Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy

Keywords: Data power; Right to data protection; Privacy; Special responsibility; Regulation; Mergers

The power exercised by technology companies is attracting the attention of policymakers, regulatory bodies and the general public. This power can be categorised in several ways ranging from the 'soft power' of technology companies to influence public policy agendas to the 'market power' they may wield to exclude equally efficient competitors from the marketplace. This paper is concerned with the 'data power' exercised by technology companies occupying strategic positions in the digital ecosystem. This data power is a multi-faceted power that may overlap with economic (market) power but primarily entails the power to profile and the power to influence opinion formation.

While the current legal framework for data protection and privacy in the EU imposes constraints on personal data processing by technology companies, it ostensibly does so without regard to whether or not they have 'data power'. This article challenges this assumption. It argues that although this legal framework does not explicitly impose additional legal responsibilities on entities with 'data power', it provides a clear normative indication that the volume and variety of data and the reach of data processing operations are relevant when assessing both the extent of obligations on technology companies and the impact of data processing on individual rights. It suggests that this finding provides the normative foundation for the imposition of a 'special responsibility' on such firms, analogous to the 'special responsibility' imposed by competition law on dominant companies. What such a 'special responsibility' might entail in practice will be briefly outlined and relevant questions for future research will be identified.

1. Introduction

The publication of the 'Cambridge Analytica' files has served to bring political and regulatory attention to bear on the power exercised by technology giant, Facebook. Yet, policymakers in Europe have been alert to the power of internet platforms for several years.[1]

[1] A platform is defined in the Commission's public consultation as 'an undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups'. European Commission, 'Public

For example, in 2015 the European Union (EU) Commission suggested that the way in which certain online platforms 'use their market power raises...issues that warrant further analysis beyond the application of competition law in specific cases'.[2] The EU Commission was right to suggest that the power exercised by digital platforms leads not only to economic consequences (which fall primarily within the scope of competition law) but also has broader societal ramifications. These economic and societal consequences stem, in large part, from the control exercised by digital giants over vast quantities of data, including personal data, leading some to query whether technology giants should be (further) regulated.[3] Critics of such further regulation suggest that targeted legislation – data protection legislation – already exists to regulate the processing of personal information by technology giants. Furthermore, they may suggest that competition law is waiting in the eaves, ready to be applied to curb the excesses of market power should the need arise. This article contributes to this debate by advocating that the rights to privacy and data protection found in European human rights instruments – in particular the ECHR and the EU Charter of Fundamental Rights – provide the normative foundations needed to justify the introduction of additional legislative and regulatory measures designed to tackle 'data power'. It also outlines some such potential measures and seeks to promote future scholarship on this topic by identifying pertinent research questions pertaining to each of them.

This paper shall therefore be structured as follows. In section two, the concept of 'data power' shall be introduced and outlined. Section three then examines the extent to which the EU privacy and data protection framework[4] takes account of scale and size, both in terms of the quantity of personal data processed and the size of the entities controlling personal data processing operations. This section concludes that although the legal framework does not

---

consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy' (September 2015). Available at: https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud, 5/. All urls last accessed on 9 April 2018, unless otherwise indicated.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final, 12.

[3] For instance, see: Aliya Ram, 'Tim Berners-Lee hits out at big tech companies' Financial Times, 12 March 2018. Available at: https://www.ft.com/content/743c9032-230c-11e8-add1-0e8958b189ea ; Jane Dalton, 'Facebook and Google are becoming too big to be governed, French president Macron warns', The Independent, 1 April 2018. Available at: https://www.independent.co.uk/news/world/europe/facebook-google-too-big-french-president-emmanuel-macron-ai-artificial-intelligence-regulate-govern-a8283726.html; and, for academic commentary, Lina Khan, 'The New Brandeis Movement: America's Antimonopoly Debate' (2018) 9(3) Journal of European Competition Law and Practice 131.

[4] As 'privacy' is a general principle of EU law (see Case C-137/79 *National Panasonic v Commission* [1980] ECR I-2033, paras 18–20), the EU jurisprudence fully incorporates the Article 8 ECHR jurisprudence and therefore this can be described as part of the EU legal framework.

explicitly impose additional legal responsibilities on entities with 'data power', it provides a clear normative indication that the volume and variety of data processed and the reach of data processing operations are relevant when assessing both the extent of obligations on technology companies and the impact of data processing on individual rights. Section four then identifies some of the potential policy ramifications of this finding and maps a future research agenda to explore the options identified.

2. The 'Data Power' of Technology Companies

2.1 Defining 'data power'

The power exercised by technology companies could be classified in numerous often-overlapping ways. For instance, technology companies exercise what might be described as 'policy power', a form of soft power allowing them to influence public discourse and policy discussions. This policy power was the subject of critical attention in the Summer of 2017, for example, when the head of 'Open Markets' at the New America Foundation, a Washington-based think tank, was allegedly dismissed from the Foundation as a result of his outspoken criticism of Google.[5] Such power can also be exercised when technology companies fund academic papers, an equally contested practice, or, more commonly, when they engage in lobbying. The EU's new data protection legislation – the General Data Protection Regulation (GDPR)[6] – has the unenviable honour of being the most lobbied piece of EU legislation to date.

Equally, we might think of the power exercised by technology companies as a form of media power. This is because online platforms such as Google and Facebook have the power to influence opinion formation by controlling what content their users see and when they see it. Users of social media increasingly rely on it as a news source while search engines are a credence good, leading to the so-called 'search engine manipulation effect' or SEME.[7] SEME does not mean that search engines deliberately manipulate their users but rather that users

[5] Kenneth P. Vogel, 'New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic, The New York Times, 1 September 2017. Available at: https://www.nytimes.com/2017/09/01/us/politics/anne-marie-slaughter-new-america-google.html.

[6] 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 - GDPR) [2016] OJ L119/1.

[7] Robert Epstein and Ronald E. Robertson, 'The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections' (2015) 112(33) Proceedings of the National Academy of Sciences of the United States of America E4512-E4521.

trust search engines to provide them with neutral, objective answers to search queries and thus they have the power to sway public opinion. Yet, although technology companies have this influence over opinion formation and exercise de facto control over the effectiveness of freedom of expression in the digital context, they generally benefit from intermediary liability exemptions and are not treated as media outlets and subject to traditional press regulation.[8]

This power of technology companies might be classified in a third way as 'market power'. Market power is a concept used in the application of competition law and economic regulation and is defined as the power of a company to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers.[9] Competition law intervention is, to a large extent, conditional upon a company occupying a dominant position, or acquiring a dominant position, on a relevant market and abusing that position of power.

In order to define the relevant market, a price-based substitutability test is applied which queries whether a customer would switch to another supplier if a company increased its prices in a small but significant manner. Companies to whom users would switch in the event of such a price increase operate on the same relevant market, and therefore exercise a competitive constraint on one another. However, if one company has – amongst other things[10] – a high market share on that market, it could be in a position of market power. What should be immediately apparent is that such a test does not adequately capture the relationship between individuals and digital platforms. First of all, many platforms are 'free at the point of access', therefore users find it difficult to perceive a change in price between platforms. Secondly, while platforms may compete on one side of the market (for instance, social networking sites, search engines and e-commerce platforms may compete to attract advertisers), users do not experience these platforms as competitors. For example, a user wishing to purchase a second-hand bicycle is more likely to turn to E-Bay than to Facebook in her search. Thus, the concept of market power – as currently defined – does not necessarily reflect the true power of certain platforms as experienced by users. Indeed Pasqualte accuses some scholarship of promoting the 'structural production of ignorance', by 'characterising scenarios as "consent" and "competition" when they are experienced by consumers and users

[8] In the EU this follows from Articles 12-15 of the E-Commerce Directive [Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market 2000 O.J. L178/1/. (EC)

[9] Case 27/76 *United Brands v Commission* [1978] ECR 207.

[10] Other factors, such as barriers to entry to a market, the stability of the market etc might be relevant.

as coercive and manipulative'.[11] Moreover, legal mechanisms that rely on the concept of market power, such as competition law and economic regulation, are concerned with economic harm rather than broader societal harms, a fact that has been noted by the European Commission.[12] Yet there have been calls in recent years to incorporate broader societal values, such as privacy, into economic assessments of the impact of competitive practices on quality[13] and for a change in how markets are defined so they more accurately reflect the reality of digital markets. For instance, the French *Conseil National du Numerique* has suggested that the notion should consider factors other than market share such as the power to 'undermine innovation through control of key resources, critical access points, visibility, information, etc.'[14] To date, these calls have however largely fallen on deaf ears.

It is for these reasons that this paper introduces the concept of data power. Data power is a multi-faceted form of power stemming from a company's control of data flows. Digital platforms are able to control such data flows as they are an example of a two, or multi-sided, market. This means that they act as the intermediary between one side of the market, for instance individual internet users, and others with whom they connect, including other individuals, advertisers, service or content providers. As online platforms act as an interface for these online interactions, they are in a unique position to control the flow of information – between participants in the digital ecosystem, and to gather data about the actions of each of these parties in the digital sphere.

While all digital platforms have this potential ability to control and gather data, some companies appear to have a superior ability to do so as a result of the volume and the variety of the data available to them. This is most notably the case of Facebook and Google, which shall be considered as examples here. These platforms can be set apart from others in four (non-exhaustive) ways. First, these platforms are omni-present in the digital environment. For instance, in 2016 only two of the top 10 smartphone applications in the US (based on the number of average unique users per month) were not owned by either Google or by Facebook.[15] Moreover, as discussed below, their presence has been augmented by a lax ex

[11] Frank Pasquale, 'Privacy, Antitrust and Power' (2013) George Mason Law Review 1009,1011.
[12] Digital Single Market Communication (n 1 above), 12.
[13] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Competition and Data Protection in EU Law' (2017)1 Common Market Law Review 1.
[14] *Conseil National du Numerique* (*CNNum*), 'Platform Neutrality: Building an open and sustainable digital environment', May 2014 (available at http://www.cnnumerique.fr/wp-content/uploads/2014/06/PlatformNeutrality_VA.pdf), 21.
[15] Sarah Perez, 'Facebook & Google dominate the list of 2016's top apps', 28 December 2016. Available at: https://techcrunch.com/2016/12/28/facebook-google-dominate-the-list-of-2016s-top-apps/

ante regulatory regime for mergers and acquisitions, allowing Google and Facebook to acquire would-be competitors and innovators. Crucially, this omni-presence allows these companies to gather a significant volume of data from a wide variety of sources. Furthermore, these platforms act as critical chokepoints (or gatekeepers) in the digital ecosystem: the exclusion of an application from Google's Android Operating System is likely to scupper its economic viability while Facebook and Google Search can significantly impact the extent to which information is disseminated by making it more or less visible on their platforms.

2.2 The implications of 'data power'

It is suggested here that, just as the actions of a company with 'market power' have an additional impact on the relevant market on which they operate, the actions of strategically placed companies with 'data power' have detrimental effects on individuals beyond that of companies that do not have 'data power'. While an exhaustive enumeration of such consequences is beyond the scope of this paper, two examples will suffice. First, the implications of profiling based on personal data processing may be particularly acute when conducted by those with data power.[16] Profiling can be used to differentiate between consumers based on the quality or the price of goods and services offered to them.[17] In practice, a company with data power could facilitate such a practice by restricting the products that are displayed to consumers or changing the order in which they are listed to display poorer quality products first in some circumstances. Profiling can also prey on user vulnerability.[18] While such profiling is not the sole purview of the digital platform with data power, it is problematic in this context. In particular, it exacerbates the asymmetry of power between companies which already have a 'self-reinforcing data advantage', and their users who are rendered transparent by this process to their own detriment.

---

https://techcrunch.com/2016/12/28/facebook-google-dominate-the-list-of-2016s-top-apps/ . Apple Music and the Amazon Application were the only two exceptions with Google owning five applications (YouTube; Google Maps; Google Search; Google Play; G-mail) and Facebook owing three (Facebook; Facebook Messenger; Instagram).

[16] The techniques used to profile or categorise individuals have been clearly outlined by the CMA in its report on uses of consumer data, and by the FTC in its report on data brokers. FTC, 'Data Brokers: A Call for Transparency and Accountability', May 2014; and, CMA, 'The commercial use of consumer data: Report on the CMA's call for information', CMA38, June 2015.

[17] As the CMA notes, the 'collection of consumer data may enable firms to make judgments about the lowest level of quality needed by consumers/groups of similar consumers. This may enable a firm to engage in quality discrimination where quality differences are not reflected in the price of goods or services.'

[18] Studies conducted by the UK Office of Fair Trading (OFT) on online targeted advertising and pricing, indicate that certain misleading pricing techniques could 'result in consumers making purchasing decisions they would not have made were prices more clearly advertised, or spending more than they needed to'.

A further concern is that those with data power will go beyond registering perceptions and create them. Research indicates that a Google search for Caucasian names present more neutral results than for typically African-American names. Given the reach of companies with data power and their control over the flows of personal data, this has the potential to have a tangible impact on opinion formation, including on political issues. As such, this data power leaves individuals open to manipulation and exploitation in ways that are difficult to detect and quantify.

Given these exacerbated concerns in the presence of data power, it is legitimate to query whether additional legal obligations should be applied to companies with such power. This paper argues that the legal framework for privacy and data protection provides a clear normative indication that the volume and variety of data processed and the reach of data processing operations are relevant when assessing both the extent of obligations on technology companies and the impact of data processing on individual rights.

3. The Normative Foundations for Regulating 'Data Power' in Privacy and Data Protection Law

3.1 Insights from the Right to Respect for Private Life

Pursuant to the case law on Article 8 ECHR, the mere fact of systematically collecting and storing an individual's publicly available personal data can constitute an interference with the right to private life. The European Court of Human Rights (ECtHR) has emphasised that an individual does not waive his rights by engaging in public activities that are subsequently documented.[19] It has also held that it is irrelevant whether this systematic collection and storage of data inconveniences the applicant, or whether the information concerned is sensitive or not.[20] The ECtHR has not had the opportunity to consider whether the aggregation of distinct datasets by a public authority (for instance, the consolidation of personal data held by a tax authority with that held by a department for social welfare) constitutes an interference with the right to privacy. However, it is suggested that such personal data aggregation can, in some circumstances, interfere with the right to private life. This is because personal data reveals more than the sum of its parts. By combining

[19] *Rotaru v Romania* (App No 28341/95) (unreported) 4 May 2000
[20] *Amann v Switzerland* (2000) 30 EHRR 843.

information from different quarters, it is possible to infer more about an individual than each individual piece of information reveals. The EU Court of Justice made its support for this theoretical underpinning explicit in the *Digital Rights Ireland* judgment.[21] It highlighted that the aggregation of communications traffic data permits 'very precise conclusions to be drawn concerning the private life of individuals' and that the retention of such data 'is likely to generate in minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[22] Indeed, this is why one of the critical 'v's' in the four v's often discussed in the Big Data context is 'variety', or variety of data. Moreover, this aggregation can render the individual totally transparent, allowing the entity holding the information to know perhaps more about the individual than he knows about himself. This transparency is problematic as it may have a chilling effect on individual behaviour. It can also leave the individual vulnerable to influence and discrimination by third parties. Furthermore, as information is power, and it increases the quantity of information in the hands of the entity aggregating data, it also increases the power of that entity and therefore exacerbates pre-existing power and information asymmetries.

At present, the systematic collection, storage and aggregation of personal data by companies with data power has an equally– if not more – negative impact on the rights of individuals as when these activities are undertaken by public authorities. Indeed, companies with data power are often referred to as gatekeepers as they have the power to determine what information can and cannot be made available to their users (by controlling the proverbial gate). Pursuant to regulatory theory, gatekeepers are non-state actors with the capacity to alter the behaviour of others in circumstances where the state has limited capacity to do the same.[23] This movement away from state actors towards the exercise of quasi-regulatory powers by private actors leaves a potential gap which, it is suggested, most of the recent regulatory initiatives targeted at digital platforms are grappling to define and to fill. This therefore begs the question whether there is a normative justification for extending the application of fundamental rights, or the duties flowing from these fundamental rights, to these actors. This question has, however, already been resolved by the jurisprudence of the ECtHR through its use of the doctrine of 'positive obligations'. According to this doctrine,

---

[21] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238.
[22] Ibid, [37]
[23] Emily Laidlaw, 'A framework for identifying Internet information gatekeepers' (2010) 24(3) International Review of Law, Computers & Technology 263, 265.

the State has a positive duty to take concrete steps in order to guarantee fundamental rights.[24] Such a positive duty to protect the fundamental right to respect for private life has been recognised by the Court in its jurisprudence.[25] Therefore, it can be said that the ECHR rights not only secure protection *against* the State but also protection *by* the State.[26] In the context of the right to private life this therefore means that the State has a positive obligation to safeguard the privacy rights of individuals from interference by other individuals and, critically, private entities such as companies with data power. The extension of such human rights obligations to private actors has not been without controversy. For instance, it has been suggested that it 'trivialises, dilutes and distracts from the great concept of human rights' and that 'it bestows inappropriate power and legitimacy on such actors'.[27] According to Frantziou, one of the primary concerns in this regard is that the imposition of human rights obligations on private actors will 'eventually reduce fundamental rights to ordinary private law claims, thus removing their symbolic value and the normative superiority that the possess constitutionally'.[28]

Two points might be made in this regard. First of all, if regulation is introduced to strengthen the obligations incumbent on private parties to respect fundamental rights, such regulation does not directly impose fundamental rights obligations – it does so indirectly. What is at stake is therefore the indirect application of fundamental rights obligations. Similarly, the interpretation of legislative provisions in light of Articles 7 and 8 of the EU Charter clearly creates obligations for private parties, albeit indirectly. Secondly, and beyond this semantic point, it can be argued that there is a strong case to be made to extend such fundamental rights considerations to private parties in the online environment. This is because, as the French *Conseil Nationale du Numerique* acknowledges, the digital ecosystem cannot be stifled 'under the oligoplisation by multinationals, whose influence equals or surpasses that of the State, but whose interests do not necessarily encompass the general interest'.[29] Put simply, given that the human rights system was codified in order to curtail the power of the State, when private parties exercise similar – or greater – power, it is legitimate to curtail this power in a similar manner. This article seeks to go beyond this now widely accepted claim

[24] For an early example, see *Airey v Ireland* (1979–1980) 2 EHRR 305, para 32.
[25] *X & Y v Netherlands* (1985) 8 EHRR 235.
[26] Andrew Clapham, 'The "*Drittwirkung*" of the Convention' in R St J McDonald, F Matscher, and H Petzold (eds), *The European System for the Protection of Human Rights* (Martinus Nijhoff Publishers, 1993) 163, 190.
[27] Clapham, *Human Rights Obligations of Non-state Actors* (OUP, 2006), 438.
[28] Eleni Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the European Union: Rediscovering the Reasons for Horizontality' (2015) 21(5) European Law Journal 657, 674.
[29] *CNNum*, 'Platform Neutrality' (n 14 above), 15.

that the application of human rights obligations should be indirectly extended to private actors. It suggests that additional legislative measures can be applied to companies with data power as a result of the volume and variety of data they process and the extent of their reach. Indeed, existing data protection law provides the normative foundations for such a claim by recognising that such factors are relevant when determining the nature and extent of data protection obligations.

3.2 The Ostensible Neutrality of the Data Protection Rules

The EU data protection rules apply to the 'processing' of 'personal data', with both of these terms defined expansively. This personal data processing is conducted by a 'data processor' but overseen by a 'data controller', the 'entity which alone or jointly with others determines the purposes and means of personal data processing'.[30] The EU data protection rules do not therefore make a (formal) distinction between personal data processing by public or private actors. Nor do these rules distinguish between the size of the entities conducting or controlling data processing, or the scale of the data processing activities. This is evident when one considers how the EU's Court of Justice has interpreted the so-called household exemption. Pursuant to this exemption, personal data processing 'by a natural person in the course of a purely personal or household activity' falls outside of the scope of the data protection rules.[31] While this exemption might have been interpreted by the Court to exclude small-scale data processing operations from the scope of application of the rules, the Court has steadfastly refused to do so. This is most evident in the unfortunate case of *Lindqvist*. Mrs Lindqvist, an elderly Swedish lady who had embarked on a part-time word processing course, was criminally prosecuted for unregistered personal data processing when she published the personal details of her church colleagues on a website without their consent. The Court in this case refused to apply the 'household exemption' given that, by uploading the information to the internet, Mrs Lindqvist had made it available to an indefinite number of people.[32]

The Court has more recently confirmed its restrictive interpretation of this provision in *Ryneš*[33], when the processing concerned was of personal data captured by CCTV footage. This footage was taken from a camera that the applicant had mounted outside his front door to film his garden path and part of a public footpath. Mr Ryneš was again a sympathetic

[30] Art 4(7) GDPR.
[31] Art 2(2)(c) GDPR.
[32] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, [47]
[33] Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů* [2014] EU:C:2014:2428.

applicant: he had installed the camera in response to attacks perpetrated against his family in previous years. He had also taken several precautionary steps to limit the interference with the rights of others caused by his processing, for instance he did not have real time access to the footage captured by the camera and the footage was deleted, if not required for the purpose of identifying would-be attackers, on a weekly basis. It was argued that Mr Ryneš' subjective intention was relevant to the application of the exception: he intended to process this data for purely personal purposes.[34] However, the Court held that the provisions of the Directive must 'necessarily be interpreted in the light of the fundamental rights set out in the Charter' and that exceptions to the Directive must be narrowly construed.[35] It therefore emphasised that the processing must be *purely* for personal or household purposes; as this surveillance covered a public space (albeit to a limited extent) it could not benefit from this exception.[36]

Lindqvist and *Ryneš* give the impression that the scale of personal data processing, or the reach of the data controller, are irrelevant for the purposes of the data protection regime. Yet, it is suggested that this impression is erroneous, as the Court's judgment in *Google Spain* illustrates. In that case, the Court emphasised that the personal data processing by search engines is distinct from that conducted by publisher websites[37] and is more likely to significantly affect the individual's rights to privacy and to the protection of personal data. It highlighted that the Google search engine enables any internet user to obtain a 'structured overview' of information relating to the individual, including 'information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been interconnected only with great difficulty'.[38] It also emphasised that this potentially detrimental effect on the individual is heightened 'on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous'.[39] It can therefore be concluded that in determining the nature and extent of the interference with a fundamental right respective the Court emphasises the interconnected nature of Google's data – a factor determined by the scale of its processing operations – and the ubiquity of Google,.

---

[34] Opinion of Advocate General Jääskinen, Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* EU:C:2014:2072, para 43.
[35] Para 29.
[36] Para 30 and 33.
[37] Para 36.
[38] Para 80.
[39] Para 80.

3.3 The Extent of Data Protection Obligations

While in *Google Spain* Google's ubiquity and the quantity of personal data it processed were relevant to the Court's assessment of the extent of the interference with the individual's rights, in the European Commission's initial proposal for the GDPR the size of the data controller was a factor in determining its obligations. In particular, the European Commission initially set out specific provisions for small and medium sized enterprises (SMEs).[40] For instance, the Commission was required to take appropriate measures for these companies when elaborating upon the procedures and mechanisms for exercising the rights of the data subject[41]; when further specifying certain aspects relating to the information to be provided to the data subject[42] and the responsibility of the data controller to ensure and to demonstrate that personal data processing is compliant with the Regulation.[43] The Commission had also proposed some leniency when it came to sanctioning SMEs for a 'first and non-intentional' breach of the GDPR, provided that the personal data processing was only ancillary to its main activity.[44] SMEs were also exempt from the obligation to designate a data protection officer[45] and to maintain documentation of all processing operations[46], provided that the personal data processing is an activity ancillary to its main activities.[47]

These exemptions for SMEs were motivated by a desire to reduce the regulatory burden on SMEs[48] and, no doubt, in part the initial thinking was that data processing by SMEs was likely to be less risky from a human rights perspective. However, the Commission proposal faced significant criticism on the grounds that it is inappropriate to distinguish between companies on the basis of size in this context: a very small (micro) enterprise might process vast quantities of sensitive data (for instance, the programmers of a fitness tracking

---

[40] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. According to recital 11, the 'notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium sized enterprises.'
[41] Ibid, Art 12(6).
[42] Ibid, Art14(7).
[43] Ibid, Art 22(4).
[44] Ibid, Art 79(3)(b).
[45] Ibid, Art 35(1)(b)
[46] Ibid, Art 28(4)
[47] Article 25(2)(b) also exempts third-country SMEs from the obligation to designate a representative in the Union.
[48] For instance, the Commission initially claimed that 'The data protection reform is geared towards stimulating economic growth by cutting costs and red tape for European business, especially for small and medium enterprises (SMEs).' See, European Commission, 'Progress on EU data protection reform now irreversible following European Parliament vote', 12 March 2014. Available at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm .

application) while a very large enterprise with thousands of employees (for instance, a textiles manufacturer) might process very little personal data, sensitive or otherwise.

Although the Commission was cognisant of this criticism and had attempted to mitigate its formalistic effects[49], it is unsurprising that amendments introduced during the legislative process placed less emphasis on the status of SMEs, preferring instead to focus on the scale of the personal data processing and the ensuing risks to the rights and interests of data subjects.[50] For example, the European Parliament replaced the Commission's proposal that SMEs should not employ a data protection officer with a suggestion that only legal persons which process data relating to more than 5,000 data subjects in any consecutive 12 month period should be obliged to hire a data protection officer.[51] This provision was ultimately replaced with one provides that an officer is needed if 'the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale'.[52]

Thus, emphasis on size was replaced by an emphasis on 'risk' in the final text of the Regulation. While some authors[53] and the Article 29 Working Party[54] assert that the data protection regime has always been a framework designed to regulate risk, the emphasis on risk in the Data Protection Directive[55] and in the jurisprudence of the Court[56] is subtle. In

---

[49] For example, while it exempted SMEs from the obligation to designate a data protection officer, the Commission nevertheless provided that a data protection officer is needed where 'the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects'. Ibid, Art 35(1)(c).

[50] This is not to say that all references to SMEs have been removed from the text of the GDPR. For instance, recital 167 GDPR specifies that in exercising its implementing powers, the Commission 'should consider specific measures for micro, small and medium-sized enterprises'.

[51] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 0011—C7-0025/2012—2012/0011. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN. Art 35(1)(b).

[52] Art 37(1)(b) GDPR.

[53] For instance, Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 3.

[54] It suggests that 'due regard to the nature and scope' of processing has 'always been an integral part' of the application of the fundamental principles applicable to controllers (such as the purpose limitation, data accuracy, etc) as they are 'inherently scalable'. A29WP, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', adopted on 30 May 2014 (WP218) 2.

[55] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/23. For instance, Article 8 of this Directive stipulates that the data subject's explicit consent is required as a legal basis in order to process sensitive personal data, which is arguably based on 'risk' considerations.

[56] For instance, see Case C-342/12, Worten—Equipamentos para o Lar SA v Autoridade para as

contrast, the GDPR places a general obligation on data controllers to take appropriate measures to implement the Regulation 'taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of the data subjects'. This emphasis on risk is also present in other provisions of the GDPR, such as those on data protection by design, the information to be provided to the data subject, data protection impact assessments and the security of sensitive data. The controller must take into account the risks to the rights and freedoms of the data subject in implementing each of these provisions. Unlike the Directive, the Regulation also attempts to identify data processing scenarios that might be particularly risky, such as when the data of vulnerable individuals like children or sensitive personal data are processed. It also specifies that the risks may be 'physical, material or moral' and identifies some potential harms such as identity fraud and discrimination.[57]

In the context of the present discussion, it is relevant to note that the GDPR, like the Directive, does not formally distinguish between data processing by small or large entities, or even on the quantity or scale of the personal data processing. Rather, it prefers to focus on the level of risk that a given processing operation may entail. However, this does not mean that the Regulation only applies to risky data processing operations: risk does not operate as a threshold condition in this way. Rather, as Hustinx points out, a risk-based approach simply means that 'more detailed obligations should apply where the risk is higher and less burdensome obligations where it is lower'.[58]

Thus, both the Court, through its rigorous interpretation of the household exemption, and the EU legislator, by refusing to tailor the application of the GDPR to SMEs, reject an approach to the application of the EU data protection rules based on size. No enterprise is too small, or no individual too insignificant, to fall within the scope of the data protection rules. However, once within the data protection rules, the volume and variety of the data processed and the its reach may be relevant in two ways: it may be relevant when assessing the scale of the obligations imposed on a data controller and it may be relevant when assessing the impact of

---

Condições de Trabalho (ACT) EU:C:2013:355, [24]. The Court recalled that the Art 17(1) obligations placed on the controller to implement 'appropriate technical and organisational measures' require the controller to 'ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected'.

[57] Recital 60 GDPR.

[58] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46 EC and the Proposed General Data Protection Regulation', 20, 38. Available at: https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf .

data processing on the rights of the individual. As noted above, pursuant to the risk-based approach, the scale of the obligations imposed on the data controller may depend on the 'riskiness' of a particular operation: important factors in this regard might include the nature of the personal data processed and also the size or scale of the personal data set. In *Google Spain* while the Court did not expressly single out the undertaking's size or the size of its dataset as significant factors, this is implicit in its finding that the *ubiquity* of Google was a crucial element in determining the extent of the interference with individual rights. Thus, we can conclude that although EU data protection law is ostensibly ambivalent to data power, it in fact provides a clear normative nudge that such power merits particular attention.

4. Tackling 'Data Power'

If the normative nudge from data protection and privacy law is accepted and we recognise the need to devote additional regulatory attention to companies with data power, it is necessary to consider potential causes of such data power and to identify appropriate regulatory responses. Several (non-exhaustive) factors that contribute to 'data power' might be identified: network effects; data as a barrier to entry; data-sharing agreements; data-driven mergers and acquisitions; and, a weak culture of data protection enforcement. An appropriate regulatory response to data power will address or mitigate these factors. As such, three potential responses are identified. At its most evident, the legislative framework for data protection could be strengthened. A more dramatic additional option would be to treat companies with data power as 'public utilities' and to regulate them as such while a more modest option would be to prevent companies with data power from artificially aggregating data through corporate agreements and data-driven mergers. This article briefly considers each of these options, which should not be treated as complements, and identifies pertinent research questions for future multi-disciplinary scholarship by those concerned with the rise of data power.

4.1 Enhancing the effectiveness of data protection

An immediate objection that might be raised to the imposition of additional regulatory duties on those with data power is that the very existence of data protection legislation should preclude the need for such additional measures. The data protection has thus far failed to curtail this power. This might be explained by two factors: one substantive, the other

procedural. From a substantive perspective, the data protection regime emphasises individual control over personal data by granting the individual 'micro-rights', which she ought to exercise. Yet, it is increasingly recognised that the role of the individual in achieving his or her optimal level of data protection should not be overstated: the volume of personal data processed as well as the complexity of personal data value chains limit the role the individual can meaningfully play in this picture. Information-forcing mechanisms are therefore unlikely to be effective given the extent of the power and information asymmetries in the information ecosystem. For instance, despite two decades of data protection legislation, the vast majority of individuals express concern over the processing of their personal data and feel like they lack control over this data and express their concern about this.[59] From a procedural perspective, the individual has not been assisted in this task of curbing data power through robust enforcement of the data protection framework. To date, this framework has been the subject of little public and private enforcement and a weak regime of sanctions.

The entry into force of the GDPR may remedy these deficiencies. Although it remains an individual-centric regime, placing increasing emphasis on individual control over personal data, it also introduces mechanisms to ensure the more effective enforcement of the data protection rules.[60] Most obviously it provides for enhanced administrative sanctions for breach of its provisions.[61] However, it also allows strengthens the hand of the individual vis-à-vis individuals by introducing a number of mechanisms for redress. As the enforcement of data protection law by national data protection authorities and in domestic courts has been quite limited to date, the introduction of Article 80 GDPR, entitled 'representation of data subjects' is perhaps of most significance. This provision enables collective actors to exercise the individuals' right to an effective remedy and to complain to a data protection authority, provided that the individual mandates them to do so. Furthermore, Article 80(2) allows Member States the possibility to introduce measures enabling representative actors to lodge a complaint before a DPA or to have an effective remedy against a DPA or data controller,

[59] See, for instance, the results of the Eurobarometer survey on data protection which concluded that only 15% of those surveyed felt they had complete control over the information they provided online and, of the other 85% of respondents, two-thirds claimed to be concerned about this lack of control. Eurobarometer, 'Special Eurobarometer 431: Data Protection – Summary', June 2015, 4. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2017/surveyKy/2075/p/2 .

[60] These mechanisms are contained in the provisions providing more support for supervisory authorities and more effective cooperation between them as well as oversight by a new agency (Chapter VI, Independent Supervisory Authorities, Chapter VII Cooperation and consistency); and in and Chapter VIII on Remedies, liability and penalties.

[61] Arts 83 and 84 GDPR.

independently of the data subject's mandate. The vast majority of EU Member States chose however not to implement this provision. Thus, it remains to be seen, and for future scholarship to probe, whether the modifications introduced in the GDPR will more effectively exercise a constraint on the data power of technology companies.

4.2 Data as a 'public good' and technology companies as 'public utilities'

A radical response to the presence of this data power would be to break up or unbundle certain technology companies. The European Parliament approved a resolution to this effect in 2014 when it called upon the European Commission 'to consider proposals with the aim of unbundling search engines from other commercial services'.[62] This resolution fell on deaf ears. While unbundling via regulation has occurred in some sectors, in particular where the economic operators in the sector are vertically integrated and competitive segments of their operations are used to prop up less competitive segments, competition law is often the preferred tool to deal with such problems as and when they arise. As Commissioner Oettinger put it, breaking up and expropriation are 'instruments of the planned economy, not the market economy'. Even if this option had more political support it poses further challenges for policymakers. First, it is difficult to determine which companies should be the target of such unbundling measures. For instance, Lotz highlights that Facebook Google, Amazon, Apple and Microsoft have all faced objections from users, the public and government agencies and, as such, have been lumped together under labels such as 'Big Tech', 'The Frightful Five' and GAFA. She suggests that conceiving of them as such makes their threat and influence overwhelming and masks the distinctiveness of their business models and practices.[63] Secondly, the purposes of this unbundling need to be defined. As Bennett Moses rightly suggests rather than thinking in terms of 'regulating technologies' or specific companies, it is preferable to identify how they fit into 'a pre-existing legal and regulatory landscape'.'64 Therefore, a crucial preliminary step when considering regulatory intervention of any form, especially radical regulatory intervention in the form of unbundling, is to articulate clearly what problems we seek to remedy and to identify scientifically the targets of that regulation.

---

[62] European Parliament resolution of 27 November 2014 on supporting consumer rights in the digital single market (2014/2973(RSP)).

[63] Amanda Lotz, 'Big Tech' isn't one big monopoly: it's 5 companies all in different businesses, https://inforrm.org/2018/04/01/big-tech-isnt-one-big-monopoly-its-5-companies-all-in-different-businesses-amanda-lotz/ .

[64] Lyria Bennett-Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (2013) 5(1) Law, Innovation and Technology 1, 17.

This article suggests that data power – the concentration of large volumes of data of different varieties in the hands of private economic entities – is the problem and that the holders of data power should be the ultimate targets of additional regulatory measures to curtail this power. Yet, this claim begs three significant questions, or sets of questions, that merit further investigation.

The first, and potentially most difficult, question to answer is what volume of data and what variety of data ought to be deemed problematic. The benefits of large-scale data aggregation and processing are frequently extolled in the context of 'big data' processing. The predictive power of processing such data can, for instance, lead to more relevant search results and shopping suggestions as well as the more efficient allocation of resources. Moreover, even in the context of public sector data processing the 'systematic collection and storage' of personal data by public authorities is an interference with the right to private life which can be justified. Defining the quantity and quality of data at which private sector data consolidation becomes problematic, and the circumstances in which such the disadvantages of such consolidation outweighs the advantage is is therefore a formidable challenge.

The second question relates to the role, if any, network effects and 'data as a barrier to entry' play in establishing data power. The presence of network effects means that 'greater involvement by agents of at least one type increases the value of the platform to agents of other types' (indirect network effect) or agents of the same type (direct network effects).[65] Therefore, direct network effects might be experienced in the context of a social networking service where the more individuals avail of the service, the more utility that service is to others. Indirect network effects occur when two or more distinct sides of a market benefit as a result of interaction on a platform. For instance, the more users avail of a search engine service like Google's search, the more interest advertising on that platform is for advertisers as they will reach a wider possible market. In particular, the data amassed by Google Search from past search results can be used by Google Search to enhance the relevance of its future search results. This superior ability to attract eyeballs – user attention – leads in turn to a superior ability to monetise their offerings. It is unsurprising that the entirety of the growth in digital advertising revenue in 2016 was extracted by two companies: Google and Facebook. The presence of network effects might point to the conclusion that the markets concerned are

[65] Colin Blackman and Romain Bosc, 'What is a platform and should they be regulated? Summary report', Centre for European Policy Studies (CEPS), 17 November 2015. Comments of Nicolai von Gorp, (https://www.ceps.eu/sites/default/files/CEPS%20What%20is%20a%20platform_summary%20report.pdf).

'winner takes all' markets. Similarly it has been suggested that if data is a barrier to entry to certain digital markets, then it is not possible to compete effectively with those already in possession of such data. This would further entail and exacerbate data power.

Both of these questions – whether network effects play a role in establishing data power and whether data constitutes a barrier to entry in digital markets – are empirical questions that have been singled out as questions but not yet adequately probed. According to Evans and Schmalense it is 'naïve armchair economics' to suggest that personal data is an indispensable input for competition (and therefore the lack thereof is a barrier to entry). Similarly, Varian claims that the quantity of data held by a company is never decisive rather it is what is done with this data that is important. However, in response it is possible to highlight that, to date, companies such as Google and Facebook have sought to guard their own datasets zealously and have as discussed below, demonstrated a clear appetite for more data through data-driven mergers and agreements. Further, they have offered no alternative to their 'free-at-the-point-of-access' services offered in exchange for personal data. Indeed, Pasquale suggests:

> If the platforms at the heart of the digital economy were entirely committed to monetization and efficiency, they would offer consumers more options. A user might be offered the opportunity to pay, say, twice the discounted present value of the data he was expected to generate for the platform. In return, he is assured that his data is unavailable for the platform's use. But such a seemingly Pareto-optimal arrangement is not on offer, and its invisibility suggests why imbalances of power, rather than efficiency or consent, ought to be the normative focus of antitrust and privacy law.[66]

If network effects are found to play a role in establishing data power it is also necessary to query whether these network effects are likely to work in reverse. Such reverse network effects are arguably visible in the decline of the shops on suburban high streets in the face of competition from digital retailers being a prime example. This is just one small example of the broader challenge in this area: regulators deciding to act in this field will need to tackle with the so-called Collingridge dilemma, or pacing problem. If regulators intervene too early, regulation might be pre-emptive and may not be based on adequate information. However, if regulation is delayed to a later stage of the technology's development and deployment, the technology may be too entrenched to regulate effectively.[67] As the *CNNum* points out, timing

[66] Pasquale, 'Privacy, Antitrust and Power' (n 11 above) 1023.
[67] Bennett-Moses, 'How to Think about Law, Regulation and Technology' (n 64 above) 7.

is of the essence in this context: 'before a player reaches critical mass, there is not much to monitor, but once a player does, it is often too late'.[68] Coates refers to this as the 'Goldilocks' problem, adding a third hurdle based on Schumpter's 'creative destruction'[69]: 'even when the porridge is just right, you still should not eat the porridge because something even better than porridge will come along soon'.[70] The issue of when to intervene can lead to regulatory paralysis.

Thirdly, if data is necessary to compete in relevant markets and network effects play a significant role in establishing and maintaining data power, then it is necessary to consider what regulatory remedies might flow from this.

A more moderate solution mooted is to treat the data held by companies with data power as an 'essential facility' or a 'public utility', rather than treating the company in its entirety as a public utility. In considering this solution however two key factors require further deliberation: first, what impact would this decision have on innovation? For instance, it has been argued that in order to benefit from network effects it is necessary to get the right *type* of customer on board and that this itself is an art. A good example here might be a booking application such as OpenTable, where it is not the overall quantity of restaurants that are available to book via the application is important. Instead, it is important that the restaurants available are in locations where there is a high density of OpenTable users. More importantly, the externalities of such data duplication need to be considered: such a solution may be sub-optimal – or even counter-productive – from a data protection and privacy perspective as, for instance, it would mean that personal data may be replicated outside the confines of the original data controller-data subject relationship.

4.3 Preventing the artificial aggregation of data

A third response to data power might be to prohibit the artificial aggregation of data power by companies with data through mergers and acquisitions and data-driven agreements. These acquisitions have been numerous (Google has acquired, on average, more than one company per week since 2010) and often high profile. While Facebook's Mark Zuckerberg stated in 2010 that the company's acquisitions were 'talent acquisitions', motivated by the desire to

[68] CNNum, 'Platform Neutrality' (n 14 above), 20.
[69] Joseph A Schumpeter, *Capitalism, Socialism and Democracy* (New York: Harper & Row, 1942).
[70] Kevin Coates, 'An Emerging Competition Law for a New Economy? Introductory Remarks for the Chillin' Competition Panel', 21 January 2016. Available at: http://www.twentyfirstcenturycompetition.com/2016/01/an-emerging-competition-law-for-a-new-economy-introductory-remarks-for-the-chillin-competition-panel/.

recruit the staff of the acquired company, subsequent acquisitions appear to be motivated by the desire to acquire data. Facebook's acquisition of consumer communications application Whatsapp is perhaps the most prominent example of this. Facebook acquired Whatsapp in 2014 for USD$19 billion, having obtained clearance for the transaction from both the US Federal Trade Commission and the EU Commission.

While the EU Commission cleared this transaction on the grounds that it would not significantly impede effective competition on any of the relevant markets, it failed to consider the impact of potential data aggregation from an individual's perspective. For instance, when considering the potential role of data in the post-merger landscape, it examined only whether other companies active in the market for online advertising services would have sufficient data to compete. In particular, it concluded that even if Facebook used data gathered via Whatsapp to improve advertising on its social networking service, there would continue to be a large amount of valuable user data that was not within Facebook's exclusive control. The Commission did evoke privacy, noting that it can constitute an important dimension of competition between Facebook and Whatsapp but concluding that they did not compete on this basis (ie privacy was not an important factor in the decision to use these applications).[71]

The Commission did not however consider whether the potential to aggregate data across platforms would have a negative impact on users. Two reasons explain this. First, the Commission may have been reluctant to explore this option in full given its firm assertion that 'any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules'.[72] Secondly, the Commission may have been confident about this approach as it naively believed that integration of data between Facebook and Whatsapp was unlikely to be straightforward from a technical perspective. Indeed, the Commission had asked Facebook whether it planned to link or match customers' profiles on Whatsapp with these customers' profiles on Facebook post-acquisition. Facebook had assured the Commission that the matching of Facebook and

[71] This, as Stucke and Grunes point out, misses the point from a user perspective. A very high percentage of Whatsapp users were already using Facebook's social network. This means that they could easily have used Facebook Messenger, which is integrated in the company's social network and offers similar functionalities. However, they chose not to: one reason for this may have been the superior privacy and data protection offered by Whatsapp. Thus, Whatsapp could have been viewed as a maverick in the market offering users a viable alternative to consumer communications applications using the prevailing industry model (a free platform subsidized by data-driven behavioural advertising). Maurice E. Stucke and Allen P. Grunes, *Big Data and Competition Policy* (OUP, 2016), 131-132.

[72] Case No. COMP/M.7217, *Facebook/ WhatsApp* C(2014) 7239 final, 3 October 2014, [164].

Whatsapp users would need to be done manually, by the users themselves. The Commission however subsequently concluded that this and other information provided by Facebook regarding the possibility of matching Facebook IDs automatically with Whatsapp users' mobile numbers was incorrect or misleading and that such information had been provided at least negligently. The Commission therefore fined Facebook €110 million.[73]

Crucially however, this transaction also boosts the power of Facebook: an already significant data aggregator. Other acquisitions, for instance, Google's takeover of various home monitoring and automation developers in 2014, allowing it to gather data from inside the home from cameras and smart technology sensors, were also given the go-ahead by competition authorities. These conglomerate mergers were not viewed as problematic given that Google did not compete with any of the companies it was acquiring. However, once again this analysis ignores the data-driven impetus for the transaction and the subsequent accumulation of power – data power – in the hands of the tech giants.

A similar impact could, of course, be achieved through data-driven agreements. Indeed, critics of further intervention in data-driven mergers point to this possibility in order to highlight its futility. Olhausen and Okuliar, for instance, argues that any attempt to introduce privacy considerations into merger control would be thwarted by companies entering into agreements with other companies to data-share instead of merging.[74] Onboarding agreements are on such form of agreement. Onboarding agreements allow for the combination of data collected online and offline. For instance, EPIC – a US not-for-profit organisation – is, it is reported, currently taking legal action in the US against Facebook on these grounds. Facebook allegedly partners with Acxiom which holds data on 700 million people and Datalogix which holds $2 trillion worth in offline purchase-based data. Again, in examining the legality of such agreements competition authorities consider simply their economic effects on equally efficient competitors rather than the broader societal implications of data consolidation by private actors. Partnership agreements between those with data power and other stakeholders, for instance public bodies, may also aggrevate such power. One such example is the partnership between Deepmind (held by Alphabet, Google's parent company) and the NHS Royal Free Trust in London. This partnership saw the NHS Trust hand over the data of 1.6 million patients of the Trust without their consent and without a commitment on

[73] Case No. COMP/M.8228, *Facebook/ WhatsApp* C(2017) 3192 final, 17 May 2017.
[74] Ohlhausen and Okuliar, "Competition, Consumer Protection, and the Right (Approach) to Privacy", (2015) Antitrust Law Journal 121, 132.

Deepmind's part to separate this data from that held by its parent company. While such examples are thankfully rare, they do illustrate that such public-private collaborations may augment and enhance the datasets of digital giants.

Despite this aggregation of data power through acquisitions and agreements, the competition law framework does not at present consider its direct non-economic impact on individuals. This situation could be rectified if competition authorities would themselves reconsider how they analyse such data-driven mergers and agreements or, preferably, if economic transactions could be subject to a parallel non-competition analysis in order to examine their broader societal impact. There has been much resistance to the introduction of non-competition concerns into merger analysis. Yet, given the unprecedented power of technology companies, being exercised across all walks of life, this option might be the least radical available to policymakers to keep this power in check.

Precedent for such an assessment of the compatibility of a proposed merger with fundamental rights exists. Although the Commission has sole jurisdiction to provide clearance for a merger with an EU dimension, a merger may be remitted to a Member State for a further assessment on non-competition grounds. This power is provided for by Article 21(4) of the EUMR which states that:

> 'Member States may take appropriate measures to protect legitimate interests other than those taken into consideration by this Regulation and compatible with the general principles and other provisions of [EU] law".

Most EU Member States have enacted broad powers, in addition to their competition law powers, to examine the impact of a merger on the 'public interest'. In such circumstances, the application of competition law, or purely economic considerations, is excluded in order to preserve a particular value. Some of the public interests recognized as legitimate in this provision are 'public security, plurality of the media and prudential rules'.[75] Member States may then prohibited the merger provided that this action is proportionate and non-discriminatory. This provision does not therefore, as Jones and Davies observe, confer new

[75] S 47. For instance, in the UK the Enterprise Act 2002 enables the Secretary of State to prohibit or authorise relevant mergers on specified public interests grounds, including national security, the stability of the UK financial system and media public interests considerations. This power is subject to some conditions and new public interest considerations may be added by order of the Secretary of State.

rights on Member States. Rather, it 'articulates their inherent power to impose, subject to EU law, obstacles to investment or make it subject to additional conditions and requirements, on the basis of public interest grounds'.[76]

It is suggested that as media plurality considerations can be taken into account when analyzing media mergers, a strong case can be made by analogy that data protection and privacy considerations should also be taken into account. Media plurality, like data protection and privacy, is provided for explicitly by the EU Charter, Article 11 of which states unequivocally that 'the freedom and pluralism of the media shall be respected'. Mergers in media markets are therefore routinely subject to a non-competition analysis, with a negative impact on media plurality treated as a separate rationale for market intervention.[77]

Such a regulatory response does however beg a number of question that require further attention. One such question, already mentioned above, is how to identify an objective threshold for intervention on the grounds of data power: what factors should be taken into consideration? How much personal data is too much? While it is true that it would be challenging to pinpoint such a threshold, it would not be impossible. Again, precedent exists in the context of media plurality: for instance, the European Commission support an independently implemented Media Plurality Monitor (MPM) which enables it to identify potential risks to media pluralism in Member States. Moreover, the MPM adopts a broad notion of media pluralism that incorporates political, cultural, geographical, structural and content related dimensions.[78] It should also be noted that even under the current merger framework, the Commission is asked to make assessments that involve quasi-subjective metrics. For instance, how can decreased choice weighted against increased efficiency? Such incommensurability abounds even within the 'objective' economics-based framework of competition law.

5. Conclusion

As the Conseil National du Numerique acknowledges, the strength of internet platforms lies in their 'ability to create great value from the data retrieved from users'. It also, however, suggests that the use of this data must ensure respect for the 'data rights' of users and that

[76] Alison Jones and John Davies, 'Merger Control and the Public Interest: Balancing EU and National Law in the Protectionist Debate' (2014) European Competition Journal 453, 488.
[77] For a discussion of how this operates in the UK, see Rachael Craufurd Smith and Damian Tambini, 'Measuring Media Plurality in the United Kingdom: Policy Choices and Regulatory Challenges' (2012) 4(1) Journal of Media Law 35.
[78] For further information and access to the 2016 report see: http://cmpf.eui.eu/media-pluralism-monitor/ .

recent events have illustrated that current practices do not make it possible to reach these goals.'[79] This article has argued that more must be done to tackle 'data power'. The rights to data protection and privacy, through their preference for data minimisation and disaggregation and their attempts to curtail the implications of power on individuals, provide a solid normative foundation for such additional measures. The challenge is however to identify practical regulatory responses to such data power. This paper has suggested a number of options and identified relevant queries for scholars concerned with data power to interrogate.

[79] CNNum, 'Platform Neutrality' (n 14 above), 6.