828, OJ L, 2024/1799) regarding access to spare parts and repair-related information, the Access to in-Vehicle data initiative (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en).

[68] This does not mean that the value of innovation is not considered as it appears from the emphasis put on the 'innovation principle' introduced in the 2019 Commission Communication on Better Regulation and the revised Better Regulation Toolbox of November 2021 'to ensure that EU legislation is analysed and designed so as to encourage innovation to deliver social, environmental and economic benefits'. However, the EU view on innovation takes a broader perspective as to the promotion of innovation incentives, not just of digital platforms, but of all complementors in a business ecosystem and third-parties cumulative innovators and emphasizes not just innovation but responsible/sustainable (SDGs oriented) innovation.

[69] This has motivated, for instance, the adoption of the DMA: DMA, Recital 33 (which adopts the economic desert justification for regulating the division of the economic rents as it highlights that '(m)arket participants, including business users of core platform services and alternative providers of services provided together with, or in support of, such core platform services, should have the ability to adequately capture the benefits resulting from their innovative or other efforts'.

[70] Inspired by Y. Barzel, Economic Analysis of Property Rights (CUP, 1997, 2nd ed.) (who noted that due to the fact that transactions are costly, as an economic matter property rights, defined as expectations of net utility) are never fully delineated, thus criticizing the Coase theorem that as rights are well defined, income is maximized regardless of who has these rights, but also disconnecting economic property rights from the legal entitlement) such authors argue that firms can use 'capturing' strategies to appropriate the data in order to exploit it economically getting a 'property-like exclusive position on them through technological control', the Data Act recognizing this status quo and enabling the data holders to receive 'reasonable compensation' for the use by third-parties of this data: M. Eckardt & W. Kerber, Property rights theory, bundles of rights on IoT data, and the EU Data Act, (2024) 57 European Journal of Law and Economics 113, 123–126.

[71] H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 345 & 355.; M. Eckardt & W. Kerber, Property rights theory, bundles of rights on IoT data, and the EU Data Act, (2024) 57 European Journal of Law and Economics 113, 133.

[72] See, B. Lundqvist, An access and transfer right to data—from a competition law perspective, (2023) 11 Journal of Antitrust Enforcement 157. See also, M. Eckardt & W. Kerber, Property rights theory, bundles of rights on IoT data, and the EU Data Act, (2024) 57 European Journal of Law and Economics 113, 135.

[73] See, J. Prufer & I. Graef, Governance of Data Sharing: a Law & Economics Proposal (January 22, 2021). TILEC Discussion Paper No. 2021–001, CentER Discussion Paper No. 2021–004, available at SSRN: https://ssrn.com/abstract=3774912

based on utilitarian innovation-promotion justifications. Some, finally, combine the ownership and governance of data dimensions by suggesting data-trustee solutions putting non-personal data under the governance of a neutral data trustee to enable cumulative innovation.[74]

Calls for a property rights approach that would recognize the co-ownership of data and its linkage to the process of co-generation of value taking place in the communities of co-opetition that are business ecosystems, may exercise some appeal, particularly as the absence of property rights on data may lead to a 'missing market' problem.[75] Indeed, the lack of property rights and the consequent missing markets issue may prevent parties from negotiating a transaction that reflects Pareto efficiency. Although this may be a valid point, it is also inspired by a narrow view of the function of property rights, perceived as rights *in rem* (against a thing, here data) and rights awarded for purely economic efficiency reasons. Clear and strong property rights are an indispensable tool for markets to work and to create the economic incentives for the expansion of the data 'output'. One may oppose this call for the formalisation of clear and strong property rights, an approach that would emphasize the relationship between legal entitlements and a (fair)[76] distribution and use of resources and, taking a relational approach to data governance, think of property rights as *tools* to regulate relations *among* people concerning things rather than relations between people (an individual) *and* a thing (her property).[77] We believe that focusing on the (legal and economic) relations between the different players in the digital economy concerning data, as these are expressed in the regulatory compass, will better unveil the political, economic and social choices made as to the distributional dimensions of allocating data as productive assets among the different groups involved or the social productivity of data as assets, than a discussion over what bit of the 'good' (here data) is owned by whom. 'Fair' access may thus be differently perceived depending on which of the three dimensions of 'fairness' prevails in a specific data governance regime: (i) one emphasising the role of digital entrepreneurial heroes in this Schumpeterian dynamic process, (ii) one that focuses on the dynamics of the (bilateral) power asymmetry between the platform and its users and the impact of behaviour surveillance, and finally, (iii) one that considers both vertical and horizontal data relations and highlights the contributions to the co-creation of value and innovation of a community of actors, within or from outside the ecosystem, raising issues of adequate compensation of the innovation efforts of all contributors, and more generally of an appropriate, from a social contract perspective, vertical and horizontal allocation of the benefits and costs resulting from data flows. Having presented the theoretical contours of the issue of 'fair' data access, we examine the specificity of 'health data', considering the economic implications that their nature, but also the structural positions of the economic actors involved in their harvesting and exploitation, may impose on data flows.

(arguing for imposing an obligation to firms active in data-driven markets to share their data if their market shares exceeds 30%).

74 M. Eckardt & W. Kerber, Property rights theory, bundles of rights on IoT data, and the EU Data Act, (2024) 57 European Journal of Law and Economics 113, 136.

75 There are no markets in which data and/or attention are demanded by companies and supplied by users, and this being traded at publicly known prices. For instance, users cannot determine the value of their data to the digital platform as they do not have access to the information regarding the transactions on the other side of the platform between the company and the advertisers.

76 And/or more innovative, sustainable . . . or whatever other value the social contract in question has considered as key for the regulatory framework.

77 D. Kennedy, Some Caution about Property Rights as a Recipe for Economic Development, (2011) 1(1) Accounting, Economics, and Law, Article 3, 26 (noting that '(o)nce we think of a property right as a relationship between two people, it is clear that the state also has a role as the enforcer—and definer—of the rights of one against the other [. . .] Thought of this way, the distributional dimension in routine enforcement of property rights is quite visible').

III. HEALTH DATA AS A COMPETITIVE BOTTLENECK-SOURCE OF DOMINANCE AND EXPLOITATION[78]

The changes brought about by digital technology have indeed radically transformed the pharmaceutical, healthcare and health insurance industries.[79] Globally, Big Data and algorithms are playing a key role as they enable the development of custom/tailored solutions 'beyond the pill' that combine drugs, sensors that collect information about the patient's condition and different kinds of analytics (e-medicine records, including diagnostic results, medication history and genomic or gene expression data, lifestyle data). With this data, medical providers may offer personalized medication and patient care. By collecting and evaluating personal data from different channels, platforms and devices and being able to share this information, the different parts of the human health value chain (medicine, preventive medicine, care, and so forth) can also form a single picture for the consumer/patient. This technological capability may lead to the development of new business models in the industry.

Healthcare providers and health insurance companies are increasingly relying on the data they collect to personalize their offering and limit their risks when managing costly medical conditions, exacerbating the information asymmetry they already benefit from vis-à-vis their customers. The latter do not have access to an equivalent volume of data or advanced data analysis techniques. Essentially, this digital transformation has created both a need and an opportunity for companies in the broader healthcare and health insurance industry to connect different markets and economic organisations, leading to more open business models with an emphasis on creating shared value with complementary partners in larger digital heath ecosystems.[80]

There are several different types of data that may be considered (see the non-exhaustive list in Table 1):

Some of this data (or datasets) is protected by intellectual property rights, for instance, sui generis right for databases,[81] some genetic resources such as isolated human DNA sequences are protected by patents,[82] or trade secrets.

Currently, the European market for electronic health records (EHR), accounts for $2.37 billion in 2024, and with a rising use of electronic health data solutions in hospitals, and particularly clinics and ambulatory surgical centres, it is forecasted to reach $3.94 billion in 2034, the biggest geographic markets being the UK and Germany.[83] While an important share of this market is currently held by hospitals (using their proprietary systems), specialized EHR commercial providers/EHR vendors, such as Epic and Cerner/Oracle, both US healthcare software companies, which incorporate AI advancements in their software, have come to dominate the European EHR market for both inpatient and outpatient. This is a concentrated market with the top 3 firms in the most advanced EHR US market representing more than 70% of the market in 2024.[84] To the value of the European health data market, one should add the value

[78] This Section partly draws on some materials included in a Section of the HCC, Market Inquiry in Healthcare, https://www.epant.gr/en/enimerosi/health.html, drafted by the author. The author would like to thank Christy L. Kollmar for some joint research work on some aspects of the topic covered in this Section.

[79] See, https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion.

[80] See, https://www.mckinsey.com/industries/healthcare/our-insights/the-next-wave-of-healthcare-innovation-the-evolution-of-ecosystems.

[81] Consolidated text: Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, https://eur-lex.europa.eu/eli/dir/1996/9/2019-06-06.

[82] Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions, (1998) OJ L 213/13, Art. 5(2). For a discussion of the broader public interest raised by patent policy regarding human genes and different tools employed to ensure that gene patents do not impede innovation and the practice of medicine and scientific progress, see L.B. Andrews, Genes and patent policy: rethinking intellectual property rights, (2002) 3 Nature Reviews Genetics 803.

[83] See, https://www.factmr.com/report/europe-electronic-health-records-market.

Table 1. Types of health-related data

Type of data	Examples	Data holder
Clinical data	Patient data, such as demographics, medical history, diagnoses, immunizations, medical notes, laboratory and radiology data and vitals	Doctors Hospitals
Clinical trial data	Clinical trials, early-stage R&D data	Pharmaceutical companies
Lifestyle data	Search results, mental state and emotions: fears and attitudes, health related data (for example, diet, exercise)	Online marketplaces Search engines Mobile apps Digital device manufacturers (for example, smart watches, smartphones)
Healthcare data	e-healthcare applications in which smart sensors and microscopic devices outside or inside the human body collect necessary medical information and exchange data related to health care and contribute to finding ehealthcare solutions	Medical device companies
Medical data record and history	Information on the patient's injuries, surgeries, immunisations, medicines taken, results of physical exams and tests	Health care and insurance providers
Genetic and other 'omics' data	DNA (genomics), RNA analysis (transcriptomics), proteomics (proteins), metabolomics (metabolites)	DNA testing companies (such as Illumina, Ancestry DNA), metabolomic services companies such as Metabolon, biobanking companies, and so forth.
Data on costs, quality and consumption of pharmaceuticals and healthcare	Pharmaceutical prescription activity, data on hospitalisation activity, mortality data, healthcare surveys, national statistics	Public health authorities, insurance companies and specific health data companies (for example, IQVIA)
Healthcare-related financial data	Payments to doctors, for hospital care, pharmaceutical consumption	Financial institutions (banks, payment cards companies)

of the health-related lifestyle data, held by Big Tech platforms, or the data on the consumption of pharmaceuticals (again a concentrated market with large players such as IMS, IQVIA), thus expanding the market further to the broader digital health ecosystem.

Of particular interest is also the recent move of Big Tech to the healthcare sector with a series of reported data-sharing agreements, partnerships and acquisitions, which may disrupt the legacy players in the wider healthcare and health insurance industry.[85] The example of Google's expansion in the digital health space has already been thoroughly examined in the economic

[84] These are Epic Systems Corp (38%), Oracle/Cerner (22%), Meditech (13%), also present in a number of jurisdictions outside the US. See, https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems.

[85] See, DoHealth-CareCompaniesShareMyData?AnalysisFindsTheyDo-Bloomberg; https://www.emarketer.com/insights/big-tech-in-healthcare-report/; Big Tech players make big healthcare moves in 2022 (emarketer.com); insights51.pdf (bis.org). However, for a different conclusion as to the low likelihood of a disruption of the healthcare market and its legacy players, see Why the Tech Industry Won't Disrupt Health Care (hbr.org)

literature.[86] One could also cite the recent incursions of Amazon in the health space, with the acquisition of PillPack in 2018 and two years later with the launch of Amazon pharmacy, or its ventures in healthcare services delivery, with the acquisition of One Medical in 2022,[87] and the development of Alexa health-related products/features for remote caregiving services (Alexa Together and Alexa CareHub). Apple has also ventured in digital health and digital therapeutics with products like Apple Watch, which has incorporated health monitoring features to improve cardiovascular health, including the ability to track one's heart rate, blood oxygen levels, or glucose monitoring, disrupting the competitive position of specialized existing market players in this market,[88] and the launch of platforms like HealthKit which may compete with medical equipment companies,[89] or its acquisition of Gliimpse already in 2016, a personal health data platform which harvests user data from labs, hospitals and pharmacies, and the launch of HealthApp, allowing users to store, visualize and share their health data,[90] or of Vision Pro, a mixed-reality headset which enhances visualization in diagnostic imaging and surgical planning.[91] Microsoft has built tools for digital health in its cloud services Azure, such as the Azure Health Bot or FlyWheel, a medical imaging AI.[92] Big Tech also spearheads the use of AI in digital health further accelerating the convergence of digital and physical healthcare solutions, such as Amazon's Comprehend Medical, a natural language processing service extracting health data from medical prescriptions, procedures, or diagnoses, or the launch of purpose-built tools in AWS Health Services, such as HealthLake which aggregates, standardizes and structures health data, and HealthImaging, storing medical images and analysing them with AI.[93] Microsoft's DAX Copilot uses AI to write up clinical summaries integrated with electronic healthcare records and Microsoft's Fabric which stores and analyses healthcare data.[94] Nvidia has recently focused on technological advancements in vision language models (VILA), replicating physical environments to develop healthcare digital twins, and has recently launched Isaac for healthcare, an AI-driven surgical system relying on detailed biomechanical simulations which also generate anatomical synthetic data required for the simulations.[95]

Recent market studies have put forward a four-steps strategy of 'digital colonisation' by Big Tech of the digital health space.[96] First, they supply data infrastructure services to primary care providers (hospitals) typically lack capabilities in data management in exchange for data access. Second, they leverage these relationships to gain indirect access to health data developing unique universal databases capturing data from multiple channels that establish a competitive

[86] See C. Rikap, The expansionary strategies of intellectual monopolies: Google and the digitalization of healthcare, (2022) 52(1) Economy and Society 110.

[87] G. Growth, The Rise of Big Tech in Healthcare: Opportunities and Challenges (June 24, 2024), available at https://www.galengrowth.com/the-rise-of-big-tech-in-healthcare-opportunities-and-challenges/

[88] Privacy International, Digital health, big tech and your privacy (November 7th, 2024), available at https://privacyinternational.org/long-read/5451/digital-health-big-tech-and-your-privacy.

[89] J. Mendes-Roter, Friend or Foe? A Look at Big Tech's Impact in the Digital Health Space, Forbes (November 26, 2025), available at https://www.forbes.com/councils/forbescommunicationscouncil/2024/11/26/friend-or-foe-a-look-at-big-techs-impact-in-the-digital-health-space/

[90] Privacy International, Digital health, big tech and your privacy (November 7th, 2024), available at https://privacyinternational.org/long-read/5451/digital-health-big-tech-and-your-privacy.

[91] N.M. Shanbhag, A. Bin Sumaida, K. Al Shamisi, K. Balaraj, Apple Vision Pro: A Paradigm Shift in Medical Technology. Cureus. 2024 Sep 17;16(9):e69608. doi: 10.7759/cureus.69608.

[92] Privacy International, Digital health, big tech and your privacy (November 7th, 2024), available at https://privacyinternational.org/long-read/5451/digital-health-big-tech-and-your-privacy.

[93] Ibid.

[94] Ibid.

[95] M. Tolooui et al., Introducing NVIDIA Isaac for Healthcare, an AI-Powered Medical Robotics Development Platform 9March 18, 2025), available at Introducing NVIDIA Isaac for Healthcare, an AI-Powered Medical Robotics Development Platform | NVIDIA Technical Blog.

[96] H. Özalp, How Big Tech is breaking into the healthcare sector (Said Business School, August 8th, 2022), available at https://www.sbs.ox.ac.uk/oxford-answers/how-big-tech-breaking-healthcare-sector.

bottleneck. Third, they use AI trained because of access to this data to provide superior data-driven insights, developing important network effects and technological dependencies striking deals with public and private health services provides (for example, NHS trusts in the UK). Finally, the fourth step involves the development of new purpose-built products and services in digital health, such as non-invasive devices or complimentary services that commoditize the primary care companies which continue to provide the main infrastructure of patient care at their cost, while Big Tech focuses on the valuable segments of the human health value chain.

The use of personal health data by companies with market power or through a central position in an ecosystem may be found, under certain conditions, to constitute anti-competitive exclusion and to also produce effects of an exploitative nature. Regarding the exclusionary effects, as is the case with other types of personal data, human health data sources are heterogeneous—qualitative and quantitative, with the data collected at different time intervals and in different contexts. There exist also population-based datasets from public health authorities, insurance companies, and specific health data companies that harvest data on the cost and consumption of pharmaceuticals or healthcare use over the lifetime. However, unlike other personal data that is also collected and usually widely available (for example, through intermediaries/brokers), health data may be more difficult to access due to its special status and the legal protection provided. This can sometimes lead to a greater likelihood of input or customer foreclosure-type business practices. Health data (including genetic and omics data) can be personal or non-personal based on identifiability and sensitivity. Health data, including genetic and omics data, may be characterized as personal or non-personal depending on the identifiability of individuals and whether it reveals sensitive information. However, the critical consideration should not be the data's status or its *ex ante* classification but rather its proposed use, the scope of access requested, and the data's uniqueness and 'informational content'.[97]

Personal data are subject to a protective legal regime, which may raise barriers to a wide sharing of data.[98] Article 8 of the Charter of Fundamental Rights of the European Union describes the right to the protection of personal data, in conjunction with the General Data Protection Regulation (GDPR), which lays the foundations for the processing of personal data. The latter recognizes health data care as a distinct 'category of data' and provides a definition of health data for data protection purposes, where it invokes clearly defined safeguards for personal health data and provides legal transparency and certainty when interpreting the rules to 'enable effective and comprehensive protection' of such healthcare data.[99] In general, the GDPR provides more rights to citizens in understanding how their personal health data is used and delineates clearer obligations/responsibilities for data controllers/users regarding the proper consumption of personal health data (for example, disease management and promotion of health research).[100]

Recital 35 of the GDPR defines health data as 'all data pertaining to the health status of a data subject, which reveal information relating to the past, current or future physical or mental health

[97] J. Rahnasto, Genetic data are not always personal—disaggregating the identifiability and sensitivity of genetic data, (2023) 10(2) *Journal of Law and the Biosciences*, lsad029.

[98] C. Legido-Quigley, N.J. Wewer Albrechtsen, M. Bæk Blond, *et al.* Data sharing restrictions are hampering precision health in the European Union, (2025) 31 *Nature Medicine* 360–361.

[99] See, Health | European Data Protection Supervisor (europa.eu); 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, OJ L 119, 4.5.2016/1

[100] 'The new EU Regulation on the protection of personal data: what does it mean for patients?,' European Patients Forum, https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf, 3 & 21.

status of the data subject.[101] When narrowing the focus to the particular types of healthcare-related data regulated by the GDPR, Article 4 highlights and defines three important categories, within which the lawfulness of their processing merits further discussion: 'genetic data',[102] biometric data'[103], and 'data concerning health'.[104] For data processing, Article 6 provides that the processing of general data (non-health-related data) is lawful if at least one of the criteria explicated in (a) to (f) applies.[105] For health-related data, Article 9 additionally imposes further requirements for the processing of genetic data, data concerning health, and identification-related biometric data,[106] prohibiting the use of such data[107] unless one of the criteria explicated in (a) to: '(a) the data subject has given explicit consent to the processing of [said] personal (j) applies.[108]

Article 7 of the Charter of Fundamental Rights of the European Union and the ePrivacy Directive (ePD),[109] to be replaced by the proposed ePrivacy Regulation (ePR),[110] which aims to protect 'the confidentiality of communications and the rules on tracing and monitoring' of data,[111] also specifically address the confidentiality of electronic communication and the privacy controls associated with the use of digital cookies, browsers, trackers and electronic consent. This expands the scope of the important revisions proposed by the European Parliament in the ePrivacy Directive with the aim of 'specializing and supplementing it in terms of electronic communications data characterized as personal data', with any aspect beyond the proposal covered by the text of the GDPR itself. The GDPR and the ePD should be read together to fully regulate the processing of personal data.

One salient problem emerging in this context is the digital health bottleneck or hold-up that can occur due to the sensitivity of health data and its inability for (and/or protection from) easy access and sharing. Especially in the wake of COVID-19, where fast action and 'coopetition' was crucially needed,[112] patients were still facing complexity with navigating health services and data protection/access. Healthcare systems are usually struggling with inadequate resourcing/interoperability and administrative woes, and efficacious regulatory solutions are either non-existent or inadequate to keep up with technology causing 'severe administrative waste' via fragmentation and unneeded complexity.[113] As health data increases exponentially in both

[101] Intersoft Consulting, 'Recital 35—Health Data—General Data Protection Regulation (GDPR),' accessed 08 December 2022, https://gdpr-info.eu/recitals/no-35/. It should be noted that this health data includes information 'collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU' (see Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45)); see also GDPR, Recital 35.

[102] GDPR, Article 4, Definitions-Genetic data. Genetic data is defined as: 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'.

[103] GDPR, Article 4, Definitions-Biomedical data. Biomedical data is defined as: 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'.

[104] GDPR, Article 4, Definitions—Data concerning health. Data concerning health is defined as: 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

[105] GDPR, Article 6, Lawfulness of processing.

[106] GDPR, Article 9, Processing of special categories of personal data.

[107] GDPR, Article 9(1).

[108] European Patients Forum, 'The new EU Regulation on the protection of personal data', 5; see also, GDPR, Recital 32.

[109] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37.

[110] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM/2017/010 final.

[111] See, ePrivacy Directive | European Data Protection Supervisor (europa.eu).

[112] I. Lianos, T. Minssen, C. Kollmar, Tackling Grand Challenges with Competition Law: Lessons from the Pandemic, in W. Sauter, M. Canoy, J. Mulder (eds.), *EU Competition Law and Pharmaceuticals* (Edward Elgar Publishing, 2022) 281.

[113] B. Lee, Data—The Core Bottleneck to Digital Health—Overview', Medium.com, 04 April 2020, https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-1-a177f4882882.

variety and volume, the scope of healthcare's data problem, caused by a lack of interoperability, standardisation, and usability, becomes more exacerbated and cumbersome.[114] In addition, claims for intellectual property rights or to protect trade secrets may also prevent access to certain types of data.

The importance of health data for the development of new technological applications of personalized medicine and the competitive advantages offered by access to them certainly raise issues of competition policy.[115] As noted above, the development of digital technology has led to the emergence of a new set of powerful actors, digital intermediaries, with the 'matching' function of various customer groups analysing various kinds of data collected continuously from the various user groups. These entities operate according to the platform model, developing ecosystems that tend to become the focal point of the specific value chain.[116] By collecting a huge amount of health-related data and developing sophisticated algorithms and artificial intelligence, digital technology companies have also recently become important players in medical and insurance services.[117] Their strategy may consist of developing strategies of both cooperation with their ecosystem members, as they operate (orchestrate) the platform on which their ecosystem partners rely to distribute their services and products to consumers, and strategies of competition at an horizontal level in their capacity as platform and merchant, but also at the vertical level due to the competition between platform and partners for the surplus value generated from the ecosystem.[118]

The organisation of companies as platforms and the complex economy of multifaceted markets may blur the traditional boundaries of markets as perceived by competition law and the regulatory framework. This development may have the effect of making the distinction between the different segments of digital health, such as the health care value chain and the health insurance value chain, less clearcut concerning the study of their effects on competition.

Current trends in the healthcare industry require a tech-empowered regulatory solution that dismantles bottlenecks and promotes interoperability and standardisation in the protection/access and proper usage of healthcare-related data.[119] Any regulatory intervention includes the intention to provide patients with inexpensive alternatives for accessing/protecting data through third-party applications, data interoperability and sharing being enhanced to reduce redundancy and overuse of sensitive data.[120]

[114] B. Lee, Data—The Core Bottleneck to Digital Health—Parts 4 and 5′, Medium.com, 04 April 2020, https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-4-6561eaee3af6 and https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-5-b5f6ba569bbb.

[115] Council conclusions on Health in the Digital Society—making progress in data-driven innovation in the field of health, (2017/C 440/05); Communication from the Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final; Communication from the Commission, on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final.

[116] C. Dive-Reclus & T.M. Jaeger, Digital Ecosystems are the Future of Healthcare, Harvard Business Review (Oct. 19. 2022), https://hbr.org/sponsored/2022/10/digital-ecosystems-are-the-future-of-health-care; Deloitte, The power of network ecosystems—How platforms can be a force-multiplier in health, (2021), https://www2.deloitte.com/us/en/pages/advisory/articles/the-power-of-health-care-ecosystems-and-platforms.html.

[117] Insider Intelligence, Big Tech in Healthcare, https://www.insiderintelligence.com/insights/big-tech-in-healthcare-report/.

[118] A Brandenburger and BJ Nalebuff, *Co-opetition* (Doubleday, 1997); Pant, V. & Yu, E. (2016). Coopetition with frenemies: Towards modeling of simultaneous cooperation and competition among enterprises, 9th IFIP Working Conference on The Practice of Enterprise Modeling (PoEM), Available online: https://hal.inria.fr/hal01653530/file/416579_1_En_12_Chapter.pdf.

[119] B. Lee, Data—The Core Bottleneck to Digital Health—Parts 4 and 5′, Medium.com, 04 April 2020, https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-4-6561eaee3af6 and https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-5-b5f6ba569bbb.

[120] L. Ben, Data—The Core Bottleneck to Digital Health—Parts 4 and 5, Medium.com, 04 Απριλίου 2020, https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-4-6561eaee3af6 and https://medium.com/@btlee215/data-the-core-bottleneck-to-digital-health-part-5-b5f6ba569bbb.

Traditionally foreclosure/bottleneck concerns have been addressed either by applying the competition rules in advance (ex-ante) to mergers, for example, in case the conditions of theories of uncoordinated effects due to vertical anti-competitive foreclosure of inputs (input foreclosure) or customer (customer foreclosure) are met, but also of coordinated effects in certain cases, or through the application of competition rules afterwards (*ex post)* against various practices of offensive or defensive leverage (for example, tied sales, tied discounts, agreements or exclusivity discounts) that may lead to anti-competitive effects.[121] Related theoretical economic models examine how a platform can monopolize a multi-sided market. The user may generate revenue in the subsidising market by profitably enveloping another platform market with overlapping users (the target market) and linking data protection policies across the two platform marketplaces for the platform to (a) combine data generated by common users in both marketplaces without violating privacy regulations and (b) generate new revenue streams from a rich and difficult-to-replicate source data on the dominant platform of origin.[122]

A business can block/restrict competitors' access to data (or data-driven technological facilities/algorithms) in a vertical market it controls under the guise of protecting user privacy while simultaneously providing access to the same data for the companies it controls in the same markets. Such a strategy may provide the company in question, particularly in the health sector, a significant competitive data advantage and limit its competitors' access to secondary data markets. This would allow it to better target its products and services (particularly in personalized medicine services). It may thus succeed in extending its power to vertical markets and impose unfair conditions limiting the ability of users to choose the way their data is used.[123] Another theory of harm is that through vertical market (quasi-) integration, the merged entity may gain access to commercially sensitive information about the activities of its competitors operating in the upstream or downstream markets, which would allow it to apply a less aggressive pricing policy in the downstream market to the detriment of consumers, and to put its competitors at a competitive disadvantage. It may discourage their entry or expansion in a vertical market helping the digital platform to maintain its monopoly/market power[124].

Using synthetic data may offer a solution to the challenges inherent in getting access to high-quality health datasets, and particularly offer 'an attractive alternative that addresses privacy concerns, streamlines data, utility agreements, protocol submissions, and ethics review approvals', thus decreasing costs.[125] Synthetic data has been defined as 'data that has been generated using a purpose-built mathematical model or algorithm, with the aim of solving a (set of) data science task (s)'.[126] It is acknowledged that '(s)ynthetic data has the potential to estimate the benefit of screening and healthcare policies, treatments, or clinical interventions, augment machine learning algorithms (for example, image classification pipelines), pre-train machine learning

[121] Linsey McCallum, Inge Bernaerts, Massimiliano Kadar, Johannes Holzwarth, David Kovo, Marie Lagrue, Edouard Leduc, Luca Manigrassi, Jorge Marcos Ramos, Isabel Pereira Alves, Vera Pozzato, Pinelopi Stamou, A dynamic and workable effects-based approach to abuse of dominance, Competition Policy Brief, March 2023, Issue 1, https://competition-policy.ec.europa.eu/system/files/2023-03/kdak23001enn_competition_policy_brief_1_2023_Article102_0.pdf.

[122] D. Condorelli, J. Padilla, Harnessing Platform Envelopment in the Digital World, *Journal of Competition Law & Economics*, Volume 16, Issue 2, June 2020, Pages 143–187; D. Condorelli & J. Padilla, Data-Driven Envelopment with Privacy-Policy Tying (May 12, 2020). Available at SSRN: https://ssrn.com/abstract=3600725. See also, N. Economides, I. Lianos, Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective, (2021) 17(4) Journal of Competition Law & Economics, 765.

[123] See, UK Competition & Markets Authority, Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals, Case number 50972 (Feb. 11, 2022).

[124] 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, *OJ C 259, 21.7.2023, p. 1.*

[125] M. Giuffre & D.L. Shung, Harnessing the power of synthetic data in healthcare: innovation, application, and privacy, *npj Digit. Med.* **6**, 186 (2023). https://doi.org/10.1038/s41746-023-00927-3, 1.

[126] J. Jordon J. et al., Synthetic Data—what, why and how? arXiv: 2205.03257 [cs], (2022), available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/Synthetic_Data_Survey-24.pdf.

models that can then be fine-tuned for specific patient populations, and improve public health models to predict outbreaks of infectious diseases'.[127] The 'synthetic' nature of the data is a matter of degree as data may be partially or fully synthetic, the latter not containing any real-world data. Fully synthetic data may also 'address the issue of data scarcity that may affect both linear and non-linear models as well as the rapidly proliferating large language models by creating supplementations to the available datasets'.[128] However, their use has also shown the risks of bias, problems related to the representativeness of the data, and other systematic discrepancies or deviations from the 'real data', with the consequence that trust has decreased 'in clinical diagnosis derived from AI-based prediction models using synthetic datasets'.[129]

Privacy concerns may persist as it cannot be excluded that unintentionally synthetic data may disclose identifiable details about individuals or lead to reidentification, with different methods (such as differential privacy being employed to mitigate that risk).[130] In recent years, some have also questioned the role of access to large datasets as an essential part of the competitive advantage of Big Tech firms, with the view that it is AI and data analytic capabilities that are more crucial[131] also raising the possible use of synthetic data as a way out of the data bottleneck.[132] Recent research, however, has shown that synthetic data are not that effective,[133] as they collapse when they are trained in recursively generated data, and that access to real-world data is an essential ingredient for the success of new AI large language models (LLMs).[134] The problem has become apparent in the context of web-sourced datasets whose heterogeneity and scale has been key for the development of LLMs. The proliferation of data restrictions has also raised concerns about the 'rapid decline' of these 'AI Data Commons'.[135] This highlights the crucial role regulators and competition authorities may play in promoting fair access and sharing of data.

The following Sections will engage with the institutional framework put in place to deal with such bottleneck/foreclosure problems, as well as the possible entrenchment of ecosystem power in digital health. We will explore respectively the regulation of the interactions regarding access to data, first between the ecosystem orchestrators/digital platforms and end-users, second, between the ecosystem orchestrators/digital platforms and their business users/complementors, and finally between third-party businesses and digital platforms for the data end-users generate in the use of their digital health ecosystems.

IV. THE RELATION BETWEEN ECOSYSTEM ORCHESTRATORS/DIGITAL PLATFORMS AND END-USERS: ESTABLISHING THE 'FAIRNESS' INTERVENTION THRESHOLD

A. The Nature of the Distributional Problem

Discussions over the relation between the digital platforms and their end-users often delve into concepts of exploitation and 'surveillance capitalism'. Harvesting data without providing

[127] M. Giuffre & D.L. Shung, op. cit., 2 & 3 (providing examples of such use in healthcare).
[128] Ibid., 2.
[129] Ibid., 1.
[130] Ibid.
[131] See, N. Srnicek, Data, Compute, Labor, in Graham, M. and Ferrari, F. (eds.), *Digital work in the planetary market* (MIT Press. 2022), 241, 244–245.
[132] See, for a discussion, M.S. Gal & O. Lynskey, Synthetic Data: Legal Implications of the Data-Generation Revolution, (2024) 109 Iowa L. Rev. 1087.
[133] See, A. Germani, The Politics of Artificial Intelligence in Healthcare: Diagnosis and Treatment, In *AI and Society* (pp. 33–48). 2023, Chapman and Hall/CRC, 35–36; K. El Emam, Could Synthetic Data be the Future of Data Sharing?, (August 5, 2021), available at ttps://www.cpomagazine.com/data-privacy/could-synthetic-data-be-the-future-of-data-sharing (the prediction accuracy for models using synthetic data tends to be within 2–5% of the original data).
[134] I. Shumailov, Z. Shumaylov, Y. Zhao, *et al.* AI models collapse when trained on recursively generated data. *Nature* 631, 755–759 (2024). https://doi.org/10.1038/s41586-024-07566-y.
[135] See more recently, S. Longpre et al., Consent in Crisis: The Rapid Decline of the AI Data Commons, (2024), arXiv:2407.14933, also available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.dataprovenance.org/Consent_in_Crisis.pdf.

any form of compensation other than access to free services, inevitably produces distributional implications. One way to deal with these is to enact regulations that will provide some rights to the end-users. Although not traditionally considered a distributive justice tool, the GDPR and the ePrivacy Directive in the EU became the main policy instruments and generally applicable safeguards until the adoption of the DMA, Data Act and Digital Services Act (DSA), to regulate the market for data. They had, first, the minimum goal to ensure that personal information flows occur in accordance with the expectations of the users (hence the emphasis put on consent), and second, to restrict these information flows with regard to certain sensitive data. They played the role of a horizontal omnibus regulation as the same rules apply to any use of personal data and to any type of company whatever its size and power. This seemingly 'neutral' choice for horizontal privacy-promoting policies, as Goldfarb and Tucker rightly explain, has a redistributive impact to the extent that the direct benefits or negative externalities of information flows differ across socioeconomic groups and even in a horizontal data relation context some may benefit from privacy while other may lose, from an economic welfare perspective.[136]

Due to its horizontal dimension, the GDPR constitutes an imperfect tool to tame the asymmetrical bargaining power of digital platforms, on which an important part of the population depends in its day-to-day life for work and entertainment, and increasingly also healthcare.[137] As put forward in a previous publication, in a normally functioning market for personal information, transaction prices would depend on the willingness of the digital platform to buy and the willingness of a user to sell their personal information.[138] How much a user's personal information is worth to them differs in general from how much it is worth to a platform. What may seem like a small loss today may turn out to be a significant loss in the future. Even if the user can precisely estimate the value of his/her private information, it is likely that this value would differ from the value of this information to the digital platform to the extent that the value of the personal information to the platform may come as a derived demand, for instance, from the process of selling advertisements to that user or selling to third parties in secondary data markets. The value to the platform is also enhanced by the availability to it of other complementary data that the user may not be aware of.

The difference in the value of personal information between the user and the platform is a distributive issue, but traditionally this has not been considered as a competition policy concern. Parties trade goods and services when they have different valuations or willingness to buy, and willingness to sell. This is normal in markets. However, dominant digital platforms orchestrating business ecosystems may intervene in the flow of data, by imposing contractual or technological arrangements for its harvesting or use. They may exploit the data predominately to their own benefit, instead of that of their business or end-users. For instance, requirement contracts imposing as a default 'opt-in' under which the data is automatically collected by the platform may enable digital platforms to harvest the data without providing compensation to users beyond the in-kind compensation that they might receive from using the digital platform's product or service for 'free'. Thus, the data market collapses in the digital services (for example, search engine) market, and all transactions occur at a single zero nominal price. As we have

[136] A. Goldfarb & C. Tucker, Inequality, privacy, and digital market design, available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://static1.squarespace.com/static/5f03515f47274a7fa3017d54/t/5fa87ee94f8f02449ad5c073/1604878057957/GoldfarbTucker_digital_inequality.pdf.See also, S. Viljoen, A Relational Theory of Data Governance, (2021) 131(2) The Yale Law Journal 573.

[137] See, S. Hermes, T. Riasanow, E.K. Clemons *et al.* The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients, (2020) 13 Bus Res 1033; N. Domnisch, Digital Healthcare Ecosystems Are Changing Healthcare As We Know It (Forbes, April 25, 2022), available at https://www.forbes.com/councils/forbestechcouncil/2022/04/25/digital-healthcare-ecosystems-are-changing-healthcare-as-we-know-it/.

[138] N. Economides & I. Lianos, Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective, (2021) 17(4) Journal of Competition Law & Economics 765, https://doi.org/10.1093/joclec/nhab007

explained elsewhere, this is a market failure, implemented in favourable terms to the dominant platform.[139]

The expansion of an ecosystem and thus the ability of the platform to harvest more data, also enhances the platform's control of the business ecosystem and reinforces its central position in it. Indeed, all data is harvested by and can be accessed through a proprietary platform. The enhancement of the dominant position in the primary market of the platform allows in turn the platforms to make more users accept the requirement, bundling and other forms of obligations they impose to them, thereby increasing the group of users who accept these and the harm to them.

Note that what the GDPR and the privacy regulation do is to take care of the risk that users have been imposed conditions to which they did not provide their voluntary consent by changing the 'default' regime from 'opt-in' to 'opt-out.'[140] However, this is far from sorting out the distributive justice problem, as even if one changed to 'default opt-out' this will not provide an adequate response to the problem of misappropriation of rents/surplus. Indeed, the dominant platform may impose, because of its asymmetric power linked to its dominance, the conditional use of the platform to the 'consent' provided by the users of their data being harvested. Hence, an 'opt-out regime' will not be sufficient because of the asymmetrical bargaining power between the digital platforms and the users.

This brings forward a second issue: the nature of the 'consent' required for the use of personal data. Should consent be regarded as freely given to an undertaking which is the dominant platform? Should the GDPR and privacy regulation tools be complemented by additional horizontal not omnibus regulations, taking precisely into account the issue of bargaining asymmetry, which as mentioned above is not accounted for sufficiently by the GDPR?[141]

B. The Use of the Competition Law Toolkit

This gap in legal protection first led to calls for antitrust enforcement against the risk of non-price exploitation of end-users and explains cases such as the BkA *Facebook* case,[142] or more recently the *Apple App store* case.[143] 'Excessive' health data extraction as well as unfair commercial practices that are likely to harm end-users may constitute a concern for EU competition law. Although excessive health data extraction concerns personal data, and unfair commercial practices do not always constitute a data restriction of competition, both define the distributional problem in terms of power differential and set some broad principles that could be applicable to both situations. We will not focus here on 'excessive' data extraction as such, which is explored in a different publication,[144] which raises interesting questions about the application of the price/economic value *United Brands* test for exploitative conduct that was initially developed for excessive *pricing* practices,[145] but on instances of non-price exploitation following unfair commercial practices or unilateral restrictions to privacy.

[139] Ibid.

[140] GDPR could arguably do a lot more on this through Article 5 GDPR.

[141] For a discussion as to how the GDPR may better consider this asymmetrical situations: see, O Lynskey, Complete and Effective Data Protection, (2023) 76(1) Current Legal Problems, 297.

[142] Bundeskartellamt.2019.FacebookDecisioninAdministrativeProceedings,B6–22/16, (hereinafter BKA).

[143] European Commission, CASE AT.40437—Apple—App Store Practices (music streaming) (2024).

[144] N. Economides, I. Lianos, Restrictions On Privacy and Exploitation in The Digital Economy: A Market Failure Perspective, (2021) 17(4) Journal of Competition Law & Economics, 765, first version published as part of the BRICS Competition in the Digital Era Report (2019), available at https://bricscompetition.org/uploads/publications/brics-book-full-00d8c66ce2.pdf; V. H. S. E. Robertson, Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data, (2020) 57(1) Common Market Law Review 161.

[145] Case 22/76, United Brands Company and United Brands Continental BV v Commission [1978] ECR 207.

In the well-known *BkA* case, Facebook merged and collected the various sources of personal data that had been generated by users of the services owned by Facebook, services like WhatsApp or Instagram (Facebook-controlled services), and aggregated this collection of data with that which had been generated by users of third-party websites and apps in which Facebook products, such as the 'like' button and Facebook analytics, had been embedded (the Facebook third party ecosystem). The *BkA* differentiated between user data that had been generated through users using the Facebook service, and user data obtained from third-party sources that were either controlled by the Facebook corporate group, such as WhatsApp, Oculus, Masquerade and so forth, or through the use of Facebook programming interfaces on third-party websites or mobile apps (through the Facebook developer platform and Facebook Business Tools). This formed part of the broader third-party Facebook ecosystem. The *BkA* considered that the latter set of user data had not been generated through users using Facebook's social network and, as such, Facebook had not received users' consent in relation to it. This raised concerns as users were no longer able to control the way in which their personal data was used.

The reasoning the *BkA* undertook presents some interest as to the relation between harm to competition (competition law) and harm to data protection (data protection law). The BkA found that FB's conduct was a manifestation of its market power, as an undertaking without market power would not have been able to impose such unfavourable conditions and consumers were placed in a 'take-it-or-leave-it' position in the national social network market. There was at least a 'normative causality' (but not strict causality) between this dominant position and the reduction in privacy resulting out of the infringements of data protection rules. This simultaneously constituted a violation of users' constitutionally protected rights to informational self-determination.[146]

According to the *BkA*, to protect constitutional rights, the German competition law provision against unilateral conduct (§ 19 GWB) must be applied in cases where one contractual party is so powerful that it is practically able to dictate the terms of the contract, and the contractual autonomy of the other party is *abolished*. If in such a case a dominant company disposed of the constitutional rights of its contractual partners, the law had to intervene to uphold the protection of such rights. The damage for the users lies in a loss of control: they are no longer able to control how their personal data are used. Facebook's users are oblivious as to which data from which sources are being merged to develop a detailed profile of them and their online activities.

In its remedy, the BkA differentiated between user data that are generated through the use of Facebook ('on Facebook') and user data obtained from third-party sources ('off Facebook') The *BkA*'s case concerned only the second and the BkA did not examine the use of data generated by the use of Facebook's social network itself.

The case of course went to the higher courts[147] and ended with a preliminary reference to the Court of Justice (CJEU).[148] One of the issues examined at the CJEU was the power dimension which was not crucial at an operational level in the context of the GDPR but certainly

[146] The BkA referred in this context to *Pechstein,* a case in which the imbalance of power concerned the relation between an athletic association, the International Skating Union and an athlete, Ms Pechtein, who had suspended for two years from international competitions, following a decision of the ISU, later confirmed by the Court of arbitration for Sport (CAS) which was the only forum available to Ms Pechtein to challenge her suspension, and which had dismissed her request for a public hearing as well as her claim. At first instance, the German District Court of Munich found that the arbitration agreement was void for violating competition law (see LGMunich I, judgment of 26.02.2014–37 O 28331/12). Following a long judicial saga that also involved a decision by the ECHR, the German Constitutional Court (BVerfG) found that the arbitration clause was null in view, among other issues, the imbalance of power in the specific setting of sports between sports associations and the athletes that had triggered in this case the application of competition law: *BVerfG*, Beschluss vom 3.6.2022, 1 BvR 2103/16.

[147] With the Dϋsseldorf Higher Regional Court taking annulling the BkA's decision, while the Federal Court of Justice overturned the Higher Regional Court's judgment.

[148] Case C-252/21, Meta Platforms and Others, ECLI:EU:C:2023:537.

not ignored. As AG Rantos opined, '[. . .] any dominant position on the market held by a personal data controller operating a social network is a factor when assessing whether users of that network have given their consent freely. Indeed, the market power of the controller could lead to a clear imbalance [. . .]. However, it should be clarified that for such a market power to be relevant from the point of view of enforcing the GDPR, it need not necessarily be regarded as a dominant position within the meaning of Article 102 TFEU. Besides, that circumstance alone cannot, in principle, render the consent invalid'.[149] Rantos thus suggested the 'validity of the consent' to be examined 'on a case-by-case basis, [. . .] taking into account all the circumstances of the case and the controller's responsibility to demonstrate that the data subject has given his or her consent to the processing of personal data relating to him or her'.[150]

The CJEU followed the emphasis put by its AG on the power element. Referring to Recital 43 the GDPR, the Court held that the existence of a dominant position may create a clear imbalance between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the contract.[151] In this context, the CJEU indicated that the processing of personal data done by Facebook (now Meta) was not strictly necessary for the performance of the contract between it and the users of the social network Facebook. It also reaffirmed the principle that 'users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations'.[152]

The CJEU also favoured a more in-depth analysis of the existence of real 'consent' in the competition law assessment. This involves considering the burden that rests on the data comptroller according to Article 7(1) GDPR,[153] and the asymmetry of power that exists in some circumstances. For instance, when consent is provided to a dominant social network (or for our purposes a digital health platform), the BkA recognized the network is likely to benefit from strong direct and indirect network effects. There was also no option for users to engage in multihoming. Instead, they suffer from high switching costs due to identity-based network effects, the users' network not being able to switch or interoperate with another social network. With this interpretation, the CJEU's judgment thus enabled a substantive rather than a formal-only understanding of the principle of 'freely given' and 'informed' consent, mentioned in Recital 32 of the GDPR, and emphasized the concerns mentioned in Recital 43 of the GDPR over 'genuine and free choice'[154] in the presence of asymmetry or 'imbalance' of power. This, beyond the public authority-user relation that was explicitly acknowledged by the text of the GDPR, to cover also situations of private power and economic coercion. While the CJEU acknowledges that 'the fact that the operator of an online social network, as controller, holds a dominant position on the social network market does not, as such, prevent the users of that social network from validly giving their consent',[155] it also instructs the national courts to 'determine whether the users of the social network Facebook have validly and, *in particular, freely given*

[149] Opinion of AG Rantos, in Case C-252/21, Meta Platforms and Others, ECLI:EU:C:2022:704, para. 75.
[150] Ibid., para. 76.
[151] Case C-252/21, Meta Platforms and Others, ECLI:EU:C:2023:537, para. 149.
[152] Ibid., para. 150.
[153] According to Article 7(1) GDPR, 'Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data'. Following Art. 7(4), 'When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.
[154] Case C-252/21, Meta Platforms and Others, para. 140.
[155] Ibid., para. 147.

their consent', taking into account as 'an important factor'[156] in determining the validity of the consent, under the GDPR rules, the dominant position of the undertaking concerned.[157]

The *Apple App Store* case may also be analysed as a case aiming to tackle the possible exploitation of end-users by the architectural power of ecosystem orchestrators and the possibility that such design rules of digital (health) ecosystems may consist in unfair trading conditions prohibited by Article 102 TFEU.[158] The case first aimed to deal with the potential exclusionary effects of the App Store rules, particularly regarding the mandatory use of the In-App Purchase (IAP) for several categories of apps offered in the App Store. However, it was subsequently narrowed down to focus on the anti-steering provisions imposed by Apple to the business users in the iOS ecosystem preventing music streaming providers (business users/complementors), such as the complainant Spotify, from informing end-users on Apple mobile devices about alternative subscription possibilities available outside the Apple app store environment.

This issue was framed as an exploitative unfair trading conditions case. First, the anti-steering provisions were 'unilaterally imposed by Apple', an integrated ecosystem orchestrator, on its complementors in the music streaming app services market. The app store was analysed as a multi-sided platform with on one side developers and on the other end-users. Second, these rules were found 'detrimental to the interests of iOS users of music streaming services' (that is, the consumer side of the platform), as these were obliged to pay because of the anti-steering provisions higher music subscription fees than those on other devices, and they were unable to choose from a range of distribution options. Third, they 'were not necessary for the achievement of a legitimate objective or in any event not proportional for that purpose'.[159] Hence, although the abusive conduct took place in the context of the P2B relationship, the Commission focused on the anticompetitive effects produced at the P2C relationship, thus the effect on end-users.[160] An important concern in the case also was the 'quasi-regulatory powers' exercised by Apple 'for determining access conditions for developers to users of iOS devices' and which it could modify 'at any time',[161] a concern over private regulatory power reducing access (eventually to data) that also attracted the CJEU's attention, among others, in the recent *Superleague* judgment, although focusing on a procedural/rule of law perspective, rather than a substantive fairness perspective as it did in *Apple App Store*.[162]

By accepting to engage directly with the way infringements of data protection law may constitute violations of competition law, the Court broke with the more agnostic approach the Commission had followed in the context of the *ex-ante* merger control tool, where in *Facebook/Whatsapp*,[163] *Microsoft/LinkedIn*,[164] *Apple/Shazam*,[165] *Google/Fitbit*[166] and *CVC/Ethniki*[167] it left any possible exploitation concerns, in terms of the potential impact of the merger

[156] Ibid., para. 153.
[157] Ibid., para. 154.
[158] European Commission, CASE AT.40437—Apple—App Store Practices (music streaming) (2024).
[159] Ibid., para. 555.
[160] See, also G. Monti, Exploitative Abuse—Takeways from the Apple App Store Practices Decision, available at. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4853304.
[161] European Commission, CASE AT.40437—Apple—App Store Practices, para. 500.
[162] Case C-333/21, European Superleague Company, ECLI:EU:C:2023:1011, paras 135–138 (noting that when an undertaking 'has the power to determine the conditions in which potentially competing undertakings may access the market or to make determinations in that regard on a case-by-case basis, through a decision on prior authorisation or refusal of such access, that power must, in order not to infringe, by its very existence, Article 102 TFEU, read in conjunction with Article 106 TFEU, be placed within a framework of substantive criteria which are transparent, clear and precise [. . .] so that it may not be used in an arbitrary manner', such criteria being 'suitable for ensuring that such a power is exercised in a non-discriminatory manner and enabling effective review').
[163] Case No COMP/M.7217—Facebook/Whatsapp (Oct. 3, 2024).
[164] Case M.8124—Microsoft/LinkedIn (December 6, 2016).
[165] Case M.8788—Apple/Shazam (September 6, 2018).
[166] Case M.9660—Google/Fitbit (December 17, 2020).
[167] Case M.10301—CVC/Ethniki (February 24, 2022).

on end-users' privacy and data protection, to be dealt *ex post* under the EU's data protection laws. This approach has been rightly criticized, even by data protection agencies, such as the European Data Protection Board (EDPB) which noted concerning the *Google/Fitbit* merger '(t)here are concerns that the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data'.[168]

In the absence of a process of regulatory cooperation between the DG Competition at the European Commission and the data protection authorities in the EU and the European Data Protection Board (EDPB), and even more of a requirement of joint approval of digital mergers, the Commission (and National Competition Authorities—NCAs) should step in and assess the privacy and exploitation concerns raised by the transaction, adapting if it is necessary for its own criteria to integrate privacy concerns, by eventually repurposing for the occasion concepts of data protection law. This may be even more so as there is no catch-all provision in the EU for the *ex-post* assessment of privacy-reducing practices, from the perspective of competition law, and the scope of Article 102 TFEU may not be sufficiently large to cover such practices if the undertaking in question does not have a dominant position on an identified relevant market. There is not therefore any concern that such approach will stifle the growth opportunities of small and medium sized firms.

C. Regulatory Alternatives

The competition law tool kit has been recently completed by specific regulatory duties imposed to gatekeepers by Article 5(2) of the DMA. According to this provision, the gatekeeper is prohibited from doing the following: (a) processing personal data of end users using services of third parties that make use of its core platform services to provide online advertising services; (b) combining personal data from one core platform service with personal data from other core platform services, services provided by the gatekeeper, or third-party services; (c) using personal data from one core platform service in other services provided separately by the gatekeeper, and vice versa (d) signing in end users to other gatekeeper services to combine personal data, unless the end-user has been initially presented with the choice and given specific consent as defined in the GDPR. If an end-user refuses or withdraws consent, the gatekeeper cannot request consent for the same purpose more than once within a year.[169]

As is explained in Recital 36 of the DMA, the main goal of this provision is about ensuring the contestability of the core platform service in the sense that gatekeepers gain potential advantages in terms of accumulation of data. To ensure that Big Tech platforms do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to *freely* choose to opt-in to such data processing and sign-in practices by offering a less personalized but equivalent alternative, and without making the use of the core platform service or certain functionalities conditional upon the end user's consent. It is also mentioned that the less personalized alternative should not be of degraded quality compared to the service provided to end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or sign in end users to a service.[170] Article 5(2) DMA thus imposes both negative and positive obligations. It first prohibits gatekeepers from bundling data harvested across different core platform services and ecosystem

[168] European Data Protection Board, Statement on privacy implications of mergers (adopted February 19, 2020) available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf.

[169] Article 5(2) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022 (hereinafter DMA).

[170] Recital 36, DMA.

services without explicit data subject consent (opt-in system). Additionally, it imposes positive obligations on gatekeepers to provide an equivalent but less personalized alternative when users withhold consent for data use. This ensures that access to core platform services or specific functionalities is not conditional upon end-user consent to his personal data processing—a critical protection given the asymmetrical power relationship between gatekeeper platforms and end-users. Most recently, the European Commission's preliminary investigation under Article 5(2) DMA found that Meta could not restrict through its 'pay or consent' advertising model the possibility of end-users to opt for a service that uses less of their personal data but is otherwise equivalent to the more personalized service, which is more privacy-reducing, and to exercise their freedom not to consent to the combination of their personal data.[171]

This regulatory provision could also apply to digital health ecosystems to the extent that this data is harvested in a core platform service that falls within the scope of the DMA. For instance, one could imagine that it would not be possible to combine personal data harvested by a virtual assistant owned by a gatekeeper through a health-related application, in case it has been designated as a gatekeeper for this digital assistant, with data harvested by a digital health insurance app managed by the same gatekeeper.

V. THE RELATION BETWEEN ECOSYSTEM ORCHESTRATORS/DIGITAL PLATFORMS AND COMPLEMENTORS/BUSINESS USERS

A. The Nature of the Distributional Problem

As mentioned above, ecosystems group independent firms that are linked together operationally across multiple tiers in a network, in which they *compete* (for the attention of or to the benefit of a third party) but also *cooperate* to fulfil a common set of tasks increasing the value of the network.[172] They form a space of co-opetition, as independent firms forge relations of interdependence and trust consolidated over the long term through the development of an aligned vision to provide a focal value proposition to consumers.[173]

Ecosystems often are operated as walled gardens with the ecosystem orchestrator limiting the access of other ecosystem actors to the data harvested centrally by the digital platform it controls, either by the end- and business users of the digital platform or by the end-users accessing through the digital platform the products and services of its ecosystem complementors.[174] To the extent that the ecosystem orchestrators have a rule-setting authority and thus keep some form of control over the legitimate use of the data captured, they are playing a crucial role in all types of ecosystemic competition. Some scholars have however referred to the 'data commons' of the ecosystem to highlight the important contribution of the collective effort of all members of the ecosystem to this data generation, and this raises the possibility of specific data sharing obligations that would specifically apply to ecosystems.[175] Such proposals adequately consider the idiosyncrasies of the relation between ecosystem orchestrator and complementors, and

[171] European Commission, Commission sends preliminary findings to Meta over its 'Pay or Consent' model for breach of the Digital Markets Act (July 1st, 2024), available at.https://digital-markets-act.ec.europa.eu/commission-sends-preliminary-findings-meta-over-its-pay-or-consent-model-breach-digital-markets-act-2024-07-01_en

[172] European Commission, Commission Notice on the definition of the relevant market for the purposes of Union competition law, C/2024/1645, para. 104 ('Digital ecosystems are governance systems 'involving a primary core product and several secondary (digital) products whose consumption is connected to the core product, for instance, by technological links or interoperability').

[173] See also the definition of ecosystems in M.J. Jacobides, C. Cennamo & A. Gawer, Towards a Theory of Ecosystems, (2018) 39(8) Strategic Management Journal 2255.

[174] Digital platforms occupy central positions in the global internet topology, all end-users' data been harvested through the intermediation of the platform, these constituting, from a technical perspective, distributed points of control.

[175] H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 354.

hint to the need for specific rules to apply in this context concerning the regulation of data sharing, something that will be further examined in Section IV.C.. The inclusion in the European Commission's Draft Guidelines on Article 102 TFEU of a specific Section on data sharing obligations that may be imposed to ecosystem orchestrators holding a dominant position to its complementors may also provide a much-needed clarification for the use of the competition law tool in such situations.[176]

Ecosystems may compete with one another (*inter-ecosystem competition*). However, since they also rest on interactions between independent firms, multi-actor ecosystems also give rise to *horizontal intra-ecosystem competition* between firms offering rivalrous, potentially substitutable offerings within the same ecosystem, and to *vertical intra-ecosystem competition*, which refers to competition for capturing the surplus value produced by the cooperation between the ecosystem participants, including the ecosystem orchestrator.[177] Ecosystemic theories of harm that involve data and exclusion or marginalisation of competitors in vertically situated markets involve situations where potential intra-ecosystem competition is restricted through, for instance, the pre-emption of the emergence of new access points for personal or non-personal data in competitors' hands, or data-driven envelopment with privacy-policy tying (that is, pre-emptively tying data collected in unrelated markets with the aim to acquire a data advantage deterring entry in the primary market even from more efficient firms than the incumbent), or through some form of discriminatory behaviour.

For example, in the *Google Privacy Sandbox* case,[178] Google had limited rival ad tech platforms' ability to track their users and target ads, while preserving its own ability to track. Although rivals could also use primary data to provide digital advertising services, their reach and the quality of their data was lower quality than Google's. The extensive reach of Google's user-facing services and its ability to harvest data with greater precision, due to its large base of users logged into their account, provided the firm with a significant data advantage over its rivals and enabled it to reinforce its position in the advertising market. The self-preferencing of Google's own ad-tech and ad inventory also raised concerns because of its control of Chrome as Google operates at the same time as a publisher and as an ad tech provider. The third more traditional exploitation/fairness issue relates to the imposition of unfair terms on Chrome web users, as Google denies them any substantial choice as to whether and how their personal data was used to target individuals for advertising purposes.

In a different case, *Meta* was fined by the European Commission for having infringed Article 102 TFEU by tying its online classified ads service Facebook Marketplace with its dominant personal social network Facebook and imposing unfair trading conditions that authorize Meta to use ads-related data derived from competing online classified ads service providers who advertise on Meta's platforms (Meta's very popular social networks Facebook and Instagram), thus allowing Meta to use ads-related data generated by other advertisers for the sole benefit of Facebook Marketplace, providing it an important competitive advantage vis-à-vis its competitors in the online ads markets.[179]

[176] Communication from the Commission, Draft Guidelines on the application of Article 102 of the Treaty on the Functioning of the European Union to abusive exclusionary conduct by dominant undertakings, [. . .](2024). See also the proposal by H. Schweitzer & A. Metzger, op. cit., (noting that '(t)he practical effectiveness of Art. 102 TFEU in enforcing data access might increase if guidelines were to clarify that data sharing within ecosystems may constitute a special category of cases, and to develop a more structured test for this setting', further suggesting specific criteria for this test).

[177] See, M.G Jacobides & I. Lianos, Regulating platforms and ecosystems: an introduction, 2021) 30(5) Industrial and Corporate Change 1131.

[178] See, UK CMA, https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes.

[179] European Commission, Commission fines Meta €797.72 million over abusive practices benefitting Facebook Marketplace (November 14th, 2024), available at https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5801.

These cases make it clear that by matching different datasets (in the Google context web-browsing behaviour), digital platforms may expand their ecosystems in other areas and exclude or marginalize their rivals as these may not have effective access to data (particularly health data also in view of the GDPR). Of course, here the interests of the complementors to access data do not always converge with those of the end-users for privacy protection. In essence, ecosystems orchestrators and dominant platforms may benefit from a 'cross-market leverage'[180] to the extent that they will be able to use a sale in or data from one market to steer consumers toward their product or service in another market or take advantage of 'convenience bundling' (because searching for or switching to something else is costly).[181] This will allow them to capture a significant proportion of the surplus value generated by offering products or services in connected markets 'glued' together, as part of a tightly controlled by the digital platform business ecosystem (through technology and/or contractual obligations).[182]

B. The Use of the Competition Law Toolkit

Health-related data, given its critical role as an input in digital health services, may increasingly be viewed as an essential facility in the context of competition law. This characterisation stems from the unique and often irreplaceable nature of health data in developing, improving, and delivering digital health services. As health data becomes more integral to medical innovation, personalized treatments, and efficient healthcare delivery, considering it as an essential or indispensable facility for operating in the downstream to health-data markets opens the door to the application of competition law remedies, particularly mandated data access.[183] Unilateral termination of a business or end-user's access and ability to port data could also qualify as an abuse, in the absence of objective justifications,[184] following an established precedent of the CJEU regarding termination of supply to existing customers.[185] The abuse will be even more likely if in addition there is some form of discrimination/preferential treatment and/or leveraging strategy.[186] Where data access and data portability are denied to a new customer, it is unlikely this will trigger the application of the *Oscar Bronner* precedent. Such conduct usually does not fall under the 'refusal to supply' category, which only refers to situations where

[180] P. Heidhues, M. Koster & B. Kószegi, A Theory of Digital Ecosystems (July 8th, 2024), available at https://www.wiwi.uni-bonn.de/koszegi/ecosystems.pdf.

[181] See, Z. Chen & P. Rey, A theory of Conglomerate Mergers, TSE Working Paper, n. 23–1447, June 2023 available at https://www.tse-fr.eu/publications/theory-conglomerate-mergers.

[182] Ibid., See also I. Lianos, Ecosystems and Competition Law: A Law and Political Economy Approach, April 2024, CPI, available at Ecosystems and Competition Law: A Law and Political Economy Approach (pymnts.com); I. Lianos, K. H. Eller, T. Kleinschmitt, Towards a Legal Theory of Digital Ecosystems (May 27, 2024). Faculty of Laws University College London Law Research Paper No. 16/2024, Amsterdam Law School Research Paper No. 2024–22, Amsterdam Centre for Transformative private law Working Paper No. 2024–01, Available at SSRN: https://ssrn.com/abstract=4849340; M. Jacobides & I. Lianos, Ecosystems and competition law in theory and practice, (2021) 30(5) *Industrial and Corporate Change*, 1199.

[183] This might in some cases conflict with the protection of privacy and compliance to the GDPR, which opens the possibility for the dominant undertakings to argue as a form of 'objective justification' the 'privacy defense' to refuse to provide access to this personal data. See, for instance, for such a configuration, Canadian Competition Tribunal, in which case the Federal Court of Appeal confirmed the Tribunal's findings and found there was little evidentiary support for the contention that the restrictions in question were motivated by privacy concerns: Toronto Real Estate Board v. Commissioner of Competition, 2017-12-01, Federal Court of Appeal Docket: A-174 16, Citation: 2017 FCA 236, para. 131. See also for similar considerations regarding privacy as a legitimate business consideration/defence for Linkedin's conduct to restrict access of a competitor to its users' personal data available on its website, *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019); *hiQ Labs v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022); *hiQ Labs v. LinkedIn Corp.*, Case 3:17-cv-03301-EMC (US Dist. Ct, Northern Dist. Calif., 2022).

[184] See, H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 342.

[185] See, Joined Cases C- 6 & 7/73, Istituto Chemioterapico Italiano SpA and Commercial Solvents Corporation v Commission [1974] ECR 223; Case 22/76, United Brands Company and United Brands Continental BV v Commission [1978] ECR 207. See also, European Commission Draft 102 Guidelines, para. 166(a).

[186] See, Case C-377/20, Servizio Elettrico Nazionale, ENEL/Commission, ECLI:EU:C:2022:37; Case T-612/17, Google LLC, ECLI:EU:T:2021:763.

a dominant undertaking has developed an input (here data) 'exclusively or mainly for its own use'.[187] The *Bronner* doctrine does not cover situations where data is generated in the context of interactions in an ecosystem of independent undertakings, and thus is not exclusively developed for the own use of the dominant digital platform.

This was, most recently, confirmed by the CJEU in *Android Auto* in which the CJEU abandoned the *Bronner* indispensability requirement for situations in which the infrastructure in question is not owned by the dominant undertaking or has not been developed 'solely for the needs' of the dominant undertaking but also for use by third-party undertakings, the CJEU effectively excluding the application of *Bronner* for third-party ecosystems in case the platform has an open design.[188] This opens the possibility of competition law based actions to ensure data interoperability even though that digital platform in question is not indispensable for the commercial operation of the app concerned on a downstream market in case such refusal to interoperate 'has the actual or potential effect of excluding, obstructing or delaying the development on the market of a product or service which is at least potentially in competition with a product or service supplied or capable of being supplied by the undertaking in a dominant position' and 'constitutes conduct which restricts competition on the merits, and is thereby capable of causing harm to consumers'.[189]

Alternatively, some form of data exclusivity may result or form part of a take-it-or-leave-it contract, in which case it may also qualify as a conditional refusal to supply access or portability and may be subject to stricter standards than a unilateral refusal to provide access to a new customer.[190] As such refusal will take place in the context of a contractual relationship, it may also qualify as an unfair trading condition prohibited by Article 102(a).[191] The criteria of the case law are indeed open in the presence of what may qualify as a disproportional restriction in case the request for data access and portability comes from one of the business user/complementor who co-generated the data or has contributed to the development of the dataset.[192] If a refusal to provide data access and portability concerns personal data (for instance if the business user is a natural person), this refusal may also constitute an infringement of Article 15 GDPR. If committed by a dominant undertaking this could qualify as a possible 'regulatory offence' subject to the prohibition of Article 102 TFEU.[193]

It cannot be excluded that there might exist a 'hybrid' exclusionary/exploitative theory of harm,[194] as that followed in the German Facebook case by the BkA for personal data if the latter are natural persons (for example, self-employed constituting an undertaking), or more recently by the Commission in *Apple App Store*, for business users complementors.[195] Finally, although the Commission in *Apple App Store* has proven that the anti-steering provisions were detrimental to the interests of end-users, it has not excluded the possibility that Article 102 TFEU may also apply to deal with unfair conduct producing effects on business users or complementors (P2B relations), explicitly referring to Article 5(4) DMA that concerns business users as supporting

[187] European Commission Draft 102 Guidelines, para. 96. See also, Case C-165/19 P, Slovak Telekom v Commission, EU:C:2021:239, para. 45 & Case C-42/21 P, Lietuvos geležinkeliai v Commission, EU:C:2023:12, para. 79.

[188] Case C-233/23, *Alphabet and Others (Android auto)*, ECLI:EU:C:2025:110, paras 47–48.

[189] Ibid., paras 50–51.

[190] See, among others, Case C-165/19 P Slovak Telekom a.s. v Commission, EU:C:2021:239, para.50.

[191] See, I. Lianos, V. Korah, P. Siciliani, *Competition Law: Analysis, Cases and Materials* (OUP, 2019), Chapter 9.12.

[192] The important element of the test is the proportionality of the examined restriction: see, DSD (Case COMP D3/34,493) Commission Decision 2001/463/EC [2001] OJ L 166/1; Case T- 151/01, Der Grüne Punkt— Duales System Deutschland GmbH v Commission [2007] ECR II– 1607, paras. 121–122; Case C- 385/07 P, Der Grüne Punkt— Duales System Deutschland GmbH v Commission [2009] ECR I– 6155.

[193] Case C- 457/10, AstraZeneca v Commission, ECLI:EU:C:2012:770, paras 105–12.

[194] H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 342.

[195] See the discussion in Section X of this Chapter.

the view that such conditions imposed by a dominant undertaking (on business users) should be qualified as unfair.[196]

Competition law interventions may focus on both individual-level and aggregated-level/bundled health data. The important question arising here relates to the application of the unilateral conduct competition law standards if this access may qualify as an unconditional 'refusal to supply'. In this case, the relatively stricter standards following in the *IMS/NDC Health* case apply,[197] or altogether it sits outside the scope of this antitrust category with other 'theories of harm' and legal standards applying.[198] The requirement of dominance for the application of Article 102 TFEU would limit the situations in which individual-level data may constitute an 'input market' on which a firm may be found to be dominant. This is something that may be more easily imagined if the data is 'derived', for instance through Artificial Intelligence (AI).

Similarly, dominance may result from control of an aggregated dataset, protected by IP rights or trade secrets that may qualify as an 'essential facility'. It would be however difficult to imagine the situation of a total lack of substitutability for individual-level data about a business user (or even end-user). The possibility may present itself in situations of a bespoke personalized service or product as well as in situations of data for a product that is unique, without any possibility to use synthetic data. In these cases, each user may form on her own a relevant market.[199] An additional difficulty for the implementation of competition law in this context relates to the remedies that may be imposed if these go further than just a cease-and-desist order and involve some form of a more permanent monitoring of real-time and effective data access/sharing and portability. Finally, some scholars have highlighted that the current 'lack' of competition law cases may be due to the early stage of development so far of the data economy, the lack of information about the aggregated datasets held by the data holders, and the lack of data on the processing and analysis capabilities or specialized skills and staff of many undertakings (particularly SMEs).[200]

While the EU courts and the Commission have been creative in the context of *ex-post* control, and aimed to address both exclusionary and exploitative concerns, this has not been the case for ex-ante merger control, as is shown by the *Apple/Shazam*,[201] *Google/Fitbit*[202] and *CVC/National Insurance* merger decisions.[203]

For instance, in the *Google/Fitbit* case (2020), the European Commission recognized that by acquiring Fitbit, Google would own the database that Fitbit maintains of its users' health data and technology that enables data collection via wearable wrist devices. The Commission noted that this offers a significant data advantage given the increasing possibilities of 'personalisation' of the services offered by Google, which also derives data through the use of the online search engine it controls. The European Commission referred to the limitations of Article 5(1)b of the GDPR but also those of Article 9 GDPR which define, for the Commission, a general but not

[196] European Commission, CASE AT.40437—Apple—App Store Practices, para. 552.

[197] Case C-418/01, *IMS Health GmbH & Co. OHG/NDC Health GmbH & Co. KG* (*IMS Health*), ECLI:EU:C:2004:257. According to this case law, for a refusal to supply to violate Article 102 TFEY, access to the input (for which there is demand from potential purchasers) should be indispensable for the undertaking requesting access to compete with the dominant undertaking in a downstream market and the refusal should be capable of having exclusionary effects. See also Draft Guidelines on the application of Article 102 of the Treaty on the Functioning of the European Union to abusive exclusionary conduct by dominant undertakings, paras 98–99.

[198] See the discussion above.

[199] That could possibly be thought as a way out of an extreme scenario of full exploitation of the consumer surplus in the context of personalized pricing and perfect price discrimination by a supplier of a product indispensable for the user, the user ignoring the prices charged to others, thus curtailing the ability of users to collectively switch to another supplier.

[200] H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 352.

[201] M.8788—Apple/Shazam (6.9.2018).

[202] M.9660—Google/Fitbit (17.12.2020).

[203] M.10301—CVC/Ethniki (24.2.2022).

absolute prohibition for the transfer of health data, as well as the ePrivacy Directive, specifically citing Article 5(3) of this Directive about the need to provide clear and extensive information about the purpose of the processing, and the right provided to the user to refuse such processing.

The Commission referred to Google's obligation to comply with this legal framework, including the principles of purpose limitation, fair use of data, legality (particularly regarding the choice of the appropriate legal basis for the data processing) and transparency. At the same time, however, the Commission did not rule out the possibility that the merger could produce negative effects on competition, even if the use of personal data by the new entity were to be entirely legal.[204] It therefore further examined whether the combination of Fitbit's data with Google's data (and the latter's capabilities to collect and process big data) could cause anticompetitive horizontal unilateral effects by strengthening Google's position, among others, in online search and advertising markets or general search services, but also crucially digital healthcare services. Regarding the latter, it noted the wealth of business initiatives already underway in the digital healthcare sector, new entry from established players such as Amazon, finding no reason for competition concern.[205] When exploring vertical foreclosure effects, though, it noted that in the nascent digital healthcare industry, third-party apps and websites providing digital healthcare services derive the user data they need from APIs built and made available by mobile device manufacturers or other entities that collect personal data.[206] These effects had therefore to be more thoroughly examined in merger control phase II, as Fitbit, due to its significant customer base, had the largest health database (after Apple) worldwide.[207]

The Commission concluded that while, in general, user health data is available from various data sources, Fitbit user data is only available through the Web API and from certain players in digital healthcare services and therefore it could not be ruled out that Google would, post-merger, have the ability to foreclose competitors in the downstream digital health markets by limiting their access to the Fitbit Web API,[208] nor that the new entity would have the incentive to foreclose access to Fitbit Web API. For this reason, it accepted Google's Web API access commitment that ensured that players active in the downstream market for the provision of digital healthcare continue to have the same access as before the merger.

Another theory of harm in these data mergers relates to vertical integration through which a merged entity may gain access to commercially sensitive information about the activities of its competitors operating in the upstream or downstream markets. This would allow it to apply a less aggressive pricing policy in the downstream market to the detriment of consumers, or put its competitors at a competitive disadvantage, thereby discouraging entry or their expansion in the downstream or upstream market.[209] It may also facilitate coordination by increasing the level of market transparency between firms through access to sensitive information on rivals or by making it easier to monitor pricing.[210]

Applying the well-known 'ability and incentive' to foreclose framework, the Commission, examined in *CVC/Ethniki* if HHG hospitals (owned by CVC) access to patients' health data and rival hospital doctors' billing data (which constituted commercially sensitive information) would have provided Ethniki (the health insurance vertically integrated undertaking) a competitive advantage over rival health insurers.[211] Regarding patient's health data, the Commission

[204] M.9660—Google/Fitbit, para, 412.
[205] Ibid., para. 496.
[206] Ibid., para. 504.
[207] Ibid., para. 511.
[208] Ibid., para. 520.
[209] European Commission, Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings, (2008/C 265/07), para. 78.
[210] Ibid., para. 86.
[211] Case M.10301—CVC/Ethniki (February 24, 2022).

noted certain enhanced legal limitations on the use of patients' data by Ethniki post-merger transaction, resulting from the GDPR. The processing of such special category of data is indeed prohibited unless there is explicit consent allowing HHG to disclose patient data to Ethniki (or any other insurance company) for purposes other than the administration of claims. However, the Commission also noted that consent was likely to be refused in most cases and that in any case such use would have damaged HHG's reputation. It dismissed however this theory of harm finding that reaching out directly to customers to sell health insurance products was not common in Greece.[212] Adopting an ecosystemic theory of harm, similar to that put forward in the *Booking/eTraveli* case, could have engaged more thoroughly with the anticompetitive potential of this merger.[213]

C. Regulatory Alternatives

Regulatory initiatives at the EU level are increasingly aimed at mitigating potential market distortions that may arise from the denial of access, portability, or interoperability of data for business users, thereby complementing traditional competition law tools. A crucial legal distinction is made between gatekeepers and other digital platforms, with the Digital Markets Act (DMA) imposing far-reaching obligations on the former. This tiered approach recognizes the disproportionate influence of gatekeeper platforms on digital markets and subjects them to more stringent requirements, including mandated data sharing, interoperability with third-party services, and prohibitions on certain data usage practices. For non-gatekeeper platforms, less severe but still significant regulations apply, often through sector-specific legislation or broader data governance frameworks such as the Data Act, and sector-specific regulatory initiatives such as the European Health Data Space (EHDS).

1. Digital Markets Act

Turning to the DMA, although digital health services are not considered essential platform services (according to Article 2 of the Act), and therefore the obligations imposed by Articles 5 and 6 of the Act *inter alia* only apply in respect of each of the essential platform services of the gatekeepers listed in the designation decisions pursuant to Article 3(9) DMA, it cannot be excluded, as highlighted above in Section III, that conduct in a core platform service may also have an impact on other markets and services in which the incumbents are active and in which the gatekeeper may use the disproportionate advantage conferred by its position in the core platform service.

The increasing involvement of large digital platforms subject to the Digital Markets Act (DMA) in digital health and insurance services, through partnerships, data transfers, and mergers and acquisitions, raises significant concerns regarding data access and sharing. These gatekeepers' power relative to potential competitors in vertical markets is particularly problematic due to their ability to process personal data, especially lifestyle information, from a vastly larger number of third parties compared to other businesses. This data advantage can manifest in several ways that confer significant competitive edges: firstly, by combining end-user personal data collected from a core platform service with data gathered from other gatekeeper services; secondly, through the cross-utilization of personal data from a core platform service to other separately provided gatekeeper services, particularly those not directly associated with or supporting the primary core platform service; and thirdly, by linking end users across various gatekeeper services to aggregate personal data. These practices enable gatekeepers to accumulate and leverage vast, diverse datasets, potentially creating insurmountable barriers for competitors

[212] Ibid., paras 151–154.

[213] European Commission, Case M.10615—BOOKING HOLDINGS/ETRAVELI GROUP (September 25, 2023), paras 204, 904–970, 1339

and raising serious implications for market competition, innovation, and user privacy in the digital health and insurance sectors.[214]

A first set of obligations on gatekeepers included in the DMA regulate the harvesting of data. As is acknowledged in the DMA, the gatekeepers do not only harvest directly personal data from end-users. Also, third parties (complementors and other business users) provide gatekeepers with personal data of their own end users to make them use certain services provided by the gatekeepers in the context of their core platform services.[215] This accumulation of personal data may provide a competitive advantage to the gatekeeper, particularly vis-à-vis a business user/complementor with which they compete in a different market than the core platform service, on which the gatekeeper is also active. This may raise entry barriers in this vertical market, as well as in the market of the core platform service, the second possibility being explicitly acknowledged in the DMA.

As discussed above, the Article 5(2) DMA's prohibition enters into play (a) when personal data (for example, lifestyle data) of end-users using services of third parties that make use of core platform services of the gatekeeper (complementors, business users) is processed for the purpose of providing online advertising services, (b) when the gatekeeper combines personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services (complementors, business partners), (c) when even without combining the datasets, there is a cross-use of personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa, which will inevitably provide the gatekeeper a competitive advantage vis-à-vis other business partners/complementors with which it also competes at the platform/ecosystem level.[216]

In this context, consent by the end-user is still necessary (also for the data harvested by complementors/business users) as end users may freely choose to opt-in to such data processing and sign-in practices, but also to ensure that consent will be genuine and not extracted due to the asymmetry of power between the end-user and the gatekeeper, the DMA further obliges the gatekeeper to offer a less personalized but equivalent alternative, which should not be different or of degraded quality compared to the service provided to the end users who provide consent, and this without making the use of the core platform service or certain functionalities conditional upon the end user's consent.[217] Although the provision acknowledges that consent to allow the gatekeeper to process personal data for providing online advertising services may be granted either directly to the gatekeeper's core platform service, or through each third-party service that makes use of that core platform service, there is no specific requirement as to the possibility of the gatekeeper to limit the extent of the consent provided by the end-user for the use of her personal data by a third party, unless one may consider that such behaviour constitutes an infringement of the anti-circumvention clause of Article 13 DMA[218] or could fall under the scope of competition law (see the analysis above in Section IV.B).

However, the provision is further subject to a quite broad exception as the gatekeeper remains free to process personal data or to sign in end users to a service, relying on the legal basis under Article 6(1), points (c), (d) and (e) of Regulation (EU) 2016/679 when the processing is necessary for compliance with a legal obligation to which the data controller is subject. This is done to protect the vital interests of the data subject or of another natural person or to ensure

[214] DMA, Recital 36.
[215] Ibid.
[216] Ibid.
[217] DMA, Recital 36 and 37.
[218] Particularly Art. 13(4) & 13(6) DMA.

the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The use of other legal bases, such as performance of contract and legitimate interest (Article 6(1)(b) and (f) GDPR) cannot apply in this context.

The text of the DMA does not however contain any reference to the limited legal bases for the processing of specific categories of data, such as genetic data, biometric data and data concerning health, which are listed in Article 9(2) GDPR (in particular (a), (h) and (i), which provide an exception to the prohibition of processing such data under Article 9(1) GDPR. It is possible to interpret this omission as not enabling the gatekeeper to process this type of personal data, either harvested by the gatekeeper in its platform or by business users/complementors of the gatekeeper's business ecosystem, if the data subject refuses consent, thus limiting effectively the other legal bases of Article 9(2) with the exception of course of Article 9(2)(a).

Furthermore, Article 6(2) DMA establishes a ban on gatekeepers of using, when in competition with business users, 'any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of those business users'. This provision targets situations in which the gatekeeper has a dual role, providing core platform services and also other services together with or in support of the core platform service to its business users, while also competing or intending to compete with the same business users to provide similar services or products to the same end users. The provision has a broader scope than Article 5(2). First, it does not only concern personal data but also non-personal data, for which the provisions of the GDPR do not apply. Second, it covers both individual as well as aggregated data. Third, as indicated by Article 6(2)(2) DMA, it also includes 'any aggregated and non- aggregated data generated by business users that can be *inferred from*, or collected through, the commercial activities of business users or their customers, including click, search, view and voice data, on the relevant core platform services or on services *provided together with, or in support of*, the relevant core platform services of the gatekeeper'.[219] Also, in contrast to Article 5(2), this article contains a clear prohibition that may not be waived based on consent or any other grounds.

A second set of obligations in the DMA (Article 6(9) imposed on gatekeepers relate to the provision of access rights and portability free of charge to data provided or generated in the context of the use of the relevant core platform service or other services in support of the relevant core platform services. These rights benefit end-users and third-party business users authorized by an end-user,[220] but also third-party business users/complementors that provide related services to the core platform and thus co-generate this data, as long as the end-users engage with the products or services provided by them.[221] These stricter obligations to gatekeepers acknowledge that '(d)ue to their gateway position and superior bargaining power, it is possible that gatekeepers engage in behaviour that does not allow others to capture fully the benefits of their own contributions, and unilaterally set unbalanced conditions for the use of their core platform services or services provided together with, or in support of, their core platform services'. Such 'imbalance' also consists in 'excluding or discriminating against business users, in particular if the latter compete with the services provided by the gatekeeper'.[222]

Access should again be effective, high-quality, continuous and done in real-time, for example by putting in place 'high quality application programming interfaces or integrated tools for small volume business users'.[223] The provision is also of quite broad application as it concerns

[219] Art. 6(2) paragraph 2. Emphasis added.
[220] Art 6(9) DMA.
[221] Art. 6(10) DMA.
[222] DMA, Recital 33.
[223] DMA, Recital 60.

aggregated and non-aggregated/individual data, including personal data. However, there is a specific restriction concerning personal data, as access to, and use of such personal data may be provided only 'where the data are directly connected with the use effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users opt in to such sharing by giving their consent'.[224] This limits the opportunity of business users/complementors to expand their client base.[225] Furthermore, business users should receive, either directly or through the gatekeeper, the consent of the end-users for the use of their personal data.

In this context, the DMA provides a more specific anti-circumvention measure prohibiting gatekeepers from designing and steering user consent to their benefit and limiting access to their competitors business users, and in particular from using 'any contractual or other restrictions to prevent business users from accessing relevant data' and imposes a positive obligation to gatekeepers to 'enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required' under the GDPR and the ePrivacy Directive.[226]

A more specifically circumscribed access right is also provided for in Article 6(11) DMA with regard to the relation between gatekeepers and third-party business users that have not taken part in the generation of the data, thus sitting outside the business ecosystem. This will be further discussed in Section V.

2. Data Act

The EU Data Act complements the DMA, by focusing on barriers to data sharing, and adapting rules of contract law to prevent the exploitation of contractual imbalances that hinder fair access to and use of data. It also imposes some public law-type regulatory obligations to promote contestability by enabling the switching between data processing services but also by enhancing the interoperability of data and data-sharing arrangements.[227] By containing general access rules, according to which a data holder is obliged by law to make raw data either recorded intentionally by the user or constituting a by-product of the user's action (for example, performance data such as average battery level) or data generated even if the product is in standby mode (for example, heart-rate in a fitness tracker), available to a data recipient, the Data Act, also stipulates that such access rules should be based on fair, reasonable, non-discriminatory and transparent (FRAND) conditions.[228] The Regulation also recognizes the principle that all persons can have access to the data they generate.[229]

The Data Act establishes a new horizontal (to the extent they apply to all economic sectors and may concern all firm sizes) access right for data harvested by data holders to the benefit of product users and derivatively for third-parties business users/complementors, authorized by product users to get access to the data generated by their use of the product. This also covers all types of data, personal or non-personal.[230] The link here between the data holder and the third-party business user/complementor is indirect, as data access can only be provided 'upon request

[224] DMA, Art. 6(10).

[225] See, P. Hacker, J. Cordes, J. Rochon, Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond, (2024) 15 European Journal of Risk Regulation 49, 76.

[226] DMA, Recital 60.

[227] Data Act, Recital 5.

[228] Ibid., Recital 38.

[229] Ibid., Recital 20.

[230] There is a wide coverage of the categories of data that may be subject to the access provisions of Art. 4 of the Data Act, this including raw and 'pre-processed data as well as the relevant metadata. However 'information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data, in particular by means of proprietary, complex algorithms, including those that are a part of proprietary software', does not fall within the scope of the Data Act and consequently is not subject to the obligation of a data holder to make it available to a user or a data recipient, unless of course it is otherwise agreed between the user and the data holder. Data Act, Recital 15.

by a user [end-user of a connected product or related service],[231] or by a party acting on behalf of a user'.[232] Article 3 of the Data Act imposes an obligation to manufacturers to technically design and provide the connected product/device data and related service data, including the relevant metadata necessary to interpret and use those data, 'by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format' so that they are directly accessible to the end-user and thus easily shared with third parties.[233] The Act also recognizes a non-waivable right to the user of the connected product/device to access and use the product and related service data (Article 4(1)) and to share them with third parties (who thus become data recipients) for the provision of services agreed with the user (Article 5(1)), free of charge to the end-user. This should take place in a 'comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time'.[234]

The third party's right to access data in this context is fundamentally a derivative right, stemming from and constrained by the end-user's primary right to their data. This derivative nature imposes significant limitations on how third parties can utilize the data and associated metadata. Specifically, their access and use are strictly bounded by the purposes and conditions explicitly agreed upon with the end-user, ensuring alignment with the user's intentions and expectations. Furthermore, this derived right is subject to full compliance with the General Data Protection Regulation (GDPR), adding an additional layer of legal constraint. This framework effectively creates a chain of responsibility and consent, where the end-user's rights and privacy preferences cascade down to shape and restrict the data practices of third parties, thereby maintaining user control and data protection principles throughout the data sharing ecosystem.[235]

Although the Data Act's data sharing obligation covers the situation of a third party offering an aftermarket service that may be in competition with a service provided by a data holder, it also prohibits the use of data accessed under the Act for developing a competing connected product. One of the aims here is to protect the data holders' innovation efforts and incentives to invest.[236] Note that gatekeepers are not considered as an eligible third party under Article 5 and thus cannot be data recipients. Also, they cannot 'solicit or commercially incentivize a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Articles 4 and 5 of the Data Act'.[237] In sharing the data with the third-parties data recipients, the data holders may require a (licensing) contract under FRAND terms.[238] Any compensation agreed between the data holder the data recipient for making data available in B2B relations should be 'non- discriminatory and reasonable and may include a margin', with further specifications detailed in the Act.[239]

[231] Data Act, Art. 1(3)(b) & Art. 2(12) (user is defined as a 'natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services'). A connected product consists in an 'item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user': Art. 2(5).

[232] Data Act, Art. 5(1).

[233] Product data is defined in the Act as' data generated by the use of a connected product that the manufacturer designed to be retrievable from the connected product by a user, data holder or a third party, including, where relevant, the manufacturer' whereas related service data is defined as 'data, which also represent the digitisation of user actions or events related to the connected product which are generated during the provision of a related service by the provider'. Such data may be 'recorded intentionally' or be data 'which result indirectly from the user's action'. Data Act, Recital 15.

[234] Data Act, Art. 5(1).

[235] Data Act, Art. 6(1).

[236] Data Act, Recital 32 and Art. 6(2)(e). The obligations imposed by Articles 4 and 5 apply neither to manufacturers that are microenterprises/small enterprises, nor under certain circumstances to SMEs. Data Act, Art. 7.

[237] Data Act, Art. 5(3).

[238] Data Act, Art. 8.

Commentators have challenged the effectiveness of the data-sharing mechanism in the Data Act and criticized it focus on the interests of the connected product/device manufacturers instead of cumulative innovation and competition.[240] They also noted the numerous restrictions, hurdles and unclear rules that may limit the incentives and ability of data recipients, such as the fact that the data sharing initiative that needs to be taken by the end-users of the connected product or service, and the need for a bilateral negotiation between the data holder and the data recipient. More importantly, the Data Act applies for online product-related usage of data (for example, through the use of a medical device or sensor) and does not cover situations of online-service related use of data (in the context of healthcare services provision).[241]

This brings me to the more complex fairness issues raised by the third dimension, the relation between external to the digital health ecosystem third-party business users and ecosystem actors (including data holders, business and end-users).

VI. THE RELATION BETWEEN EXTERNAL TO THE ECOSYSTEM THIRD PARTY BUSINESS USERS AND ECOSYSTEM ACTORS (DATA HOLDERS, BUSINESS AND END-USERS)

A. The Nature of the Distributional Problem

This Section explores the distributional issues raised in the context of requests to access data made by actors that have not contributed to its generation and are therefore external to the 'data ecosystem' composed by the data holder (for example, the digital platform or the manufacturer of the device) who often is the ecosystem orchestrator, and the business and end-users whose data or data in possession is often harvested by the platform.

Third-party users of digital platforms may adopt diverse strategies in relation to the platform ecosystem. Some may position themselves as actual or potential competitors to the core platform or to secondary activities conducted by existing business users. Others may operate in distinct economic segments not yet explored by the platform's ecosystem. In this complex landscape, facilitating access to data held by the platform or its business users serves multiple crucial objectives. Primarily, it aims to enhance market contestability and competition, challenging the entrenched positions of dominant digital platforms or business users in specific market segments. This data access also plays a vital role in fostering innovation within the broader data economy by enabling the development of new products and services that rely on the harvested data as a critical input. By democratising access to this valuable resource, regulators and policymakers seek to create a more dynamic and competitive digital marketplace, where smaller players and new entrants can leverage shared data to innovate and compete effectively against established entities.

As highlighted in the first Section, the concept of fairness in data access extends beyond addressing imbalances between parties directly involved in data co-generation to encompass broader economic and social objectives. This expanded view recognizes that providing access to data held by dominant platforms or within business ecosystems can serve as a mechanism to enhance equality of economic opportunities and mitigate structural inequalities in the digital economy. By enabling access to crucial data resources, this approach aims to empower a wider range of market actors, particularly those experiencing vulnerability due to the dominance of Big Tech platforms. These platforms leverage their 'ecosystem glue' and the social structure of the

[239] Data Act, Art. 9.

[240] W. Kerber, Eu Data Act: Will new user access and sharing rights on IoT data help competition and innovation?, (2024) 12 Journal of Antitrust Enforcement 234.

[241] See also, H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 348.

digital economy to extend their influence across various economic activities. Consequently, data access regulations serve not just to rectify specific unfair advantages but to rebalance the entire digital marketplace, this fostering a more diverse and competitive environment. This broader conception of fairness in data governance reflects an understanding of competition law and data regulation as forms of social regulation,[242] aimed at addressing 'structural inequalities'[243] and promoting innovation and economic opportunity and dynamism beyond the immediate concerns of data generation and ownership.

B. Competition Law as a Default Solution

As the request to access the data will come from a third-party business user (that is external to the ecosystem), any refusal to provide access or portability of data may qualify either as a refusal to deal with a new (non-existing) customer)[244] if the input (here data) was developed by the dominant undertaking 'exclusively or mainly for its own use',[245] or, to the extent that the data is covered by IP property rights held by the dominant undertaking (data holder), qualify as a unilateral refusal to license. A common characteristic of these set of cases is the requirement that access to the input is that the input (here data) is indispensable for the undertaking requesting access to compete with that the undertaking is dominant in a downstream market and that the refusal is capable of having exclusionary effects, which in this specific context means the capability to eliminate all competition on the part of the requesting undertaking.[246] Of particular importance here is to distinguish cases in which the property rights concern the structure of the data from those in which the data itself is proprietary.

In *IMS/NDC Health*, the European Commission,[247] in a decision confirmed by the CJEU,[248] considered the regulatory framework and particularly German legislation, according to which pharmacy consumption data had to be appropriately anonymized in a manner compatible with personal data and business confidentiality, so that they could be aggregated only at zip code level. This dataset was therefore organized into a 'mosaic structure' which grouped pharmacies into commercially useful geographical clusters which would not allow identification of any pharmacy. IMS claimed copyright for a grid it had developed which divided the territory of Germany into 1860 sections or 'bricks' ('mosaic structure') and refused access to this dataset to its rival, NDC.

Note that in this case it was not the data itself that was considered a key facility, but the segmentation of the data and its analysis in this specific mosaic structure (the data structure).[249] There was also no denial to access individual-level data, only access to the dataset (the 'mosaic structure'). This was constituted by inferred and aggregated data, which benefited from some form of IP protection. The pharmaceutical companies received detailed information on the demand and based on this they structured their supplies to pharmacies accordingly. The 'mosaic

[242] For a discussion, see I. Lianos, Competition Law as a Form of Social Regulation, (2020) 65(1) The Antitrust Bulletin 3, 34–38.

[243] P. Pettit, Freedom in the Market, (2006) 5 Pol. Phil.. & Econ., 131; R. Claassen & L. Herzog, Why Economic Agency Matters: An Account of Structural Domination in the Economic Realm, (2019) EUR. J. POL. THEORY (2019), 147,488,511,983,218 (noting the importance of preserving the 'economic agency' of the economic actors (their autonomy of action) from domination).

[244] Case C-7/97, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG et al., ECLI:EU:C:1998:569.

[245] European Commission Draft 102 Guidelines, para. 96. See also, Case C-165/19 P, Slovak Telekom v Commission, EU:C:2021:239, para. 45 & Case C-42/21 P, Lietuvos geležinkeliai v Commission, EU:C:2023:12, para. 79.

[246] European Commission Draft 102 Guidelines, para. 99. The input is indispensable if 'there is no real or potential substitute to it', which means that the data in question 'cannot be duplicated realistically and in a viable way due to physical, technical, legal or economic reasons', equivalent data cannot be obtained from other sources, and access to this data is 'necessary for the requesting firm to remain viably on the market and exert an effective competitive constraint'. Ibid., para. 101.

[247] COMP D3/38.044—NDC Health/IMS Health (3.7.2001).

[248] Case C-418/01, *IMS Health GmbH & Co. OHG/NDC Health GmbH & Co. KG* (*IMS Health*), ECLI:EU:C:2004:257.

[249] C. Tucker, Digital Data as an Essential Facility: Control, CPI Antitrust Chronicle (Feb. 2020).

structure' had indeed become a *de facto* industry standard. Any other way of dataset aggregation was potentially incompatible with German law because a differential aggregation could theoretically be used to identify an individual pharmacy if a company was present in more than two datasets. The European Commission ordered IMS to grant access to the specific mosaic structure on commercially reasonable terms. The CJEU ruled that a refusal to grant a license to exploit intellectual property rights does not in itself constitute an abuse of a dominant position but under exceptional circumstances if three conditions are cumulatively met, and particularly the refusal prevents the appearance of a new product for which there is a potential demand from consumers, it is unjustified and can exclude any form competition in a secondary market, that refusal to provide access to the data (structure) may constitute an abuse.

With regard to other forms of abuses in this context, we refer to the discussion in Section IV.B., as the same principles apply for a dominant undertaking's conduct restricting access to data that affects complementors already active in its business ecosystem.

C. Building a Regulatory Infrastructure for Health Data Access and Sharing: The Added Value of the EHDS

Regulating access and portability of data for third parties that are not part of the digital ecosystem and presumably have not contributed to the generation and harvesting of this data has the potential to expand the right to access to situations that the property rights rhetoric, even in its co-ownership version, would not have envisaged. An argument may be made in favour of such a duty to provide access to gatekeepers, given their sheer power and size, as all industry depends on them for having access to millions or even billions of consumers. Although the DMA does not include an expansive obligation to data sharing as the one stipulated in Articles 6(9) and 6(10) to the benefit of ecosystem business users that contributed to the co-generation of data, a more specifically circumscribed access right is recognized in Article 6(11) DMA, this time to the benefit of third-party business users that have not taken any part in the generation of the relevant data. This obliges gatekeepers to provide to any third-party undertaking providing online search engines (for example, a vertical health-related medical search engine), at its 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 its online search engines', so that these rivals may 'optimise their services and contest the relevant core platform services'.

The purpose followed by this right is to enhance contestability of the online search market.[250] The protection of any personal data of the end users remains a responsibility for the gatekeeper who should make the necessary to avoid any possible re-identification risks, by anonymizing such personal data so that the data subject is not or is no longer identifiable, without however substantially degrading its quality or usefulness.[251] Note that in addition to its narrow scope of application for this obligation, this provision applies only for the core platform services designated by the Commission, and access is mandated to the only benefit of third-party online search engines.

Although applying to undertakings that are not gatekeepers, the provisions of the Data Act do not offer an adequate scope to the right to access data as the third party's right to access data is 'derived' from the end-user's right and can only be exercised following a request by the end-user. It also does not concern all digital health services, but only data access obligations for 'connected products' (for example, medical and fitness devices, wearables that obtain, generate or collect data of the person using the wearable or their environment, but also virtual assistants insofar as they interact with the connected product or service) and 'related services' offered as part

[250] DMA, Recital 61 & Art. 6(11).
[251] DMA, Recital 61.

of the purchase, rent or lease contract for the connected product. These involve the exchange of data between the connected product and the service provider and are 'explicitly linked to the operation of the connected product's functions, such as services that, where applicable, transmit commands to the connected product that are able to have an impact on its action or behaviour'.[252] For instance, a health app that works on a smartphone, and does not require a medical device or a wearable device may not fall within the scope of the Data Act, unless they function as an IoT product.

However, as discussed above, the remit of the EU's fairness-promoting interventions is broader, as it aims to challenge structural inequalities of opportunity and to promote new entry as part of a broader innovation and competition enhancing industrial policy paradigm, something that becomes more pronounced in the design of sector-specific (for example, open health) data sharing initiatives. In the European Strategy for Data and the establishment of the European Health Data Space (EHDS),[253] the Commission noted in the proposal of the EHDS regulation its ambition to create a 'health specific ecosystem' comprising of rules and practices geared towards both primary and secondary usages of health data, the governance of which aims at 'empowering individuals through increased digital access to and control of their electronic personal health data, at national level and EU-wide [. . .] as well as fostering a genuine single market for electronic health record systems, relevant medical devices and high-risk systems'.[254]

The purpose of the EHDS is to facilitate the exchange of both primary and secondary health data from decentralized databases, by creating 'additional' rights 'to access, control, and share specific categories'[255] of personal electronic health data, and to provide 'common rules, standards and infrastructures and a governance framework'.[256] 'Primary use' access refers to situations in which the personal electronic health data is used to provide direct health services to the specific individual from whom data is harvested, 'including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social, administrative or reimbursement services' whereas 'secondary use' refers to situations in which electronic health data (individual level personal or non-personal as well as aggregated datasets) are used to benefit the society as a whole, and are not related directly to the provision of healthcare to a patient, such as activities of research, innovation, policy-making, patient safety, personalized medicine, official statistics, or regulation.[257]

The benefits of the primary and secondary use access to data provided by the EHDS are multiple for all stakeholders involved. These include (1) individuals/patients who will be able to have full control and rights over their personal health data,[258] (2) healthcare professionals involved in the treatment of a natural person who will benefit from an increased access/interoperability of the data generated, particularly six priority categories of electronic health

[252] Data Act, Recital 17.

[253] The first proposal of a European Health Data Space regulation was published in 2022 (EuHDS Regulation Proposal, COM/2022/197 final). The EHDS Regulation was published in March 2025: Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, OJ L, 2025/327, 5.3.2025.

[254] See, https://www.european-health-data-space.com. Key provisions of the Regulation, particularly on primary use and on EHR systems will apply from 26 March 2029 for certain types of health data and from 26 March 2031 for others. The provisions on secondary use will apply for most of the data categories by 26 March 2029 and for some from 26 March 2031, while the possibility of third countries to become authorized participants to the EHDS will apply by 26 March 2034. See, European Commission, Frequently Asked Questions on the European Health Data Space (updated March 5th, 2025), available at https://health.ec.europa.eu/latest-updates/frequently-asked-questions-european-health-data-space-2025-03-05_en at 7–8. The EHDS also requires the Commission to take any necessary implementing acts by March 26, 2027.

[255] European Commission, Frequently Asked Questions on the European Health Data Space, op. cit., at 10.

[256] EHDS Regulation, Art. 1(1).

[257] EHDS Regulation, Art. 2(2)(d) & (e).

[258] EHDS Regulation, Art. 3.

data,[259] thus greatly facilitating their work in the context of primary use of data,[260] (3) health care providers who will need to perform fewer duplicate tests, thus reducing the cost of care and achieving better time allocation, (4) researchers who will benefit from a more immediate capture and consumption of high-quality health-related data without undermining the integrity of patients' medical privacy rights, (5) regulators and policymakers who will have easier access to data that will ultimately lead to more efficient and resilient health care systems and more effective and targeted policymaking, and (6) the industry which will have access to the necessary data to develop new more innovative products, devices and services.[261]

With regard to primary use, the regulation grants patients immediate, free access (without the healthcare provider or a third party being able to directly or indirectly charge data subjects a fee or costs, or require compensation, for making electronic health data available) to priority categories of their personal electronic health data[262] with several key rights: adding information, correcting errors, restricting access, and tracking which healthcare professionals have viewed their records.[263] Patients can also grant access to other healthcare providers or request their current provider to transfer all or part of their electronic health data to another provider of their choice—immediately, at no cost, and without obstruction from either the healthcare provider or the systems manufacturers.[264] The purpose of this sector-specific regulation mandating access to health data is to complement but also go further than previous sector-specific initiatives regarding health data access, such as the CBHC Directive, which concerned the right of patients to have access to the electronic record of the treatment they received when they travelled to another EU country to receive medical care,[265] as well as horizontal initiatives such as the GDPR, the Data Act or the DMA,[266] considering the sensitivity of health data and consequently possible chokepoints that may emerge. It also provides a governance framework to facilitate data exchange and sharing.[267] The data sharing obligation goes further than the Data Act: it does not allow data holders to charge for providing access to health data to third parties (for example, a clinic or a hospital) for primary use, whereas the Data Act accepts that data holders may charge third parties for primary use.[268]

The EHDS Regulation also facilitates the cross-border sharing of information for primary use with the development of a European Electronic Health Record Exchange Format and of a central interoperability platform for digital health ('MyHealth@EU').[269] It also moves further than the GDPR and the Data Act regarding interoperability as in addition to creating a platform infrastructure it also introduces mandatory certification and interoperability requirements for

[259] Patient summaries, ePrescriptons, electronic dispensations, medical images, medical reports, laboratory results, and discharge reports.

[260] EHDS Regulation, Art.4 & 5.

[261] 'Questions and answers—EU Health: European Health Data Space', EEπ, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_2712.

[262] Art. 14 EHDS Regulation (such as patient summaries, electronic prescriptions, medical imaging studies, discharge reports etc.).

[263] EHDS Regulation, Art. 3. 4, 5, 6, 8 & 9.

[264] EHDS Regulation, Art. 7.

[265] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45.

[266] For other sector-specific (vertical) initiatives see, the provisions of PSD2 regarding access to data in the context of payment systems. The PSD2 allows these new payment service providers to obtain access to payment accounts of data subjects for the purposes of providing the said services.

[267] European Parliament, The European Health Data Space (2022), available at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740054/IPOL_STU(2022)740054_EN.pdf,13.

[268] EHDS Regulation, Art. 7 which provides natural persons the right to give access to or request a data holder from the health or social security sector to transmit their electronic health data to a data recipient of their choice from the health or social security sector, immediately, free of charge and without any hindrance from the data holder or from the manufacturers of the systems used by that holder.

[269] EHDS Regulation, Art. 15 & 23.

electronic health data providers, including for wellness applications.[270] Particularly, providers of EHR systems, medical equipment and high-risk AI systems are obliged to ensure that their products and services comply with common standards enhancing interoperability. This infrastructure makes health data access and health data portability more effective for primary use.[271]

Of particular significance for our purposes are the provisions on secondary use, which occur either at the initiative of the patients, or that of other data applicants that can be any natural or legal person.[272] This access for secondary use should be made available by health data holders (with the exception of natural persons including individual researchers and microenterprises), public and private entities, to, at a minimum, seventeen predefined categories of electronic health data,[273] through the intermediation of a health data access body that Member States should designate for secondary use of data.[274] In essence, health data holders must make available most categories of health data indicated in Table 1, with the exception of data that is not health-related or generated for non-health purposes, data that is inaccessible for sharing because it is stored locally on users' devices, or data held by healthcare providers that qualify as micro-enterprises.[275] This body may oblige data holders to make electronic health data that they control available.[276] According to the EHDS, health data holders for secondary use include healthcare and care providers, researchers in these sectors, and developers of related products or services (for example, undertakings developing wellness applications) and can be public, not-for-profit, or private.[277]

This mandatory access regime is managed through the intervention of health data access bodies.[278] Mandatory access to health data is provided for specific types of secondary use by third parties (explicit authorized uses), such as, among other things, for personalized healthcare, training, testing and evaluation of algorithms or the development and innovation activities for products or services in healthcare and health insurance,[279] even when these are protected by intellectual property rights and trade secrets.[280] The principle of access to health data is broadly construed, as demonstrated by the wide interpretation of purposes for which electronic health data can be processed for secondary use. For instance, what constitutes 'scientific research related to health or care sectors', encompasses research being carried out by both non-profit and profit entities.[281]

Secondary use of electronic health data is, however, prohibited if it would allow, among other things, taking decisions detrimental to a natural person or exclude them from the benefit of an

[270] EDHS Regulation, Chapter III.

[271] These rights result from Art. 15 GDPR providing to every data subject the right to access the personal data concerning him or her, and from Art. 20 GDPR granting data subjects a right to port these personal data, although the scope of this portability right is limited as it does not include real-time and full portability akin to 'data interoperability'. H. Schweitzer & A. Metzger, Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, (2023) 72(4) GRUR International 337, 340 and the bibliography cited.

[272] EHDS Regulation, Art. 50.

[273] EHDS Regulation, Art. 51 (e.g. electronic health records, person-generated electronic health data resulting from the use of medical devices, wellness applications or other digital health applications, genetic, genomic, proteomic and other omics data, health-related administrative data, electronic health data from clinical trials, electronic data related to insurance status, professional status, education, lifestyle, wellness and behaviour data relevant to health). According to Art. 51(2) Member States may provide for additional categories of health data.

[274] EHDS Regulation Art. 55.

[275] See, European Commission, Frequently Asked Questions on the European Health Data Space, op. cit., at 25–28.

[276] EHDS Regulation, Art. 2(2)(γ).

[277] EHDS Regulation, Recital 59.

[278] EHDS Regulation. Art. 57.

[279] EHDS Regulation, Art. 53(1)

[280] EHDS Regulation, Art. 52.

[281] EHDS Regulation, Art. 53(1)(e). See, European Commission, Frequently Asked Questions on the European Health Data Space, op. cit., at 31.

insurance contract, to develop products or services that may harm individuals and societies, or to 'carrying out advertising or marketing activities'.[282]

The EHDS does not impose any restrictions as to who can request access for secondary use: any natural or legal person may submit a data access application and may be awarded a data permit by the health data access body if the application fulfils one of the permitted purposes listed and the data users may access and process the electronic health data 'only in accordance with the data permit issued' and subject to conditions, such as the fact that 'they shall not re-identify' or attempt to re-identify the natural persons from which data was obtained.[283] An additional requirement for the date users is that they publish the outcome of the research based on the data no later than 18 months after the completion of the electronic health data processing or after having received the answer to the data request.[284] Access is provided through the intermediation of the health data access body that may issue a data permit and then request the electronic health data from the data holders, the data being made available to the data user within three (3) months after it has been received by the data holder.[285] The duration of the data permit should be that necessary to fulfil the requested purposes and in any case that duration should not exceed 10 years.[286]

For secondary use and interoperability of health data, a legal and governance infrastructure is also put in place, building on the establishment of health data access bodies in several Member States, with cooperation at EU level, through a network guaranteeing central access to health data.[287] Interoperability is defined broadly in the EHDS Regulation as 'the ability of organisations, as well as of software applications or devices from the same manufacturer or different manufacturers, to interact through the processes they support, involving the exchange of information and knowledge, without changing the content of the data, between those organisations, software applications or devices'.[288] This covers not only 'technical interoperability' (through the use of common protocols regarding the conversion, identification and logical addressing of transmitted data over a network), but also 'semantic interoperability' (through 'interfaces' containing the information necessary to 'run' the programs in a compatible format) and eventually 'semantic interoperability' (concerning the way the data—inferred in this context—is not only exchanged but also understood by AI tools).[289] The EHDS also provides for a specific organisational and technological infrastructure for secondary use (Health@EU) with the purpose of providing services to support and facilitate the exchange of electronic health data between national contact points for digital health of the Member States.

The statutory right for third parties to access data established by the EHDS Regulation is more expansive than the 'derived' right recognized in the Data Act, which only covers third parties that are acting on behalf of the end-user of the product and concerns individual-level data access and portability (thus not including aggregated or inferred data) and applies to data processing respecting the conditions agreed with the end-user. Gatekeepers are not excluded, as in the Data Act,[290] from being eligible third parties that may benefit from data access or

[282] EDHS Regulation, Art. 54.
[283] EHDS Regulation, Art. 61.
[284] EHDS Regulation, Art. 61(4).
[285] EHDS Regulation, Art. 60(2), a period which can be extended by a maximum of months.
[286] EHDS Regulation, Art. 68(12) with a possibility for one more extension for a period which does not exceed 10 years, at the request of the health data user.
[287] The health data access bodies ensure that role: EHDS Regulation, Art. 55.
[288] EHDS Regulation, Art. 2(2)f.
[289] EHDS Regulation, Recital 33, Art. 2(2)(f) and 23(8). On the broad definition of interoperability, see U. Gasser, 'Interoperability in the Digital Ecosystem', (2015), Berkman Centre Research Publication No. 2015–13 (defining interoperability as the 'ability to transfer and render useful data and other information across systems, applications, or components'); H. Hovenkamp, Antitrust Interoperability Remedies' (2023). All Faculty Scholarship. 2814. https://scholarship.law.upenn.edu/faculty_scholarship/2814.

portability, the EHDS not including even any reference to the term 'gatekeeper'! Similarly, the Data Act prohibited a third party from using the data it receives to develop a product that competes with the connected product from which the accessed data originate or share the data with another third party for that purpose, the purpose here being to protect the innovation incentives of the data holder manufacturer of the IoT product. However, no such limitation seems to exist in the EHDS Regulation, probably because the inclusion of similar limitations might have seemed unnecessary because secondary data users are obliged to share the research results or outputs of secondary use, including information for the provision of healthcare,[291] and the purpose for the secondary use of data is, as mentioned above, limited to very specific purposes.[292] The EHDS Regulation has also a broader scope than the DMA, to the extent that it does not only apply to gatekeepers but to any manufacturer and supplier of electronic health records systems and wellness applications placed on the market and put into service in the EU.

The EDHS goes further than the data access rules contained in horizontal regulatory initiatives, such as the data portability provided for in Article 20 GDPR. which only applies to data processed on the basis of consent or contract, only covers raw data and is of little practical utility in the context of digital healthcare applications as under the GDPR there is no requirement for the data controllers to support the same format of data as the entity requiring access to data but only a commonly used format.[293] The EDHS also covers raw as well as inferred data[294] (for example, a diagnosis done by a physician or a machine). For instance, while under the GDPR and Data Act the access/portability obligation covers only the raw material harvested (for example, number of steps taken by the use), the EDHS regulation also covers the software's conclusion regarding his or her health condition). It also enables the exchange not just of individual personal data but also of non-personal data and expands access to aggregated data, which are not covered by the GDPR portability remedy, with a view that sharing diagnostic and treatments for one set of patients may provide benefits for the clinical treatment of other patients.[295]

The provision of access to health data for both primary and secondary use requires data holders to incur additional costs. These costs are merely fixed, to build the health data access technical infrastructure, as the marginal costs for each transfer are close to zero.[296] With regard to secondary use, according to the EHDS Regulation, health data access bodies or trusted data holders may charge fees which 'shall be in proportion to the cost of making the data available and they shall not restrict competition'.[297] The EHDS specifies the cost-oriented structure of the pricing of this access in the sense that the health data access bodies should be able to cover the costs of their operations with fees set up in a proportionate, justified and transparent manner.[298] Part of these fees may include compensation for the data holders for the costs incurred 'for compiling and preparing the electronic health data to be made available for secondary use', in which case this part of the fees will be paid to the health data holder.[299] Any fees paid (including the compensation to data holders) by the data users shall be transparent and non-discriminatory.[300] The EHDS Regulation proposal also included the possibility to pay

[290] Data Act, Art. 5(3) & Recital 40 (the reason being the 'unrivalled ability of those undertakings to acquire data').
[291] EHDS, Regulation, Art. 61(4). The results and outputs should only contain anonymous data.
[292] EHDS Regulation, Art. 53.
[293] European Commission, Frequently Asked Questions on the European Health Data Space, op. cit., at 12. In the context of the EHDS, there will be an obligation on both sides of the data exchange to support export/import of data in the Electronic Health Record Exchange Format put in place by the EHDS.
[294] EHDS Regulation, Recitals 6 and 15.
[295] European Parliament, The European Health Data Space (2022), op.cit.,17.
[296] Ibid., 36.
[297] EHDS Regulation, Article 62(1).
[298] EHDS Regulation, Art. 62(3) and Recital 70.
[299] EHDS Regulation, Art. 62(2).
[300] EHDS Regulation, Art. 62(3).

additional fees to data holders for 'enriched data',[301] which however does not appear in the published text of the Regulation. If the data holders and the data users do not agree on the level of the compensation, the EHDS Regulation stipulates that 'the health data access body may set the fees in proportion to the cost of making electronic health data available for secondary use' and in case of further disagreement with the decision of the health data access body, there is a possibility to have recourse to dispute settlement bodies set by the Data Act.[302]

Commentators have criticized the approach followed by the EHDS Regulation Proposal and now the Regulation for not taking into account the fact that data holders may not have the incentive to incur fixed costs to build data-sharing infrastructure, particularly if they do not know the subsequent level and frequency of use of data that would have enabled them to calculate a fee rate or a marginal remuneration that would have fully compensated them for the incurred fixed costs.[303] For this reason, there have been suggestions for the development of a 'data cooperative' that 'would allocate participant data providers a share in the innovation value or health services market value to which their data contributed'.[304] As is however acknowledged, this approach may also run into difficulties, related to the measurement of the marginal value of data, and to the presence of a multi-sided business models and platforms, which makes such calculations more complex.[305]

The European Health Data Space Regulation's provisions for broader access to health data may create tensions with the GDPR, particularly given the special and sensitive status accorded to health data under data protection frameworks. The EHDS Regulation acknowledges that 'health data used for secondary use can bring great societal benefits', although it also recognizes the risks to privacy: for instance, it requires that secondary use should be 'based on pseudonymised or anonymised data, in order to preclude the identification of the data subjects'.[306] The data minimization principle may also require that, if anonymization would not suffice for the specific secondary use envisaged and there is a need to provide access to personal health data, health data 'should only be made available in pseudonymised format'.[307] This came as a reaction to concerns expressed by data protection authorities at an earlier version of the Regulation. It also integrates the 'citizen-centric' design that was early on promoted in the legislative process, but which later seems to have played a less significant role.[308] However, even this more measured approach did not alleviate concerns expressed by some stakeholders that the balance between privacy rights and data access in the EHDS proposal disproportionately favoured the latter.

Commenting on the EHDS proposal, the EDPB (European Data Protection Board) and the EDPS (European Data Protection Supervisor) released a joint opinion in 2022 in which they expressed 'certain key concerns', particularly regarding the protection of rights to privacy and data protection, concerning the categories of personal data, and the secondary use of such data.[309] According to this Opinion, the EHDS creates exceptions to the protection of personal

[301] EHDS Regulation Proposal, Art. 42(3).

[302] Regulation 2023/2854, Art. 10.

[303] European Parliament, The European Health Data Space (2022), op.cit., 37.

[304] Ibid.

[305] Ibid. For a more detailed discussion, see EY, Realising the value of health care data: a framework for the future, (2019) available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/life-sciences/life-sciences-pdfs/ey-value-of-health-care-data-v20-final.pdf.

[306] EHDS Regulation, Recitals 53 & 72. It is also acknowledged that certain categories of health data can remain particularly sensitive even when they are in anonymized format, which may subject access to them to specific limitations (see Recital 92).

[307] EHDS Regulation, Recital 72 & Art. 66(3).

[308] See, recital 19 of the Proposal and Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format (OJ L 39, 11.2.2019) and the discussion in P. Terzis & OE Santamaria Echeverria, Interoperability and governance in the European Health Data Space regulation, (2023) 23(4) Medical Law International 368, 371–372.

data as provided for in Articles 6 and 9 GDPR, mainly due to the facilitation of the secondary use of personal data from wellness and other digital applications, as well as wellness and health-related behavioural data. The joint Opinion raised the concern that the health data derived from wellness apps and other digital health apps are not subject to the same data quality requirements as those harvested from medical devices. It noted that 'these applications generate an enormous amount of data and can be highly invasive since it relates to every step individuals takes in their everyday lives'.[310] The Opinion also stated that '(even) if health data could be indeed separated from other kinds of data, inferences such as food practices and other habits could be easily made, revealing particularly sensitive information such as religious orientation'.[311] It is true that the EHDS Regulation Proposal did not adequately address these concerns, as it enabled access to data harvested by wellness apps or other wearables, only subject to the condition that users of these apps are informed about the capacity of such apps to be connected and to supply data to EHR systems or to national electronic health solutions.[312] The potential for conflict between the promotion of data access to enhance competition, on the one hand, and the protection of personal data and privacy, on the other, was also highlighted by some of the literature commenting on the EHDS Proposal.[313]

This raises important questions regarding the operational balancing of the various rights and interests at stake. The digital transition and growth of the EU digital health sector appears to be an important goal guiding trade-offs with privacy protection. More systematically, it also raises questions about the need for more extensive and intensive cooperation between data access regulators (including competition authorities) and data protection authorities, either in a more general context or specifically in the field of health data protection.[314] It also echoes discussions during the GDPR's adoption regarding data reuse for research purposes, which centred on balancing privacy risks against collective research and, with regard to health data, health benefits, as well as patient individual rights. These deliberations ultimately led to derogations favouring data access for scientific purposes in the GDPR's final text (Article 89), which prompted some observers to conclude that this represented 'a paradigmatic shift of the discourse around the GDPR-implementation away from 'protecting data' as key concern to 'protecting health' of individuals and societies at large'.[315] While the discussion at the GDPR involved a rhetoric about balancing between privacy and the interests and rights of patients, leading to the institution in Article 89 GDPR of some derogations to the core protective provisions of the GDPR (Articles 15, 16, 18, and 21),[316] the EHDS Regulation appears to strike a different balance between privacy risks and the economic (and other) benefits of secondary health data use, aligning with the EU's broader industrial policy strategy to develop its digital health

[309] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space (2022), available at https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en.

[310] Ibid., p. 4.

[311] Ibid.

[312] EHDS Regulation Proposal, Recital 35.

[313] See, M. Shabani & S. Yilmaz, Lawfulness in Secondary Use of Health Data: Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS, (2022) Technology and Regulation 128; P. Terzis & OE Santamaria Echeverria, Interoperability and governance in the European Health Data Space regulation, (2023) 23(4) Medical Law International 368.

[314] We may refer here to the emphasis put by the CJEU in Case C-252/21, Meta Platforms and Others, ECLI:EU:C:2023:537, para. 63, on the duty of sincere cooperation of national (competition) authorities (but this may also cover national health data access authorities) with data protection authorities, with regard to the consistency as to the implementation of the rules related to the protection of personal data and the need to consult and seek the cooperation of those data protection authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment.

[315] J. Starkbaum & U. Felt, Negotiating the reuse of health-data: Research, Big Data, and the European General Data Protection Regulation, (2019) (July–December) Big Data & Society 1, 8.

[316] Ibid., 6–8 (discussing the arguments put forward by those stakeholders which supported the collection and storage of health data in biobanks so as to promote research, particularly on rare diseases).

economy—an objective already evident in the European Commission's 2012 eHealth Action Plan.[317] Health data access within the specific purposes and under the conditions established by the EHDS Regulation remains the default position, but an opt-out mechanism accommodates the individual privacy interests of natural persons. Indeed, the final text of the Regulation requires Member States when implementing the Regulation to put in place 'accessible and easily understandable' mechanisms for natural persons to exercise their right to opt out 'at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use under this Regulation'.[318]

The EHDS Regulation nevertheless provides that, under certain conditions, a public sector body or Union institution, body, office or agency with a public health mandate—or entities entrusted with public health tasks or acting on behalf of or commissioned by a public authority—may request access to data for which an opt-out right has been exercised. This access may be granted for specific purposes, including scientific research conducted for important reasons of public interest if those data 'cannot be obtained by alternative means in a timely and effective manner under equivalent conditions'.[319] Care however should in this case be taken to respect 'the essence of the fundamental rights and freedoms', such derogation to the opt out being 'a necessary and proportionate measure in a democratic society to fulfil purposes of public interest in the area of legitimate scientific and societal objectives', any process complying with the prohibition on re-identifying or attempting to re-identify natural persons.[320]

The EHDS Regulation also establishes a potential opt-out regime for the primary use of health data, implementable at any Member State's discretion.[321] But here again, Member States retain some flexibility regarding the rules and specific safeguards governing this opt-out mechanism, particularly concerning healthcare providers' or health professionals' access to personal electronic health data in cases where processing is necessary to 'protect the vital interests of the data subject' or another natural person, even when the patient has exercised their right to opt out from primary use.[322] These opt-out provisions and the conditions to which they are subject to have the potential to readjust the current balance between data access and privacy values in favour of access.

VII. CONCLUSION

The EU legal framework relating to data access and portability has significantly evolved in recent years, with ever-expanding data-sharing obligations imposed on different economic actors through different regulatory initiatives and competition law enforcement. Although the legislator's starting point was a 'dignitary' perspective prioritizing individuals' fundamental right to access and port their generated data—suggesting a constitutional dimension to privacy protection, personal data protection, and individual rights to self-determination and digital sovereignty—subsequent legislative initiatives shifted toward a more utilitarian approach,

[317] European Commission, Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions—eHealth Action Plan 2012–2020—Innovative healthcare for the 21st century (2012).

[318] EHDS Regulation, Art. 71(1) & 71(2). It is further stipulated that 'natural persons who exercise the right to opt out should retain the ability to reverse their decision'.

[319] EDHS Regulation, Art. 71(4).

[320] EHDS, Regulation, Art. 71(5) & 71(6).

[321] Art. 8 & 10 EHDS Regulation. This means that Member States may choose to provide persons to withdraw their electronic health data completely from the data exchanges within the EHDS, although the data will be maintained in the local systems by the health professionals providing the treatment. See, European Commission, Frequently Asked Questions on the European Health Data Space, op. cit., at 14.

[322] EHDS Regulation, Recital 18 & Art. 10. Opting out from primary use does not necessarily mean that the patients are also automatically opted out from secondary use.

although this did not result in the adoption of a 'propertarian logic' with the formal recognition of property rights over data, at least in the sense of rights *in rem*.

Data-sharing obligations have expanded through the use of competition law and data access legislation to encompass situations where data is co-generated by end-users, business users, and other complementors within the context of digital business ecosystems' connexionist polity.[323] This approach may have partially drawn from a property rights narrative while adopting a relational perspective that accommodates differentiated levels of health data access based on the requesting actors, ultimately promoting data co-ownership rather than private ownership.

Simultaneously, the EU is proactively building through health data access regulation and the introduction of a cross-border infrastructure for the primary and secondary use of health data, data (but also knowledge) 'commons', open not only at the level of the ecosystem, but also more broadly to third parties data users,[324] to enhance cumulative innovation and facilitate the broader structural transformation in data-related industries currently dominated by non-EU players. Hence, this regulatory compass combines 'Schumpeterian workfare[325]'or 'Entrepreneurial State'[326] approaches with a 'Regulatory State'[327] approach that aims to promote a wider 'digital sovereignty' agenda, this time not only to ensure the digital constitutional privacy protection of natural or legal persons,[328] but also to take into consideration the structural imbalances between the various actors involved in data flows and to promote the geo-economic interests of the EU in the emerging digital health economic space competition.[329]

A fairness rhetoric is increasingly becoming an essential feature of the EU regulatory and competition landscape in this area, progressively replacing the property rights rhetoric that dominated early discussions about the emerging data economy. This shift reflects the transformational intent of these interventions—not merely to give stakeholders their due share in the data value generation and capture process, but also to ensure equality of economic opportunities for participants in the 'digital health business' and, more broadly, to facilitate the 'upgrading' of the EU economy through its digital transition.[330] The study analyses these differential data access regimes through the lens of competition law and digital regulation (including the EHDS), by examining their horizontal and vertical distributive impacts across three contexts: (i) between digital platforms/orchestrators and end users; (ii) between digital platforms and their complementors within an ecosystem; and (iii) between third-party business users external to the ecosystem and actors operating within it.

This ambition for fair conditions of data access is manifested by the legal engineering of a permanent infrastructure of data sharing, and with the enrichment of the 'commons' domain,

[323] See, I. Lianos, Minding Competition in Complex Adaptive Social Systems: The Sociological Approach to Competition Law (May 19, 2024). Faculty of Laws University College London Law Research Paper No. 19/2024, available at SSRN: https://ssrn.com/abstract=4851966, 60 et seq. (discussing how the formation of networks and connections between different actors and capabilities drives value generation in digital capitalism).

[324] The EHDS opens more widely access to health data to third parties external to a specific ecosystem in which health data was generated (see Section V.C.), but also knowledge commons to the extent that it requires the health data users to make public the results or output of secondary use (Art. 61(4) EHDS for the benefit of current or future generations. See also, P. Terzis & OE Santamaria Echeverria, Interoperability and governance in the European Health Data Space regulation, (2023) 23(4) Medical Law International 368, 372.

[325] B. Jessop, The transition to post-Fordism and the Schumpeterian workfare state, in R. Burrows & B. Loader (eds.), *Towards a Post-Fordist Welfare State?,* (Routledge, 1994), 13.

[326] M. Mazzucato, *The Entrepreneurial State* (Anthem Press, 2013).

[327] G. Majone, The rise of the regulatory state in Europe, (1994) 17(3) West European Politics, 77.

[328] G. Teubner, Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution, (2017) 3(1) The Italian Law Journal 193 (advocating for the establishment of digital constitutional rights on a transnational level).

[329] See, for instance, the recent calls by the Draghi report for the 'technological' or digital sovereignty of the EU: M. Draghi, The future of European competitiveness: A Competitiveness Strategy for Europe (part A), 2023, at 29–30.

[330] The term 'upgrading' is inspired by literature on Global Value Chains and has the specific meaning provided to it by this literature: see, O. Cattaneo, G. Gereffi, S. Miroudot, D. Taglioni, *Joining, upgrading and being competitive in global value chains: a strategic framework* (World Bank, 2013. Policy Research Working Paper, n. 6406).

thus complementing efforts to develop data commons under the Data Governance Act. For the EHDS initiative, developing data commons resources that can be used by businesses,[331] even data users situated outside the digital ecosystem controlling the data and those that have contributed to the data generation, remains a key concern. It also seeks to strengthen 'institutional-based trust' between data holders and data users,[332] through the operation of data intermediaries (including data brokers and data altruism organisations) (as established by the Data Governance Act), or through the operation of a mandated health data access framework managed and regulated by public data access bodies (as stipulated in the EHDS Regulation), both being important features of an EU Open Health strategy.

The emphasis put on health data access and the reuse of health data by EU competition law and digital regulation (DMA, Data Act and EHDS), or the constitution of health data and knowledge commons, implies that the EU legislator has the last couple of years proceeded to a different balancing between privacy risks (for the personal data of individuals) and the broader collective geo-economic benefits of developing a robust digital health economy in the EU, than at the time of the adoption of the GDPR. An opt-out mechanism certainly allows individuals to prevent the processing of their personal health data for secondary purposes (with the availability of similar mechanisms for primary use varying by Member State). However, this opt-out provision seems to be conceived as a narrow exception to the principle of data access, and subject to the specific purposes and conditions established for secondary use. This emphasis on health data access is further confirmed by the establishment by the EHDS Regulation of a public infrastructure for data sharing and interoperability, both for primary use (MyHealth@EU) and secondary use (Health@EU platforms), and EU harmonization of Electronic Health Record Systems (EHR systems)[333] as well as of health data access applications, health data requests and relevant templates.

By developing a 'health specific ecosystem comprised of rules, common standards and practices, infrastructures and a governance framework', relying on a public central digital infrastructure for cross-border data sharing,[334] the EHDS also appears to advance a strategy distinct from establishing a fully decentralized federated data infrastructure, as discussed at the time of the adoption of the EHDS Regulation.[335] Such an alternative approach would have enabled secure, eventually more privacy-centred data sharing among various actors/stakeholders (utilizing technologies like edge computing and personal health data spaces) and would have integrated diverse private initiatives.[336] Eventually, this choice may be reconsidered once technological advancements sufficiently address the privacy risks associated with sharing data across multiple sources[337] and eventually overcome the current lack of standardisation and protocols for federated data platforms. Such developments would enable broader implementation of federated data infrastructures and more decentralized health data access systems.

[331] Communication from the Commission, on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final, p.8.

[332] R. Bachmann, A.C. Inkpen, Understanding Institutional-based Trust Building Processes in Inter-organizational Relationships, (2011) 32(2) Organization Studies 281.

[333] EHDS Regulation, Chapter III.

[334] See, https://www.european-health-data-space.com.

[335] European Parliament, The European Health Data Space (2022), op. cit., 39–41.

[336] See the discussion in I. Lianos, Regulating access to data and computational infrastructure in digital health: the need for a holistic approach, in D. Mantzari & M. Ioannidou (eds.), *Research Handbook on Competition Law and Data Privacy* (forth. Edward Elgar, 2025), Chapter 1; R. Roth et al., Federated electronic health records for the European Health Data Space, (2023) *Lancet Digit Health*; 5: e840–47.

[337] See, for instance, the recent controversy in the UK about the contract between NHS and US-firm Palantir and its partners for the development of a federated data platform: R. Mason, Everything you need to know about NHS England's biggest ever IT contract, The Guardian (November 21, 2023), available at https://www.theguardian.com/society/2023/oct/12/everything-you-need-to-know-about-nhs-englands-biggest-ever-it-contract.

The study examines the interplay between these different dimensions of fairness, focusing on a particularly sensitive type of data: health data. It first examines the broader political economy of digital health and the competition issues raised by the concentrated economic structure of its value chain.[338] It then explores the interaction between various competition enforcement and regulatory tools at the EU level and the different data-sharing obligations implemented to regulate data relationships among stakeholders, with the goal of establishing a fair and dynamic digital health industry in Europe.

[338] See also, J. Kanter & M. Gaynor, The Rise of Health Care Platforms. JAMA. 2025 May 27;333(20):1773–1774. doi: 10.1001/jama.2025.3641. PMID: 40202741.

Journal of Competition Law & Economics, 2025, Vol. 00, No. 00, 1–52
https://doi.org/10.1093/joclec/nhaf016
Article