Data Brokers and European Digital Legislation

*Hannah Ruschemeier**

Targeted advertising, dark patterns and omnipresent data collection as the primary business model of the global online world have been the subject of an ongoing legal debate. One particular consideration involves the secondary use of data subsequent to its initial collection and exploitation. Data has proven to be a valuable commodity for actors previously unnoticed in digital environments: data brokers who trade in data. Their non-transparent business model carries structural legal, ethical and societal implications. This article analyses the data broker business model and the resulting conflicts with the European Data Protection Regulation (GDPR), incorporating interdisciplinary findings and the new legislative procedures at Union level into the legal analysis.

I. Introduction

While, or perhaps because data is ubiquitous and data brokers use a business model 'as old as the net itself'[1], they are not generally discussed publicly[2] or scientifically[3], as the companies involved have no interest in making details of their business models public. Big data is built on the idea that information can be gleaned from a large dataset which cannot be comprehended from its individual parts[4] and rapid datafication has fuelled business models for data brokers driving yet further datafication.[5] The term datafication itself refers to processes of rendering information into machine-readable quantifiable data for the purpose of aggregation, analysis, and anticipation of human behaviour and social interaction.

In this article, I assume that privacy is *one* of the protected goods of data protection[6], and examines the question of whether the data broker business model is compatible with European legislation on digitalisation. I will argue that this business model poses a threat to data protection and the privacy of individuals and creates ethical and structural problems for democratic societies from the perspective of EU-Law.

Resistance to such business models is once again growing as they are perceived as an outgrowth of an unequal data industry characterised by informational and economic power asymmetries.[7] German data protection authorities recently suggested banning the commercial data due to the provisions of the GDPR,[8] French[9] and Danish data protection authori-

DOI: 10.21552/edpl/2023/1/7

[*] FernUniversität in Hagen. For Correspondence: <hannah.ruschemeier@fernuni-hagen.de>.

[1] Guilherme Birckan et al, 'Personal Data Protection and Its Reflexes on the Data Broker Industry' in Rogério Mugnaini (ed), *Data and Information in Online Environment*s (Springer, Cham 2020).

[2] In the USA, there has long been a debate about the business model of aggressive data brokers, which is less pronounced in Europe.

[3] But for this see the US-focused contributions: Birckan et al (n 1); Matthew Crain, 'The limits of transparency: Data brokers and commodification' (2018) 20 New Media & Society 88; Yingzhi Nie and Xueping Han, 'Research on consumers' protection in advantageous operation of big data brokers' [2019] 22 Cluster Comput> accessed 15 September 2022; Jennifer B Glasgow, 'Data Brokers: Should They Be Reviled or Revered?' in Evan Selinger, Jules Polonetsky Omer Tene (eds), *The Cambridge Handbook of Consumer Privac*y (Cambridge Law Handbooks, Cambridge University Press, Cambridge 2018); Ashley Kuempel, 'The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry' [2016] 36 Northwestern Journal of International Law & Business; Laura Palk and Krishnamurty Muralidhar, 'A Free Ride: Data Brokers'Rent-Seeking Behavior and the Future of Data Inequality' [2018] 20 Journal of Entertainment & Technology Law; Carissa Véliz, 'Governing Privacy' in Justin Bullock et al (eds), *The Oxford Handbook of AI Governan*ce (Oxford University Press) 'Under-researched and under-regulated' Urbano Reviglio, 'The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview' [2022] 11 Internet Policy Review.

[4] Kenneth Cuckier and Viktor Mayer-Schönberger, 'The Rise of Big Data: How It's Changing the Way We Think About the World' (2013) 92 Foreign Affairs 28.

[5] Ibid.

[6] Raphaël Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection' [2013] 29 Computer Law & Security Review; Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' [2013] 3 International Data Privacy Law.

[7] Reviglio (n 3).

[8] David Sadler, 'Privacy advocates want to ban address trading' Globe Echo (03 May 2022) <https://globeecho.com/news/europe/germany/privacy-advocates-want-to-ban-address-trading/> accessed 15 September 2022.

[9] See the report of the French Data Protection Authority <https://www.cnil.fr/fr/> accessed 20 April 2023.

www.lexxion.eu

ties have warned data brokers about their business models and undertaken enforcement activities.[10]

The authorities are of the opinion that the case of commercial address trading without the consent of the data subjects is not permitted under the GDPR. The granting of consent however occurs at a time when neither the data subject nor the address trader know to whom the address may be sold in the future. Thus, this trade is likely to run up against a legal barrier. If this assessment is correct, this would have an impact on the entire application of the GDPR concerning the data broker business model.

I will argue that the business model of data brokers is in most cases not compliant with the GDPR, due to the fundamental problems of obtaining informed consent in digital environments and the need to balance this against the legitimate interest as a basis for the lawful processing of personal data. The data broker business model is not innovative digital technology but rather an invasive method transferred from analogue advertising mail and unwanted phone calls to targeted advertisement on the internet. The following briefly introduces the concept of data brokers and the cornerstones of their business model followed by an examination of the resulting problems and their connection to the socio-technological development of *datafication*.[11]

The resulting assessment, that there is no sufficient legal bases for most cases of digital commercial data trading draws on how the quantitative use of large amounts of data (big data) works through techniques such as predictive analytics, and how anonymisation and transparency are not suitable solutions. The paper concludes with an evaluation of the new legislation of the European Union and possible solutions.

II. What are Data Brokers?

The trading of data is a global industry worth multiple billions.[12] The data broker industry is very successful and active in the USA, the largest companies come from this region.[13] Europe has also seen an increasing focus on address trading, e.g. through address trading by the postal service in different countries.[14] Data brokers operate globally in a digital data ecosystem under different jurisdictions. The GDPR and other relevant European legislative acts, like the Digital Services Act (DSA) operate according to the principle of *lex loci solutionis*, thus applying to the activities of data brokers based outside the EU when they target European citizens, as reflected in the inclusion of large online platforms within the definition of data brokers.[15] Therefore, as even well-known data brokers from the USA, such as Acxiom are subject to European regulation when operating in Europe,[16] this analysis focusses on the European context

Data trading in general means obtaining or providing personal or non-personal data in exchange for money, products, and services.[17] Data brokers are companies who derive their principal revenue from providing data or inferences[18] especially about individuals and this information originates primarily from sources other than the data subject themselves. There are different kinds of data brokers working in different market areas, including marketing and advertising, credit scoring, insurance, fraud detection, and in the medical economy. No matter where the data brokers obtain their data, some of the data is user generated, provided intentionally and knowingly, but the majority of data is produced unknowingly by the data subjects: via smart wearables, connected apps, home assistant devices, and connected apps

[10] See, <https://www.vennershipley.co.uk/insights-events/data-brokers-fined-in-france-danish-fine-highlights-importance-of-employee/> accessed 20 April 2023.

[11] Cuckier and Mayer-Schönberger (n 4).

[12] Glasgow (n 3); Leanne Roderick, 'Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry' (2014) 40 Critical Sociology 729; Theodore Rostow, 'What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers' [2017] 34 Yale Journal on Regulation> accessed 15 September 2022.

[13] Jamie Pinchot, Adnan A Chawdhry and Karen Paullet, 'Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review' (2018) 19 IIS 92, 93.

[14] See eg BVwG Austria Partial recognition v. 26 November 2020 – W258 2217446-1/35E, BeckRS 2020, 51953; OGH Wien, Urteil vom 18.2.2021 – 6 Ob 127/20z (OLG Linz), BeckRS 2021, 20609; for Germany: Konstantin Kuchenbauer, 'Gewerblicher Adresshandel unter der Geltung der Datenschutz-Grundverordnung' (2022) 2 ZfDR 135.

[15] Reviglio (n 3), 4.

[16] See, <https://noyb.eu/en/illegal-credit-scores-noyb-amplify-pressure> accessed 20 April 2023.

[17] Bart Custers and Gianclaudio Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' [2022] 45 Computer Law & Security Review> accessed 15 September 2022.

[18] Further on the legal implications: Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review 1.

to create metadata,[19] providing data brokers with data from individuals who are unaware this information is being produced or processed.[20]

Sellers providing personal and non-personal data to a buyer in exchange for money, is a clear example of data trading by a data broker. From a legal perspective data brokers are defined as those obtaining direct or indirect commercial benefit within a transaction involving (personal) data, which does not include the data subject themselves. This is legally relevant as it determines which legislation, such as the GPDR, applies, and the resulting balancing of interests between data subject and data broker. Companies like Meta which give other companies access to user data in exchange for favourable treatment on their platforms will be discussed later.[21]

Data brokers operate in the field of secondary data use[22], their business model begins after data operators have received data from data subjects.[23] For this purpose, data brokers enter a civil law contract with their buyers and execute it by selling or renting data. The copies of data, like other raw materials, are often sold at a very low price[24] in a variety of cases, to different buyers.[25] These buyers then extract further information from the data sets via data mining, machine learning and predictive analytics; consequently, data brokers have no specific interests in, the purpose for which data is used, their business model begins and ends with the sale of data for the highest price to as many buyers as possible. This ultimate use however means, the data broker business model cannot be regarded in isolation from the problems around algorithmic discrimination,[26] lack of privacy[27] and structural threats for democratic values.[28] The sale of data as a product contributes to and exacerbates these problems, but so far the linkages have not been sufficiently named as the cause and to hold the brokers accountable.

1. Where do Data Brokers Obtain their Data?

Professional data brokers started collecting data long before the digital age. They have been gathering data from newspapers, magazines, mail-order retailers, polls, surveys, travel agencies, symposiums, contests, product registration, warranties, payment handling companies, and government records – effectively from every source of publicly available or easily accessible data.[29] People were receiving unwanted advertising calls and mail as a result of targeted advertising long before they went online and the structural enforcement deficit of data protection law means this will not change: individuals lack the incentive to take action against these breaches: they are annoying, but not perceived as serious. The retention of this reliance on enforcement of data subjects' rights

[19] Jurij Pfeifferet al, *Quantify-Me: Consumer Acceptance of Wearable Self- Tracking Devic*es (2016) <https://fim-rc.de/Paperbibliothek/Veroeffentlicht/560/wi-560.pdf>; Agnes Tegen, Paul Davidsson and Jan A Persson, 'Interactive Machine Learning for the Internet of Things'*, Proceedings of the 9th International Conference on the Internet of Thin*gs (ACM Digital Library, Association for Computing Machinery, New York,NY,United States 2019); Douglas J Leith, 'What Data Do the Google Dialer and Messages Apps on Android Send to Google?' in Fengjun Li et alSokratis Katsikas (eds)*, Security and Privacy in Communication Networks: International Conference on Security and Privacy in Communication Syst*ems (Springer, Cham 2023); Christian Rothet al, 'Are Sensor-Based Business Models a Threat to Privacy? The Case of Pay-How-You-Drive Insurance Models' in Stefanos Gritzalis et alIsmail Khalil (eds)*, Trust, Privacy and Security in Digital Busine*ss (Springer International Publishing, Cham 2020).

[20] Edith Ramirezet al*, Data Brokers: A Call for Transparency and Accountabili*ty (2014) <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> accessed 14 September 2022.

[21] Véliz (n 3); Glasgow (n 3) following a broader definition as well.

[22] Nanna B Thylstrup et al, 'Politics of data reuse in machine learning systems: Theorizing reuse entanglements' (2022) 9 Big Data & Society 1-10 argue that no rights of the data subject or transparency requirements can ensure protection from data reuse.

[23] Reviglio (n 3), 4 discusses whether Google and Facebook (Meta) should be considered as data brokers and concludes that they are more likely first-party data miners which distinguishes these firms from the focus on secondary data use here.

[24] Elisabeth Dwoskin, 'Data Brokers Can Buy Your Bank Account Number for 50 Cents' <https://www.wsj.com/articles/BL-DGB-39567> accessed 15 September 2022.

[25] Custers and Malgieri (n 17), 3.

[26] Sandra Wachter, 'The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law, preprint' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4099100> accessed 15 September 2022.

[27] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Helen Nissenbaum et alVictoria Stodden (eds)*, Privacy, Big Data, and the Public Good: Frameworks for Engageme*nt (Cambridge University Press, Cambridge 2014), 46.

[28] Kevin Macnish and Jai Galliott, 'An Introduction to Big Data and Democracy' in Kevin Macnish Jai Galliott (eds)*, Big Data and Democra*cy (Edinburgh University Press 2020).

[29] Abdullah Alowairdhi and Xiaogang Ma, 'Data Brokers and Data Services'*, Encyclopedia of Big Da*ta (Springer, Cham 2022); Jack Kim, 'On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship, A Report on the Canadian Data Brokerage Industry' [2006] 82 Information & Technology Law> accessed 15 September 2022.

for data protection law in its current form is a considerable factor in the new world of data trading.[30]

There are generally three options for obtaining data. The first is to simply buy data from other companies about their customers. Retailers sell data about customer transactions, websites sell clickstream data, social-media companies aggregate metadata to create individual profiles as their own individual product to be sold to data brokers.[31] In the second option, data brokers collect the data themselves via web crawlers or publicly available sources from commercial, civil society, and employment contexts or their own market research.[32] Data brokers may also extract data from various institutional resources, including federal, state, and local government and other public records like census data, court records, or commercial registers and the court system.[33] France was even moved to ban the automated analysis of judges' identity data to predict decisions in 2019, but did not block the analysis of other data or for other purposes.[34] Third, some data brokers acquire data via a daily feed from their data sources for batch processing.[35] In all cases, data brokers can combine their own sources with consumer data like social media, transaction data, data from wearables, etc.[36] There are various definitions and classifications of data brokers[37] due to how they collect their data, for the purpose of legal analysis, two elements are important: whether the data being sold is personal or non-personal and whether the entity selling the data does so for direct or indirect commercial benefits.

2. What is the Problem?

Data brokers sell data to clients in reference to a person's ethnicity, income, health status, sexual orientation, income, and other sensitive information.[38] From a legal perspective, this raises two key issues: the violation of privacy and data protection legislation, and non-transparent discrimination. Political science also argues that data traders undermine geopolitical stability and trust in data markets.[39] Treating these data as commodity than can be freely traded like any other creates significant issues for data protection and privacy both at an individual and collective level. Moreover, data brokers drive discrimination in algorithmic decisions[40] by selling data to banks, employees, insurance companies and governments.[41] practices from which consumers are currently not sufficiently protected.[42] This is partially because data brokers operate in the dark, e.g., there is no list of such companies in the EU.[43] Current laws struggle to capture such practices as data brokers are globally active and deeply integrated into the digital ecosystem.[44]

Data brokers create digital dossiers about individuals, for example consumer scores, for use by predictive analytics to forecasts about characteristics of individuals or their future behaviour.[45] This data forms the basis of largely incorrect predictions of patterns. Even the data companies considered to be the 'best' have provided only a 50% accuracy rate in the past,[46] resulting in false and unjustified derivations and pro-

[30] Pinchot, Chawdhry and Paullet (n 13), 92.

[31] Alowairdhi and Ma (n 29), 2.

[32] Kaliya Young, 'Data Broker Industry', *The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Soci*ety (Anthem Press 2020).

[33] Pinchot, Chawdhry and Paullet (n 13), 94; Reviglio (n 3), 6.

[34] Art. 33 loi 2019-22.

[35] Ramirezet al (n 20).

[36] Shivangi Mishra, 'The dark industry of data brokers: need for regulation?' [2022] 29 International Journal of Law and Information Technology, 399.

[37] Glasgow (n 3), 26.

[38] Like alcohol and tobacco interests, casino and gaming interests, religion and much more: Steven Melendez and Alex Pasternack, 'Here are the data brokers quietly buying and selling your personal information, You've probably never heard of many of the data firms registered under a new law, but they've heard a lot about you. A list, and tips for opting out.' Fast Company (02 March 2019) <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information> accessed 15 September 2022.

[39] Reviglio (n 3)., 15.

[40] Instead of all: Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' [2021] 41 Computer Law & Security Review> accessed 15 September 2022.

[41] Véliz (n 3).

[42] Nie and Han (n 3).

[43] Reviglio (n 3), 4.

[44] Chih-Liang Yeh, 'Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers' [2018] 42 Telecommunications Policy, 2.

[45] On the ethical implications of predictive analysis: Rainer Mühlhoff, 'Predictive privacy: towards an applied ethics of data analytics' (2021) Ethics Inf Technol 675.

[46] Pinchot, Chawdhry and Paullet (n 13), 96; Giridhari Venkatadriet al, 'Auditing Offline Data Brokers via Facebook's Advertising Platform' in Ling Liu (ed*), The World Wide Web Conferen*ce (ACM Digital Library, Association for Computing Machinery, New York,NY,United States 2019) show that data broker sourced information on Facebook are up to 40% non correct, even in the case of financial information.

files.[47] This is even more problematic in the age of big data where all kinds of ostensibly harmless information can lead to sensitive inferences about individuals, particularly in terms of access to financing or health care.[48]

Even the mere presence of sensitive files about individual internet users justifies the concern regarding data-security.[49] This is best exemplified by one of the worst data breaches in corporate history, executed against Equifax, one of the largest data brokers and consumer credit reporting agencies in the world.[50] In 2017, Equifax announced a data breach that exposed personal data of 147 million people, including those of customers in the UK, (then) European Union.[51] Even today, there is a lack of sufficient incentives for data brokers to encrypt and secure their data.[52]

Economically, the data broker business model increases inequality, because the valuable predictions and deductions of big data and predictive analytics require data from numerous individuals. Thus, individual data is only economically valuable as part of a data set, meaning individuals are excluded from realising value from their own data as against big data and '*Artificial Intelligence*' (AI). These structural informational power asymmetries, have not yet found an answer in data protection law.[53]

From a legal perspective, data brokers trading unmanageable quantities of data records undermine the rights of data subjects and thus the right to data protection[54] and privacy[55] under national[56] and European law. Although though much of the data is collected by data brokers is publicly available, it is still collected and especially sold without the data subjects' consent. The business model itself leads to problems in enforcing the rights of the data subject. In one case, an Austrian-based data subject filed an access request under Art. 15 GDPR to the data broker, seeking to identify where the data broker, an address publisher, had collected their data and to whom it had been sold. The company claimed not to know where it had obtained the data in question, the only information made available was that one of the addresses had been collected due to a '*relocation of the data subject*'.[57]

III. Datafication as a Socio-Technological Development

Datafication in the digital age is the structural transformation of nearly every aspect of human life into data. Since everything can be recorded as data and 'AI can make everything relevant'[58], datafication has become an irreversible, global process. Even though data brokers were active businesses before the rise of the digital economy, big data and '*AI*' have enabled a whole new dimension of data commercialisation which requires a constant data inflow. This is because the training or verification of learning systems is theoretically never complete. This perpetual development also means, there are virtually infinite possible uses for data. In the context of legal regulation, there is often a fixation on the application itself, for example the current media attention devoted to 'AI'.[59] This obscures the fact, that datafication and the success of machine and deep learning techniques have been heavily relying not only on the optimisation of hardware (processor capacity) and the availability of data (big data), but on human interaction.[60] Most individuals who are active online have developed a daily routine which discloses their personal informa-

[47] Wachter and Mittelstadt (n 18) propose a right to reasonable inferences.

[48] Wachter (n 26).

[49] Véliz (n 3).

[50] Neil Daswani and Moudy Elbayadi, 'The Equifax Breach', *Big Breache*s (Apress, Berkeley, CA 2021), 75.

[51] See, <https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf> accessed April 2023.

[52] Carissa Véliz, *Privacy is power: Why and how you should take back control of your da*ta (Penguin Random House, London 2021), 107 f.

[53] Ari E Waldman, *Industry unbound: The inside story of privacy, data, and corporate pow*er (Cambridge University Press, Cambridge, United Kingdom, New York, NY 2021).

[54] Art. 8 CFR.

[55] Art. 7 CFR.

[56] See e.g. the right to informal self-determination under the German Basic Law, Art. 1 (1), Art. 2 (1).For a critical analysis see: Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' [2021] 12 JIPITEC.

[57] NYOB, 'Address broker: GDPR-compliance "too burdensome"' noyb.eu (13 October 2020) <https://noyb.eu/en/address-broker-gdpr-compliance-too-burdensome> accessed 15 September 2022.

[58] Wachter (n 26).

[59] Hannah Ruschemeier, 'AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal' [2023] 23 ERA Forum.

[60] Rainer Mühlhoff, 'Human-aided artificial intelligence: Or, how to run large computations in human brains? Toward a media sociology of machine learning' (2020) 22 New Media & Society 1868 analyses the technical and ethical implications of AI systems based on human interaction.

tion: by using mobile applications, online shopping, using social media[61] or wearables that generate sensor data.[62] Through these activities, a huge number of individuals generate a variety of information that is delivered or sold by data brokers.[63] Today, data broker business models are inextricably linked to platformisation, the triumph of predictive algorithms and the digital oligopoly of a few global data companies. These companies have optimised the design of their interfaces so that users generate as much data as possible, which in turn can be used by the companies.[64] These clandestine mechanisms are not readily identifiable. These are further supplemented by more visible structures, such as the developing, clickworker industry in which people either work on job-platforms like Clickworker or via their smartphones,[65] which often targets economically disadvantaged people from the global south[66] who are specifically recruited to earn money through certain games.

IV. Legal Implications of Data as a Commodity

The legal nature of data has been a controversial topic. Additionally, the lines of argumentation are very diverse in different legal cultures, partially due to the particularities of national constitutional law. While some argue that data should be treated as 'property',[67] thus as an exclusive right with alignment function, others have argued solely for relative rights of use, collecting and processing of data.[68] Data ownership is not recognised under European Law. As a result, data subjects do not own their data, and cannot thus decide whether to give their data away.[69] However, the legal nature of data ownership would theoretically not prevent data trading anyway, as data subjects could also sell their personal data themselves to third parties, which could then be further sold. Under the current legislation of the GDPR and other legislative proposals of the European Commission,[70] data subjects have several rights regarding their data, eg revoking consent at any time,[71] the right to rectification,[72] the right to erasure.[73] However, these do little to counter the problematic effects of the data broker business model. This is mainly because as a business, data brokerage only works where it can systematically prevent data subjects from exercising these rights, mainly through a lack of transparency or clarity. In practice, partially due to the complexity of data supply and a lack of awareness, data subjects very rarely withdraw their consent.[74]

The fact is that data is a commodity in practice and that this commodity is traded commercially. At issue here is not users of purportedly free online services who 'pay'[75] with their data, but the data broker business model that relies on the secondary use of data. The initial obtaining of data involving the data subject personally is often based on consent to a powerful data controller, e.g. a social platform. However, the data subject is usually not aware of the sale of their data, or the scope of secondary data processing (see below), is not involved in the contract of sale, and has no possibility to negotiate conditions prohibiting secondary use of the data.

[61] Alowairdhi and Ma (n 29).

[62] Jan B Brönnekeet al, 'Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring' [2021] 21 Sensors> accessed 15 September 2022.

[63] Ramirezet al (n 20).

[64] See the examples of the ESP game Mühlhoff (n 60) on the concept of hidden labour by users: Paško Bilić, 'Search algorithms, hidden labour and information control' [2016] 3 Big Data & Society> accessed 15 September 2022.

[65] Alex de Ruyter, Martyn Brown and John Burgess, 'Gig Work and the Fourth Industrial Revolution, Conceptual and Regulatory Challenges' [2018] 72 Journal of International Affairs> accessed 15 September 2022.

[66] Richard Heekset al*, Digital Labour Platforms in the Global South: Filling or Creating Institutional Void*s? (2020).

[67] Patricia Mell, 'Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness' [1996] 11 Berkeley Technology Law Journal> accessed 15 September 2022; Michael C Pollack, 'Taking Data' [2019] 86 The University of Chicago Law Review> accessed 15 September 2022.

[68] Gianclaudio Malgieri and Václav Janeček, 'Data Extra Commercium' in Sebastian Lohsse, Reiner Schulze Dirk Staudenmayer (eds), *Data as counter-performance - contract law 2.0?: Münster Colloquia on EU Law and the Digital Economy* V (Nomos; Hart Publishing, Baden-Baden, London 2020)

[69] Custers and Malgieri (n 17).

[70] See VII.

[71] Art. 7 (3) GDPR.

[72] Art. 16 GDPR.

[73] Art, 17 GDPR.

[74] Custers and Malgieri (n 17), 8;

[75] Katherine Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' [2015] 2013 University of Chicago Legal Forum> accessed 15 September 2022 analyses the flaws in the analogy of data collection to payment.

V. Compliance with the GDPR

The GDPR does not directly address the subject of data brokers or data trading. Having data as its regulatory object would suggest that the GDPR regulates data trade. But data protection law is not aimed at restricting trade on the data economy, instead providing for the protection of personal data as consequence of the right to data protection. Data protection is the protection of fundamental rights. Regardless of the legal discussion about the legal nature of data, they are in any case factually transferable. Transferability means that a person other than the subject of that data can exercise the assigned powers,[76] in the case of data brokers, the trading of personal data of third-party data subjects. A distinction needs to be made between the rights of data subjects and the actual processes: although the rights of data subjects are inalienable,[77] data brokers actually monetise their data.

1. Scope of Application of the GDPR: Trading Data is Processing Data

The GDPR regulates the processing of personal data, consequently the information which data brokers trade have to be connected to an individual during the process of data processing. As the sale of that data is viewed as a contract, it does not necessarily fall within the scope of the GDPR. As long as the data subject is not named in the contract itself, which is unlikely when it comes to the sales of large data sets, there is no processing of personal data. But the execution of the contract will require the transfer of the data as the object of the contract to the buyer. This transmission constitutes the processing of personal data within the meaning of Art. 4 GDPR, which defines processing among others as 'as collection, recording, organisation [...] disclosure by transmission, dissemination or otherwise making available' thus capturing the transfer of data between the data broker and the buyer.

2. Legal Basis for Data Trading

The basic premise of Art. 6 (1) of the GDPR requires a legal basis for every processing of personal data. The existence of a legal basis also depends on the type of data, for example, Art. 9 GDPR defines stricter provisions for sensitive data.

In practice, data traders invoke legitimate interest as grounds for processing. For example, in the case of address trading, where effective consent can only be given to a specific address trader.[78] Although, Art 6 (1) b GDPR states that processing is legal when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, this legal basis is not relevant in the case of data brokers as this consent cannot be transferred to other transactions and the data subject itself is not a party of the data trade contract.

a. Consent

At a practical level, the most relevant legal basis for the lawfulness of processing data in digital environments is consent,[79] Art. 6 (1) a, Art. 7 GDPR. Problems with the legal construction of consent have been widely discussed[80], and without reproducing those discussions here, it should be noted that the requirements of informed and voluntary consent are not met in most cases of internet use. Furthermore, the digital era renders consent a fiction.[81] Users of the internet can easily see the arguments to this ef-

[76] By implication: Susan Rose-Ackerman, 'Inalienability and the Theory of Property Rights' (1985) 85 Columbia Law Review 931., 935.

[77] Custers and Malgieri (n 17), 9.

[78] Kuchenbauer (n 14), 138.

[79] Utz et al (n 79).

[80] Art 29 Working Party, 'Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation', adopted on 13 May 2013, <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf> accessed 15 September 2022; Barocas and Nissenbaum (n 27), 58; F. H Cate and V. Mayer-Schonberger, 'Notice and consent in a world of Big Data' [2013] 3 International Data Privacy Law accessed 15 September 2022; Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' [2013] 11 Northwestern Journal of Technology and Intellectual Property accessed 15 September 2022; Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74; in the context of automated processing: Michèle Finck, 'Smart contracts as a form of solely automated processing under the GDPR' (2019) 9 International Data Privacy Law 78.

[81] Hannah Ruschemeier, 'Privacy als Paradox?' in Michael Friedewald Alexander Roßnagel (eds)*, Künstliche Intelligenz, Demokratie und Privathe*it (Nomos, Baden-Baden 2022). For an overview of the debate see: Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' [2018] 4 J Cyber Secur.

fect: individuals cannot keep track of the numerous actors and processing purposes involved,[82] particularly as user-friendly consent forms cover such a quantity of information for each website that informed decision-making becomes impossible.[83] In the recent case of the Transparency and Consent Framework (TCF), the Belgian data protection authority noted that the TCF makes it difficult for users to obtain more information about the identity of all data controllers to whom they are giving consent before that consent is given. In particular, the Belgian DPA argued that the numerous recipients of consent would require users to spend a disproportionate amount of time reading all the disclosures, meaning consent could rarely be sufficiently informed.[84] Often, users are unaware of profiling[85] and thus cannot consent to further decisions about or based on that profiling.[86] Similar ignorance exists regarding the collective dimension of modelling predictive analytics, used for example by social media platforms to make predictions about their users. Collective data exploitation is inherent in the way predictive analytics works, but personal consent can de lege lata only refer to one's own data. However, where the release of one's own data has consequences for third parties, consent can never be a suitable instrument.[87] This applies to data brokers as well: data subjects will likely not foresee the consequences of giving consent to the selling of their individual data, especially in relation to connected services in the Internet of Things. Informed consent would require the data subject be informed in advance of whom the data is sold to, for what purposes, if that buyer will resell the data etc.

While it is theoretically possible to pursue the data broker business model in compliance with the GDPR, this would require preconditions for informed, freely given consent from the data subject to all purposes for which their data will be processed.

Data brokers selling large data sets, and predictive analytics, affects a majority of people by definition[88], making these conditions seem impossible to meet.

b. Legitimate Interests and Requirements of Art. 6 (1) f GDPR

Art 6 (1) f GDPR provides that processing is lawful where necessary for the purposes of pursuing the legitimate interests of the controller or by a third party, except where such interests are overridden by the need to protect the interests or fundamental rights and freedoms of the data subject which require protection of personal data, particularly where the data subject is a child. In the case of direct marketing there is no fundamental reservation of consent, which results from the reverse conclusion to Art. 21 (2) GDPR.[89] Here it is specified that the data subject has the right to object at any time where the data are processed for direct marketing purposes. However, as data brokers do not perform direct marketing, instead focussing on selling consumer profiles for other purposes like credit scoring etc, this does not apply. Whether preparatory measures like algorithmic grouping for concrete group-oriented advertising fall under the scope of the significant interferences of Art. 22 (1) GDPR is currently under debate.[90] The legality of data trading therefore depends on how the legitimate interest is defined.[91]

i. Legitimate Commercial Interest of the Data Broker

The broad wording of legitimate interests extends the understanding of legitimacy to cover every legal, economic, or idealistic interest with only hypotheti-

[82] In addition there is the problem of Dark Patterns: Mario Martini and Christian Drews, ‘Making Choice Meaningful – Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy Law’ (2022) <https://ssrn.com/abstract=4257979> accessed 20 April 2023.

[83] Zhonghao Yuet al, ‘Tracking the Trackers’ in Jacqueline Bourdeau (ed)*, Proceedings of the 25th International Conference on World Wide Web, Montreal, Canada, May 11 - 15, 20*16 (International World Wide Web Conferences Steering Committee, Geneva 2016).

[84] *Complaint relating to Transparency & Consent Framewor*k [2021] (Autorité de protection des donnes)DOS-2019-01377, available in English at: <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf> accessed 20 April 2023.

[85] Miranda Mowbray, ‘5 Big Data Ethics: Darth Vader and the Green Cross Man’ (2022) Future Law 131, 139.

[86] Maja Brkan, ‘Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond’ (2019) 27 Int J Law Info Tech 91.

[87] Rainer Mühlhoff and Hannah Ruschemeier, ‘Predictive Analysis und DSGVO’ in Telemedicus e.V. (ed)*, Recht der Informationsgesellschaft 2022* .

[88] Ibid.

[89] Recital 47 states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. This does not mean that the balancing of interests is no longer necessary, but only that the conditions for carrying out such a balancing of interests are met.

[90] Wachter and Mittelstadt (n 18).

[91] CJEU Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* [2014] para 28; CJEU Case C-597/19 *M.I.C.M vs Telenet BVBA* [2021] para 110.

cal and public interests excluded. Hence, interests are legitimate when they are following other norms of data protection law or the legal system in general.[92] The criterion of legitimacy does not limit the legal basis of data processing in a significant way, but data processing must be necessary for an interest to be legitimate. The question of whether the GDPR allows any conclusions at all about the assessment of purely commercial interests is controversial. Neither the GDPR nor the right to privacy[93] define an exclusive economic right of the individual to commercialise their data. While operating profit-oriented business models is legitimate or even desirable from a legal system perspective, data broker business model appears to be at odds with the requirements of necessity.

ii. Necessity and Overriding by the Interests of the Data Subject

Relying on the legal basis of legitimate interest to justify data processing for monetisation purposes is problematic.[94] Efficiency and expediency alone can demonstrate legitimate interest, but cannot satisfy the second requirement, that the processing of the data is *necessary*. Usually, the interests of the data controller, in this case the data broker, are opposite to the interests of the data subject concerning their fundamental rights to data protection. In contrast with the legitimate interest, the criterion of necessity is interpreted rather narrowly. Data processing is only necessary when the legitimate interest cannot be achieved by other means, indeed CJEU case law is limited to what is absolutely necessary[95]

Thus, the principle of proportionality requires necessity be determined on a case-by-case basis.

As the processing of certain sensitive data is prohibited, the nature of the data is the first relevant consideration when evaluating the rights and interests of the data subject.[96] This consideration must include the category of data, the special circumstances of the individual case,, requiring a balance of the imminent consequences and risks associated with the data processing.[97] This becomes particularly clear for sensitive data under the special requirements of Art. 9 (1) GDPR: in addition to the problematic processing basis of consent under Art. 9 (2), only the case of Art. 9 (2)e, according to which the data subjects themselves have made the sensitive data public.[98] This is further complicated by the fact that predictive analytics and big data make it almost impossible to draw a line between sensitive and non-sensitive data as any information about individuals can be inferred.[99] In the case of publicly available data, the CJEU has decided that data, made publicly available by the data subject themselves, is less protected than other kinds of data, with the specific purpose the individual was following while making data publicly available being key: being listed in the phone book is not the same as agreeing to advertising calls. Conversely, the processing of non-publicly accessible data is a serious interference with the fundamental rights of the data subject.[100]

This leads directly to the principle of data minimisation in Art. 5 (1) c GDPR: the processing of data must be limited to what is necessary for the purpose of the processing. This minimal processing however is challenged by the use of automated processing, big data[101] and predictive analytics can deepen the interference with the rights of the data subject.

Where data is traded for advertising purposes, the data broker seeks to provide a data set that offers the most accurate possible target group analysis of potential customers. For this custom tailoring data brokers use additional statistical and personal data consisting of a multitude of individual characteristics which aggregate and process the data. At certain intervals new target group analyses are carried out to update the system. Data brokers provide data that is of interest and relevance for their client's uses, usually requiring a significant quantity.[102] Therefore, da-

[92] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217, 2014), 32.

[93] Art. 8 CFR.

[94] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller (2014, WP 2017), 26.

[95] CJEU Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* [2014] para 28; CJEU Case C-597/19 *M.I.C.M vs Telenet BVBA* [2021] para 110.

[96] Art. 9 (1) GDPR unless there is an authorisation pursuant to Art, 9 (2).

[97] CJEU Case C-136/17 *GC and Others v CNIL* [2019] para 53.

[98] Custers and Malgieri (n 17), 9.

[99] Wachter (n 26), 20 '*AI can make everything relevant*'.

[100] CJEU Case C-469/10 *ASNEF v FECEMD* [2011] para 45.

[101] Michiel Rhoen and Qing Y Feng, 'Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science' [2018] 8 International Data Privacy Law> accessed 15 September 2022.

[102] Glasgow (n 3), 32.

ta brokers operate commercial data trading as a mass procedure. The goal of processing more and more data to achieve 'better' results via predictive analytics or to provide a broader data base to buyers is inherent to the data broker business model and does not comply with the principle of data minimisation.

Data brokers may achieve purely commercial interests with less data, temporary stored data, unconnected data, etc. All these factors must be interpreted in the light of the principles of data protection law, which highlights the fact that the trading of big data is not compliant with the GDPR. Furthermore, the possibility of drawing inferences about data subjects from the data set, the level of connectivity, and the duration of the storage of the data affects the right to data protection of the individual and must be considered. This weakens the position of data traders and strengthens that of data subjects in the necessity test.

Art. 5 (1) d GDPR requires data to be accurate and kept up to date which is not necessarily in the primary interest of the data broker companies. The principle of data accuracy can be invoked against the necessity of data processing for commercial purposes: if more than half of the data is not correct and, the individual right to reasonable inferences is yet to be invoked[103], the interests of the data subject retain primacy.

Additionally, data must be processed in a way that is comprehensible to the data subject.[104] It seems impossible for the individual person to understand how the data traded by data brokers is collected and processed when it comes to large data sets. In this vein, the secrecy surrounding data aggregation further interferes with the rights of the data subject. In the system of individual rights under the GDPR, this results in the data subject losing control of their data. Combined, the business model of data brokers who seek to compile and sell comprehensive tailored data sets combined with the technical functioning of big data analytics operating behind the scenes create a considerable risk potential for the fundamental rights of the individuals whose data are concerned according to Art. 7 CFR and Art. 8 CFR

In conclusion, data trading for purely commercial interests does not usually comply with the GDPR. The problem of the enforcement deficit reinforces this as data subjects can only exercise their rights against data protection violations if they know about them.

3. Problems of Profiling and Predictive Analytics on the Internet

As discussed, users, often unaware of the results of processing, only see fairly non-invasive tailored advertising. [105] However, the operations of data brokers, in the secondary use of individual profiles result in opaque processes using data collected from a multitude of individuals which may carry darker unseen implications. [106] These operations evade the GDPR, which is aimed at individual privacy and data protection, not its application to broader population groups.[107] Additionally, even where predictive analytics operate with non-personal data, it can still draw personal conclusions about individuals. [108] While the use of the results of a prediction model for targeted advertising aimed at individual users can fall within the scope of the GDPR, the collective element of modelling itself is not regulated.[109] The legal construction of consent and purpose limitation, designed to protect individual interests, means this exploitation of collective data is problematic as it does not cover collective effects on third parties. This application of predictive analytics calls for a new understanding of data protection law which includes a collective dimension. Understanding privacy as *predictive privacy*[110], enables normative protection mechanisms that

[103] Wachter and Mittelstadt (n 18).

[104] Art. 5(1) a GDRP.

[105] Today, Meta even advertises personalised advertising for an improved user experience.

[106] Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2019) Berkeley Technology Law Journal 1.

[107] In depth: Mühlhoff and Ruschemeier (n 87).

[108] Alessandro Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection' [2016] 32 Computer Law & Security Review; Akiva Miller, 'What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing' (2014) 19 Journal of Technology Law&Policy 41; Linnet Taylor, 'Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World' in Linnet Taylor, Luciano Floridi Bart van der Sloot (eds)*, Group privacy: New challenges of data technologie*s (Philosophical studies series, Springer, Switzerland 2017); Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475; Wachter and Mittelstadt (n 18).

[109] Cf. Wachter and Mittelstadt (n 18).

[110] Developed by Mühlhoff (n 45): 'predictive privacy of an individual or group is violated when sensitive information is predicted about them without their knowledge or against their will, in such a way that unequal'.
treatment of an individual or group could result'.

effectively include the collective effects of predictive analytics.

The data broker business model, significantly increases its non-transparency. Models produced by predictive analytics systems not only effect a plurality of persons, but also enable the companies that build these models to sell the specific results of collective data exploitation to third parties. This subsequent data use and its use by different actors in successive data processing operations for different purposes further increases the harm in individual and collective terms and creates an iterative interference in the protected right to data protection and privacy.[111]

4. Anonymisation and Transparency do not Solve the Problem

Anonymisation of data, often touted as the solution to the problem of privacy, will not solve the problem of the informal imbalance between commercial actors of the data industry and the data subject.[112] On the contrary, promises of anonymised data lead users, who are unaware of its collective application, to a false sense of security.[113] In addition, too often data that was thought to be anonymous has been actually re-identifiable.[114]

The transparency requirement is also not suitable for limiting the excesses of data trading, since data brokers will never achieve meaningful transparency.[115] More information about decision options do not linearly lead to more control. The call for transparency is common, eg when it comes to data protection declarations. However, transparency alone is not enough, comprehensibility and the free choice of several options is needed Calculated 'informational self-endangerment' can only apply if complete and coherent information is available as a basis for decision-making. Comprehensive transparency and disclosure about all relevant factors alone do not achieve an informed decision when this is not accompanied by understanding. The complexity of data processing in online services renders this illusory. The amount of information needed would not lead to actual understanding, but into the next paradox: the 'transparency paradox' in which the detailed clarification required to achieve transparency requires a quantity of information that makes it difficult for the average user to understand.[116] The complexity is multiplied when it comes to secondary data use by data brokers. *Crain* argues convincingly that data brokers will not cede control over their business object to data subjects without a significant reorientation of their industry.[117]

VI. New European Digital Legislation and its Effect on Data Brokers

The new legislative acts and proposals of the European Union do not address the subject of data brokers directly: the Data Act[118], the Data Governance Act[119], the Digital Services Act/Digital Markets Act[120] and the proposal for a regulation on Artificial Intelligence[121] leave the GDPR unaffected. The Artificial Intelligence Act proposal does not regulate data brokers as it targets AI systems and not data. The objectives of the proposed DSA/DMA do not target the protection of individuals from the practices of data brokers.

The DMA includes rules that govern gatekeeper online platforms, which have a systemic role in the internal market between businesses and consumers for important digital services as an anti-trust kind of mechanism on the use of data to exclude, as opposed to the protection of individuals from the application of collected data. Therefore, it uses an approach

[111] See Hannah Ruschemeier*, Der additive Grundrechtseingri*ff (Schriften zum öffentlichen Recht, Duncker & Humblot, Berlin 2019) on iterative interferences within fundamental rights.

[112] Michèle Finck and Frank Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' [2020] 10 International Data Privacy Law.

[113] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' [2009] UCLA Law Rev.

[114] Ibid.; In the jurisdiction of the CJEU data is anonymous, if it is not possible to identify the data subject. Although the CJEU also takes indirect identificaton (especially through the process of elimination) and identification possibilitys of third partys into consideration, it only regards those means, that are likely reasonably to be used by the data controller or any other person, so that the risk of identification appears to be insignifcant in the ex ante. This excludes any means that are illegal or require disproportionate effort. CJEU Case C-582/14 *Breyer v Germany* [2016] paras 40-47.

[115] Reviglio (n 3), 13.

[116] Ruschemeier (n 81).

[117] Crain (n 3).

[118] Art 1 (3) Data Act Proposal.

[119] Art 1 (3) Data Governance Act Proposal.

[120] Art 1a No 4 g) Digital Services Act Proposal of the European Parliament; Recital No 12 of the Digital Markets Act Proposal of the European Parliament.

[121] AI-Act Proposal, Explanatory Memorandum Para 1.2.

which is less based on individual rights than the GDPR and aims primarily to protect the markets from gatekeeper online platforms, which take advantage of their systemic role to weaken other market participants. The DSA addresses online intermediaries and platforms due to their significant reach and risks for the rule of law and fundamental rights.

The proposal for a Data Act (DA) aims to pave a new path for easy switching between cloud providers and lay the foundation for transparent access for consumers and businesses to their data. Although the DA aims to shape the European Data economy, its scope of application is rather limited and it is unlikely that the data broker business model will be affected by the new regulation. The DA standardises rules for access to data generated by the operation of networked products (IoT) and connected services for the benefit of consumers, commercial users and public authorities, as well as specifications for the drafting of contracts to be concluded when a data owner transfers data to third parties in order to satisfy data access requests. The DA also pursues objectives other than protecting the legal interests endangered by data brokers. Although it is also about data subjects profiting from the use of their data, the primary aim is to remove barriers to access. The provision of Art. 27 of the Draft Data Protection Act, which requires safeguards against access to non-personal data in an international environment, also primarily refers to government access and thus does not cover private data brokers. It is significant that the draft DA does not create any independent permissions where personal data is concerned, leaving the GDPR as the sole gatekeeper of personal privacy. The same applies to the e-Privacy directive. Therefore, the problems with the protection of personal data and privacy remain.

The Data Governance Act (DGA) is intended to provide a clear framework for the use of public sector data. Such rights may include trade secrets, personal data, or intellectual property. The DGA is not relevant to the data broker business model as it regulates the framework conditions for data access from public authorities and voluntarily data sharing. The data broker business model in contrast relies on aggressive and opaque data extraction from a variety of sources rather than freely shared data alone. In addition, the DGA makes it explicit that it is not intended to create new rights of access to data or obligations to share data, nor does it create an obligation for public bodies to allow the re-use of their data, the provisions of the GDPR also take precedence, Art. 1(2), (3) DGA. Although the DGA addresses data intermediary services, which could theoretically also include data brokers, it does not cover those engaged in data trading, but rather pursue the sole purpose of making the data available to the data users, Art. 10 (1). As this is not in the interest of data brokers, there is no incentive for them to act as data brokers under the DGA. If a company directly buys data and then sells them to others, this is not covered by the regulation.

VII. Conclusion

The commodification of personal information is the root of the informal and economical power imbalances in the digital world.[122] Even though the GDPR's regulatory framework is justly subject to much criticism, it theoretically offers a handhold against the business model of commercial data trading. As in many other areas, however, data protection law is subject to an enforcement deficit. Data brokers are inextricably linked to other threats to fundamental rights posed by digital capitalism, in particular collective impact, algorithmic discrimination and informational and economic power asymmetries. Many constructive solutions focus on the creation of new data subjects' rights, but these only address part of the problem. In order to address the threats to data protection and privacy in a legally efficient way, effective enforcement of existing regulations and guidelines that also take into account the economic position of certain companies are necessary. The new EU legislation is a step in the right direction, but it lacks a framework that effectively regulates the power asymmetries between powerful data processors, such as data brokers, and data subjects. A definition of data brokers and transparency rules, as called for by the DSA for large online platforms, would be a start.

[122] Crain (n 3).