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

*Orla Lynskey**

The power exercised by technology companies is attracting the attention of policymakers, regulatory bodies and the general public. This power can be categorized 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 Article is concerned with the "data power" exercised by technology companies occupying strategic positions in the digital ecosystem. This data power is a multifaceted 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 probes 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 to do so. The volume and variety of data and the reach of data-processing operations seem to be relevant when assessing both the extent of obligations on technology companies and the impact of data processing on individual rights. The Article 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 with market power. What such a "special responsibility"

---

* LSE, Law Department. Cite as: Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 Theoretical Inquiries L. 189 (2019).

might entail in practice will be briefly outlined and relevant questions for future research will be identified.

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.[1] Yet policymakers in Europe have been alert to the power of internet platforms for several years.[2] 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."[3] 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.[4] Competition law,

---

1 Patrick Greenfield, *The Cambridge Analytica Files: The Story so Far,* The Guardian (Mar. 26, 2018), https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far.

2 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." *Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy* (Sept. 24, 2015), http://ec.europa.eu/information_society/newsroom/image/document/2016-7/efads_13917.pdf.

3 *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*, at 12, COM (2015) 192 final (May 6, 2015).

4 *See, e.g.*, Aliya Ram, *Tim Berners-Lee Hits out at Big Tech Companies*, Fin. Times (Mar. 12, 2018), 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*, Indep. (Apr. 1, 2018), https://www.independent.co.uk/news/world/europe/facebook-google-too-big-french-president-emmanuel-macron-ai-artificial-intelligence-regulate-govern-a8283726.html. This matter was investigated in a 2018 inquiry by the House of Lords. *The Internet: to Regulate or Not to Regulate? Inquiry*, Parliament, https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/

in particular Article 102 TFEU, lies waiting in the eaves, ready to be applied to sanction abuses of market power that exclude equally efficient competitors from the market or exploit consumers. Moreover, in the EU at least, data protection legislation already exists to regulate the processing of personal information by technology giants, amongst others.[5] Despite these existing legal provisions, this Article suggests 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/or regulatory measures designed to tackle "data power." It also outlines some such potential measures and seeks to promote future exploration of this topic by identifying some pertinent research questions.

This Article is therefore structured as follows. Part I articulates some of the reasons why the concept of ill-suited as a starting point for the assessment of the consequences of data aggregation while introducing and outlining an alternative conceptual lens, that of "data power". The current deficiencies of this concept are also recognized. Part II then examines the extent to which the EU privacy and data protection framework[6] takes account of scale and size, in terms of both the quantity of personal data processed and the size of the entities controlling personal data-processing operations. This Part concludes that although the 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 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. Part III then identifies some of the potential policy ramifications of this finding and maps a future research agenda to explore the options identified.

---

inquiries/parliament-2017/the-internet-to-regulate-or-not-to-regulate/ (last visited Apr. 9, 2018).

5 Council Regulation 2016/679 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

6 As "privacy" is a general principle of EU law, the EU jurisprudence fully incorporates the Article 8 ECHR jurisprudence and therefore this can be described as part of the EU legal framework (see, for example, Case C-137/79, Nat'l Panasonic v. Comm'n, 1980 E.C.R. I-2033, 18-20).

I. The "Data Power" of Technology Companies

A. 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 Market" 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.[7] 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)[8] — has the unenviable honor 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 Search, Twitter, Facebook and the Apple App Store have the power to influence opinion formation by controlling what content their users see and when they see it. Users of social media often rely on it as a news source (although this trend is perhaps on the decline),[9] while search engines are a credence good, leading to the so-called "search engine manipulation effect" or SEME.[10] SEME does not mean that search engines deliberately manipulate their users, but rather that users 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, from a legal perspective they are not treated as media outlets. Rather, they generally benefit from intermediary liability exemptions,

---

7 Kenneth P. Vogel, *New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic*, N.Y. Times (Sept. 1, 2017), https://www.nytimes.com/2017/09/01/us/politics/anne-marie-slaughter-new-america-google.html.

8 GDPR, *supra* n 5.

9 Nic Newman, Digital News Report: Overview and Key Findings of the 2018 Report, (2018), http://www.digitalnewsreport.org/survey/2018/overview-key-findings-2018/.

10 Robert Epstein & Ronald E. Robertson, *The Search Engine Manipulation Effect (SEME) and its Possible Impact on the Outcomes of Elections*, 112 Proc. Nat'l. Acad. Sci. E4512 (2015).

removing them from the scope of traditional press regulation (which would, for instance, guarantee editorial responsibility).[11]

A further way to classify the power of technology companies might be 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, its consumers.[12] Competition law intervention is, to a large extent, conditional upon the existence of market power.[13] In order to define the relevant market, a price-based substitutability test is applied that 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 in the same relevant market, and therefore exercise a competitive constraint on one another. However, if one company has — amongst other things[14] — a high market share in that market, it could be in a position of market power.

The concept of "market power" therefore gauges what constraints a platform might exercise on its competitors and its users. It suffers from two potential limitations in this context, however. First, as Pasquale suggests, competition law doctrine and scholarship often characterize scenarios as competitive "when they are experienced by consumers and users as coercive and manipulative."[15] The explanation for this is that platforms often operate in two or more related markets and competition authorities prefer to focus on the side of the market involving monetary transactions rather than on the "free" side of the market, leading to potentially counterintuitive conclusions for individuals.

Take the following as an example. Several platforms (social networking sites, search engines and e-commerce platforms) may all compete to attract advertising and therefore be treated as competitors for market definition purposes. Thus, a social networking service may be characterized as being

---

11 *See, e.g.*, Communications Decency Act 1996 47 U.S.C. § 230(c)(1) (2012) in the U.S.; Directive 2000/31/EC 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, arts. 12-15, 2000 O.J. (L 178) 1, 12-13 (EC) (In the EU).

12 Case 27/76, United Brands v. Commission, 1978 E.C.R. 207.

13 Samson Yoseph Esayas, *Competition in (Data) Privacy: "Zero"-Price Markets, Market Power, and the Role of Competition Law*, 8 Intl. Data Privacy L. 181 (2018).

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

15 Frank Pasquale, *Privacy, Antitrust and Power*, 20 Geo. Mason L. Rev. 1009, 1011 (2013).

subject to constraints from competitors when selling advertising. However, users may not benefit from this competition if they only have one choice of social networking service. An individual wishing to connect with friends and family will not view an e-commerce platform as a viable alternative to a social networking site, and therefore as a competitor.

A further explanation for this is that competition authorities face an uphill battle when trying to establish dominance or market power. While the German Bundeskartellamt's claim that Facebook has abused its monopoly power in Germany gives hope that such market power can be established, existing European jurisprudence might point in the opposite direction.[16] For instance, the European General Court noted in its *Microsoft/Skype* judgment that the consumer communications sector is fast-growing and characterized by short innovation cycles. It held that "in such a dynamic context, high market shares are not necessarily indicative of market power."[17] Indeed, proponents of Schumpeter's theory of "creative destruction" would argue that a monopoly market structure does not indicate an absence of competition, as the competitive process can also encompass dynamic competition between successive monopolies.[18] There is a strong and growing movement (the so-called "New Brandeis Movement") supporting the claim that competition law and antitrust should refocus on structures and processes of competition. However, this movement will face considerable resistance from the competition law community which may (erroneously) equate this focus on structure with the assumption that "big is bad."[19] Thus, without reform,[20] market power is a difficult concept to establish which does not necessarily reflect how digital markets are experienced by users.

---

16 Alfonso Lamadrid, *Facebook, Privacy and Article 102: A First Comment on the Budeskartellamt's Investigation*, Chilling Competition (Mar. 2, 2016), https://chillingcompetition.com/2016/03/02/facebook-privacy-and-article-102-a-first-comment-on-the-bundeskartellamts-investigation/.

17 Case T-79/12, Cisco Systems, Inc. and Messagenet SpA v. European Commission, EU:T:2013:635, para 69.

18 Joseph Coniglio, *Why the "New Brandeis Movement" Gets Antitrust Wrong*, 360 Law 1 (2018).

19 *Id.*

20 For instance, the French *Conseil National du Numerique* (CNNum) 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." Conseil National du Numerique [CNNum], Platform Neutrality: Building an Open and Sustainable Digital Environment 21 (2014).

A second limitation of "market power" is that legal mechanisms which rely on this concept as their starting point, 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.[21] As market power determines the extent to which a firm feels competitive constraints in a given market, the harms caused by market power are similarly market-orientated. Thus, EU competition law seeks to promote consumer welfare, which is enhanced when consumers receive cheaper and better-quality products as well as more choice and innovation.

This focus has been criticized by, amongst others, the New Brandeis Movement, which has suggested that a fixation on efficiency has "blinded enforcers to many of the harms caused by undue market power" and even resulted in higher prices for consumers.[22] Following sustained pressure, considerable inroads have been made in recent years to fit data protection concerns within the "consumer welfare" mold by recognizing data protection as a dimension of quality.[23] For instance, in *Microsoft/LinkedIn*, the EU Commission acknowledged that the acquisition of LinkedIn by Microsoft could marginalize competitors who offer a policy more friendly towards data protection than LinkedIn's. The Commission therefore extracted commitments from the parties to ensure this would not occur.[24] When data protection is viewed as an element of consumer welfare, then it will be weighed in the mix alongside price and other quality elements. We have yet to see a competition authority balance these facets of consumer welfare in the data protection context: where, for instance, an action leading to lower prices also led to a lower quality of data protection. Nevertheless, competition lawyers have for the most part rejected the idea that there is something distinct about personal data noting, for example, that "it is far from clear whether there is something truly unique about the digital world that warrants a fundamental rethink of the law as it stands."[25] While the law does not preclude recognising data

---

21 *Digital Single Market Strategy*, *supra* note 3.

22 Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. Eur. Competition L. Prac. 131 (2018). For an opposing perspective, see A. Douglas Melamed & Nicolas Petit, The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets (unpublished manuscript) (Oct. 3, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248140.

23 Francisco Costa-Cabral & Orla Lynskey, *Family Ties: The Intersection between Competition and Data Protection in EU Law*, 54 Common Mkt. L. Rev. 11 (2017).

24 Case No. COMP/M.8124, Microsoft/LinkedIn, C(2016) 8404 final.

25 Pablo Ibánez Colomo & Gianni De Stefano, *The Challenge of Digital Markets: First, Let Us Not Forget the Lessons Learnt Over the Years*, 9 J. Eur. Competition

protection's status of a fundamental right in this balancing exercise, it is unclear that this dignitary dimension would be given additional weight beyond price, choice and innovation factors in this context. As these two limitations indicate, while the concept of market power is relevant when considering the consolidation of data, it is not decisive, as it does not acknowledge what is distinct about data and is not equipped to tackle all data-driven harms. An analogy might be made here with the utility of market power as a measure when measuring media pluralism: in this context, experts recommend that market power indicators be combined with other indicators to determine potential risks for media pluralism.[26] These indicators include economic and sociopolitical indices, on the recognition that media pluralism is a social as well as economic concern. This Article suggests that a bespoke concept of data power could be developed which, like the media pluralism benchmark in the media context, might be of assistance when analyzing developments in data-intensive markets.

Whereas market power concerns the constraints placed on a company by its competitors and consumers on a particular market and on the economic harms that may follow from the exercise of such power, a more comprehensive conception of power is needed in order to capture adequately the power data-intensive companies wield. Data power is a multifaceted form of power available to digital platforms, arising from their control over data flows. As online platforms act as an interface between their various constituents (content providers, advertisers, individual users, etc.), 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. This gatekeeper role of digital platforms is well-documented[27] and the concepts of "platform power" and "digital dominance" have received much critical attention in recent years.[28] However, these concepts — gatekeeper, platform power, digital dominance — all suffer from a similar potential weakness: they are overly broad. In particular, they identify an infrastructure (gatekeeper; platform) or a characteristic (digital) rather than a potential regulatory challenge as a regulatory target.[29] For instance, as discussed

---

L. Prac. 1 (2018).

26 K.U. Leuven et al., Independent Study on Indicators for Media Pluralism in the Member States – Towards a Risk-Based Approach (2009).

27 Emily Laidlaw, *A Framework for Identifying Internet Information Gatekeepers*, 24 Int'l Rev. L. Computers & Tech. 263 (2010).

28 Digital Dominance: The Power of Google, Amazon, Facebook, and Apple (Martin Moore & Damian Tambini eds., 2018).

29 Lyria Bennett-Moses, *How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target*, 5 Law Innovation & Tech.

elsewhere, the term "platform power" provides little definitional clarity: on the one hand, the term "platform" is a broad one which risks bringing all two or multi-sided market structures within its scope. It is thus over-inclusive. On the other hand, the term "platform power" provides no insight into the issues that such power might pose.[30] The term "data power," by way of contrast, indicates that it is control over data that is decisive to this power and that poses potential regulatory problems. While all digital platforms have the 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: it is these companies that have "data power."

By introducing a basic (and admittedly underdeveloped) notion of "data power," this Article seeks to help reorient the discussion towards specific harms and risks outlined below. Indeed, the European Data Protection Board recently referred to the potential accumulation of significant "informational power" by companies when assessing the data protection impacts of economic concentration.[31] It is this "data power" or "informational power" which this Article seeks to probe.

Two well-known, albeit by no means exclusive, examples of firms with "data power" are Facebook and Google. A series of interconnected factors contribute to their position of power. First, they are omnipresent in the digital environment: in 2016 only two of the top 10 smartphone applications in the U.S. (based on the number of average unique users per month) were not owned by either Google or Facebook.[32] This omnipresence has been aided in part (as outlined below) by a lax *ex ante* regulatory regime for mergers and acquisitions, allowing Google and Facebook to acquire would-be competitors and innovators. While this may initially seem like a competition problem, and thus an issue of market power, it is also an issue of "data power." Such omnipresence provides access to a significant volume of user data across different applications and thus contexts. This access to a large volume and variety of data may not be relevant in a competitive context if it does not

---

1, 17 (2013).

30 Orla Lynskey, Regulating Platform Power 4-6 (LSE Working Paper No. 1/2017).

31 *European Data Protection Board Statement of the EDPB on the Data Protection Impacts of Economic Concentration* (Aug. 27, 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.

32 Sarah Perez, *Facebook & Google Dominate the List of 2016's Top Apps*, TechCrunch (Dec. 28, 2016), 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 owning three [Facebook; Facebook Messenger; Instagram]).

lead to market power, but would be relevant in establishing data power (as discussed below).

B. 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 in 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 Article, 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.[33] Profiling can be used to differentiate between consumers based on the quality or the price of goods and services offered to them.[34] 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.[35] 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.

---

33 *See, e.g.,* F.T.C. Data Brokers: A Call for Transparency and Accountability, (2014); Competition Mkt. Auth., The Commercial Use of Consumer Data: Report on the CMA's Call for Information 38 (2015) (claiming that the techniques used to profile or categorize 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).

34 The Commercial Use of Consumer Data, *supra* note 33, at 93 (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").

35 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. *See, e.g.*, Office Fair Trading, Online Targeting of Advertising and Prices (2010), http://webarchive.nationalarchives.gov.uk/20140402182803/http://oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf.

A further concern is that those with data power will go beyond registering perceptions and create them. A study of Google Search found, for instance, that there is significant discrimination in terms of the advertisement results displayed depending on the assumed race of the names searched for. In particular, Latanya Sweeney's research suggests that names linked with black people (defined by a prior study on workplace racial discrimination) were 25% more likely to return results that invited the Search user to click on a link to search criminal record history.[36] Such discriminatory delivery of advertisements risks stigmatizing black people and associating negative inferences with names linked to black people. Similarly, the suggestions offered by "autocomplete" tools by gatekeepers can influence individual perceptions For instance, there was considerable controversy in the UK when it was reported that the Google search engine failed to offer a suggested "autocomplete" search term when individuals entered the words "Conservatives are" in the search engine, yet offered several autocomplete suggestions when terms relating to rival political parties were entered into it.[37] 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.

One may legitimately query why the power to profile is highlighted here rather than, for instance, the impact that a search engine ranking can have on the visibility (and thus economic viability) of a particular business or of particular arguments that are heard, or not heard at all, due to their ranking. Indeed, such concerns about the role of intermediaries such as search engines are not new. For example, Lucas D. Introna and Helen Nissenbaum already cautioned in 2000 that search engines systematically exclude (by accident but also by design) certain sites and types of sites in favor of others.[38] Two replies might be offered in response to such objections. First, the concerns regarding data power noted here do not exclude consideration of other concerns regarding the conduct of digital platforms. Indeed, Google has recently been sanctioned by the EU Commission for the favorable positioning in Google Search of its

---

36 Latanya Sweeney, *Discrimination in Online Ad Delivery*, 11 Queue 10 (2013).

37 Media Mole, *Why doesn't Google autocomplete "Conservatives are..."?*, NewStatesmanAmerica (Feb. 3, 2016), https://www.newstatesman.com/politics/media/2016/02/why-doesn-t-google-autocomplete-conservatives-are.

38 Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 Info. Soc'y 169 (2000).

own comparison shopping service over that of its competitors.[39] Regulators are still grappling with the impact of ranking and filtering on freedom of expression, leading to the second reply: although these concerns have been long noted, we have yet to see additional regulatory obligations imposed on relevant intermediaries as a result of their power. This issue has become more pressing for several reasons: the number of users of these services has rocketed; control over various layers of the Internet infrastructure is more consolidated, placing more data and thus power in the hands of fewer actors; and the data enables a level of personalization (and manipulation) that was previously not possible.

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. The following Part 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.

II. The Normative Foundations for Regulating "Data Power" in Privacy and Data Protection Law

A. Insights from the Right to Respect for Private Life

Pursuant to the case law on Article 8 of the European Convention on Human Rights (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 emphasized that an individual does not waive his or her rights by engaging in public activities that are subsequently documented.[40] 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.[41] 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,

---

39 Commission Decision No. AT.39740 Google Search (Shopping) of 27 June 2017, 2017 O.J. (C 4444).

40 Rotaru v. Romania, App. No. 28341/95, Eur. Ct. H.R. (2000).

41 Amann v. Switzerland, App No. 27798/95, 843 Eur. Ct. H.R. (2000).

interfere with the right to private life. This is because personal data reveals more than the sum of its parts. By combining 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.[42] 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."[43] Indeed, this is why one of the critical "v's" in the five v's often discussed in the Big Data context — alongside volume, value, velocity and veracity — 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 behavior. 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 preexisting 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 behavior of others in circumstances where the state has limited capacity to do the same.[44] 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.

---

42 Joined Cases C-293/12 & C-594/12 Dig. Rights Ireland Ltd. v. Minister Commc'n, Marine and Nat. Res. and Others & Kärntner Landesregierung and Others, 2014 E.C.R. 238.

43 *Id.* at 37.

44 Laidlaw, *supra* note 27, at 265 (2010).

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, the State has a positive duty to take concrete steps in order to guarantee fundamental rights.[45] Such a positive duty to protect the fundamental right to respect for private life has been recognized by the Court in its jurisprudence.[46] Therefore, it can be said that the ECHR rights not only secure protection *against* the State but also protection *by* the State.[47] 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."[48] According to Eleni 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 they possess constitutionally."[49]

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. Second, 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

---

45 *See* Airey v. Ireland, App. No. 6289/73, 2 Eur. Ct. H.R. 305, ¶ 32 (1979) (an early example).

46 X & Y v. Netherlands, App. No. 8978/80, 8 Eur. Ct. H.R. 235 (1985).

47 Andrew Clapham, *The "Drittwirkung" of the Convention, in* The European System for the Protection of Human Rights 163, 190 (Ronald St. J. McDonald, Franz Matscher, & Herbert Petzold eds., 1993).

48 Andrew Clapham, Human Rights Obligations of Non-State Actors 438 (2006).

49 Eleni Frantziou, *The Horizontal Effect of the Charter of Fundamental Rights of the European Union: Rediscovering the Reasons for Horizontality*, 21 Eur. L.J. 657, 674 (2015).

whose interests do not necessarily encompass the general interest."[50] 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 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 recognizing that such factors are relevant when determining the nature and extent of data protection obligations.

B. 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."[51] 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 the 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.[52] 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.[53] Thus, although the household

---

50 CNNUM, *supra* note 20, at 15.

51 GDPR, *supra* note 8, at art. 4(7).

52 *Id.* at art. 2(2)(c).

53 Case C-101/01, Bodil Lindqvist, 2003 E.C.R I-12971, ¶ 47.

exemption does not look at the volume of the data processed as such, it does consider the reach of the data-processing activity (and in Mrs Lindqvist's case, the fact that it was made available to an indefinite number was critical).

The Court has more recently confirmed its restrictive interpretation of this provision in *Ryneš*,[54] 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 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.[55] 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.[56] It therefore emphasized 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.[57]

Lindqvist and *Ryneš* give the impression that the scale of personal data processing, or the reach of the data controller, is irrelevant for the purposes of the data protection regime. However, it is suggested that this impression is erroneous, as the Court's judgment in *Google Spain* illustrates.[58] In that case, the Court emphasized that the personal data processing by search engines is distinct from that conducted by publisher websites[59] 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

54 Case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, EU:C:2014:2428.

55 Case C-212/13 František Ryneš v. Úřad pro ochranu osobních údajů, EU:C:2014:2072, ¶ 43 (Opinion of the Advocate General).

56 *Id.* at ¶ 29.

57 *Id.* at ¶¶ 30, 33.

58 Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C:2014:317.

59 *Id.* at ¶ 36.

of his private life and which, without the search engine, could not have been interconnected or could have been interconnected only with great difficulty."[60] It also emphasized 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."[61] It can therefore be concluded that in determining the nature and extent of the interference with a fundamental right, the Court emphasizes the interconnected nature of Google's data — a factor determined by the scale of its processing operations — and the ubiquity of Google,.

C. 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).[62] 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,[63] when further specifying certain aspects relating to the information to be provided to the data subject,[64] and as regards the responsibility of the data controller to ensure and to demonstrate that personal data processing is compliant with the Regulation.[65] The Commission had also proposed some leniency when it came to sanctioning an SME for a "first and non-intentional" breach of the GDPR, provided that the personal data processing was only ancillary to its main activity.[66] SMEs were also exempt

---

60 *Id.* at ¶ 80.

61 *Id.*

62 *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 [hereinafter *Regulation Proposal*] (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").

63 *Id.* at art. 12(6).

64 *Id.* at art. 14(7).

65 *Id.* at art. 22(4).

66 *Id.* at art. 79(3)(b).

from the obligation to designate a data protection officer[67] and to maintain documentation of all processing operations,[68] provided that the personal data processing is an activity ancillary to their main activities.[69]

These exemptions for SMEs were motivated by a desire to reduce the regulatory burden on SMEs[70] 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's 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 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 cognizant of this criticism and had attempted to mitigate its formalistic effects,[71] 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.[72] 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 that process data relating to more than 5,000 data subjects in any

---

67 *Id.* at art. 35(1)(b).

68 *Id.* at art. 28(4).

69 *Id.* at art. 25(2)(b) (exempting third-country SMEs from the obligation to designate a representative in the Union).

70 *Id.* (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."). *See* European Commission Press Release MEMO/14/186, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014).

71 *Regulation Proposal*, *supra* note 62, at art. 35(1)(c) (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.").

72 *Contra* GDPR, *supra* note 8, at art. 92 (Recital 167 specifies that in exercising its implementing powers, the Commission "should consider specific measures for micro, small and medium-sized enterprises." This is to show that not all references to SMEs have been removed from the text of the GDPR).

consecutive 12 month period should be obliged to hire a data protection officer.[73] 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."[74] Therefore, some references to scale do remain in the GDPR. Nevertheless, for the most part, the emphasis on size was replaced by an emphasis on "risk" in the final text of the Regulation. While some authors[75] and the Article 29 Working Party[76] assert that the data protection regime has always been a framework designed to regulate risk, the emphasis on risk in the Data Protection Directive[77] and in the jurisprudence of the Court[78] is subtle. In 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 as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons."[79] 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

---

73 *Regulation Proposal*, *supra* note 62, at art. 35(1)(b).

74 GDPR, *supra* note 8, at art. 37(1)(b).

75 *See, e.g.*, Raphaël Gellert, *Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative*, 5 Int'l Data Privacy L. 3 (2015).

76 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." *Article 29 Data Protection Working Party Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks*, 2, WP 218 (May 30, 2014).

77 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31. For instance, art. 8 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.

78 *See, e.g.*, Case C-342/12, Worten — Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), EU:C:2013:355, ¶ 24 (recalling 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").

79 GDPR, *supra* note 8, at art. 24(1).

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.[80]

Although the GDPR focuses on the level of risk that a given processing operation may entail, rather than on the size of the entity or the quantity or scale of the personal data processing, 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 Peter 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."[81]

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, 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 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 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 dataset. 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. This ubiquity meant that the harm suffered by Mr Costeja Gonzalez was prima facie greater than that which he would have suffered had Google been a less significant internet actor. For instance, one could argue that the harm suffered by an individual would be greater when her name is entered into Google Search than into DuckDuckGo given the significantly higher number of users of the former. Thus, Google's

---

80 *Id.* at recital 60.

81 Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46 EC and the Proposed General Data Protection Regulation*, *in* New Technologies and EU Law 123, 159-60 (Marise Cremoona ed., 2017).

ubiquity is not relevant solely in terms of its exposure to litigation, but also because its reach is directly relevant to the detriment it can cause those whose data it processes.

We can therefore conclude that although EU data protection law is ostensibly ambivalent towards data power, it in fact provides a clear normative nudge that such power merits particular attention.

III. Tackling "Data Power"

If the normative nudge from data protection and privacy law is accepted and we recognize 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 multidisciplinary scholarship by those concerned with the rise of data power.

A. Enhancing the Effectiveness of Data Protection Legislation

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. However, 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 emphasizes individual control over personal data by granting the individual "micro-rights," such as the right to data access, the right to delete or the right to data portability, which

she ought to exercise.[82] Yet it is increasingly recognized 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.[83] 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 they lack control over this data and express their concern about this.[84] 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.[85] Most obviously, it provides for enhanced administrative sanctions for breach of its provisions.[86] However, it also strengthens the hand of the individual *vis-à-vis* platforms/data collectors 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 of the GDPR, entitled "representation of data subjects," is perhaps of most significance. This provision enables collective actors to exercise the individuals'

---

82 Christophe Lazaro & Daniel Le Métayer, *Control over Personal Data: True Remedy or Fairy Tale*, 12 SCRIPTED 3 (2015).

83 *See* Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019).

84 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. *Special Eurobarometer 431: Data Protection — Summary*, at 4 (June 2015), http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf.

85 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. *See* GDPR, *supra* note 8, at arts. 51-59 (Independent Supervisory Authorities), 60-76 (Cooperation and Consistency), 77-84 (Remedies, Liability and Penalties).

86 *Id.* at arts. 83, 84.

right to an effective remedy and to complain to a data protection authority (DPA), provided that the individual mandates them to do so. Furthermore, Article 80(2) allows Member States the possibility of introducing measures enabling representative actors to lodge a complaint before a DPA or to have an effective remedy against a DPA or data controller, 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.

B. Data as a "Common Good" and Technology Companies as "Public Utilities"

This way of tackling data power will take us on two separate courses. The first will demonstrate what possible implications there may be to considering technology companies as public utilities. A public utility is understood here as a business that furnishes an everyday necessity to the public at large. The second will discuss the possible implications of treating the data itself as a limited form of common good, the protection of which is of societal value irrespective of individual preferences. I will discuss what possible questions we might be facing by choosing either one of them.

A radical response to the presence of 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."[87] This resolution fell on deaf ears. While unbundling via regulation in the EU has previously occurred in many 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 for dealing with such problems as and when they arise.[88] As Commissioner Oettinger put it, breaking

---

87 European Parliament Resolution of 27 November 2014 on Supporting Consumer Rights in the Digital Single Market, 2014/2973 (RSP), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2014-0071+0+DOC+PDF+V0//EN.

88 For instance, the "Third Energy Package," consisting of two Directives and three Regulations providing for ownership unbundling, was adopted by the EU in 2009. See, inter alia, Directive 2009/72, of the European Parliament and of the Council of 13 July 2009 Concerning Common Rules for the Internal Market

up and expropriation are "instruments of the planned economy, not the market economy."[89] Even if this option had more political support, it would pose 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," and the "The Frightful Five." She suggests that conceiving of them as such makes their threat and influence overwhelming and masks the distinctiveness of their business models and practices.[90] Second, the purposes of this unbundling need to be defined. As Lyria 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."[91] 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.

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. However, 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

---

in Electricity and Repealing Directive 2003/54/EC (Text with EEA relevance), 2009 O.J. (L 211) 55.

89 This statement was made to a member of the German media and later reported more widely. Samuel Gibbs, *Does Europe have the Power to Break up Facebook*, The Guardian (Nov. 26, 2014), https://www.theguardian.com/technology/2014/nov/26/does-europe-have-the-power-to-break-up-google.

90 Amanda Lotz, "*Big Tech" isn't One Big Monopoly: It's 5 Companies all in Different Businesses*, Inforrm's Blog (Apr. 1, 2018), https://inforrm.org/2018/04/01/big-tech-isnt-one-big-monopoly-its-5-companies-all-in-different-businesses-amanda-lotz/.

91 Lyria Bennett Moses, *supra* note 29, at 17.

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 the disadvantages of such consolidation outweigh the advantages, is therefore a formidable challenge.

The second question relates to the role, if any, that 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).[92] Therefore, direct network effects might be experienced in the context of a social networking service where the more individuals avail themselves 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 themselves of a search engine service like Google's 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 monetize 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.[93] The presence of network effects might point to the conclusion that the markets concerned are "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.[94] 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 David Evans and Richard Schmalense, it is "naïve armchair economics" to suggest that personal data is an indispensable

---

92 Colin Blackman & Romain Bosc, What is a Platform and Should They Be Regulated? Summary Report (Nov. 17, 2015) (unpublished manuscript), https://www.ceps.eu/sites/default/files/CEPS%20What%20is%20a%20platform_summary%20report.pdf.

93 Perez, *supra* note 32.

94 *See, e.g.*, Autorité de la Concurrence & Bundeskartellamt, Competition Law and Data (2016), http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

input for competition (and therefore the lack thereof is a barrier to entry).[95] Similarly, Google's chief economist Hal Varian indicates that the quantity of data held by a company is never decisive; rather, it is the knowledge that they have accumulated that is the fundamental source of competitive advantage in online industries.[96] 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.[97]

Regulators deciding to act in this field are faced with a complex task. For instance, they will need to tackle the so-called Collingridge dilemma, or pacing problem: If regulators intervene too early, regulation might be preemptive 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 be regulated effectively.[98] As the *CNNum* points out, timing 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."[99] Kevin Coates refers to this as the "Goldilocks" problem, adding a third hurdle based on Joseph A. Schumpter's "creative destruction"[100]: "even when the porridge is just right, you still should not eat the porridge because

---

95 David S. Evans & Richard Schmalensee, *Network Effects: March to the Evidence, Not to the Slogans*, CPI Antitrust Chronicle (Sept. 15, 2017), https://www.competitionpolicyinternational.com/network-effects-march-to-the-evidence-not-to-the-slogans-2/.

96 Hal R. Varian, Use and Abuse of Network Effects, (Aug. 7, 2018) (unpublished manuscript), https://ssrn.com/abstract=3215488.

97 Pasquale, *supra* note 15, at 1023.

98 Bennett Moses, *supra* note 29, at 7.

99 CNNum, *supra* note 20, at 20.

100 Joseph A. Schumpeter, Capitalism, Socialism & Democracy (1942).

something even better than porridge will come along soon."[101] This belief that the current market players holding vast treasure troves of data will no longer be on the scene in the medium-term can lead to regulatory paralysis, with regulators holding off for the new wave of creative destruction to rectify any problems posed by data aggregation.

Third, 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," instead of 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? Second, the externalities of such data duplication need to be considered: such a solution may be suboptimal — or even counterproductive — 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.

C. Preventing the Artificial Aggregation of Data

A third response to data power, in keeping with the efforts of the "New Brandeis School" to enlist antitrust to tackle informational capitalism,[102] 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: already in 2011 Google confirmed that it was acquiring, on average, one company per week.[103] While Facebook's Mark Zuckerberg stated in 2010 that the company's acquisitions were "talent acquisitions," motivated by the desire to 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

---

101 Kevin Coates, *An Emerging Competition Law for a New Economy? Introductory Remarks for the Chillin Competition Panel*, 21st Century Competition: Reflections Modern Antitrust (Jan. 21, 2016), http://www.twentyfirstcenturycompetition.com/2016/01/an-emerging-competition-law-for-a-new-economy-introductory-remarks-for-the-chillin-competition-panel/.

102 Lina Khan, *Amazon's Antitrust Paradox*, 126 Yale L.J. 710 (2017).

103 Leena Rao, *Eric Schmidt: Google is Buying One Company a Week*", TechCrunch (Dec. 7, 2011), https://techcrunch.com/2011/12/07/eric-schmidt-google-is-buying-one-company-a-week/.

for USD$19 billion, having obtained clearance for the transaction from both the U.S. 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 in 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. It therefore concluded that the transaction would not have a negative impact on competition in the advertising market. 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 (*i.e.*, privacy was not an important factor in the decision to use these applications).[104]

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."[105] Second, 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

---

104 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 behavioral advertising). Maurice E. Stucke & Allen P. Grunes, Big Data and Competition Policy 131-32 (2016).

105 Case No. COMP/M.7217, Facebook/ WhatsApp, 2014 O.J. (C 417) 164.

of Facebook and 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.[106]

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 from a competition law perspective, given that Google did not compete with any of the companies it was acquiring. Moreover, even had the authorities considered that there was competition for data, they would likely have concluded, as they did in Facebook/WhatsApp, that data is in such abundant supply in secondary markets that this would not pose a competitive problem. 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, argue 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.[107] If this data sharing does not have the object or effect of restricting competition, it would not breach competition law. 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 aggravate 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

106 Case No. COMP/M.8228, Facebook/ WhatsApp, 2017 O.J. (C 286).

107 Maureen Ohlhausen & Alexander Okuliar, *Competition, Consumer Protection, and the Right (Approach) to Privacy*, 80 Antitrust L.J. 121, 132 (2015).

Deepmind's part to separate this data from that held by its parent company.[108] 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 noneconomic impact on individuals. This situation could be rectified if competition authorities would themselves reconsider how they analyze such data-driven mergers and agreements or, preferably, if economic transactions could be subject to a parallel noncompetition analysis in order to examine their broader societal impact. This would go against the grain, as "public interest" considerations in merger proceedings have becoming increasingly marginalized in many jurisdictions.[109] 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 noncompetition grounds. This power is provided for by Article 21(4) of the EUMR, which states that "[m]ember 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."[110] Member States may then prohibit the merger provided that this action is proportionate and

---

108 Julia Powles & Hal Hodson, *Google DeepMind and healthcare in an age of algorithms*, 7 Health & Tech. 351 (2017).

109 Int'l Competition Network Advocacy Working Grp., Competition Culture Project Report 10 (2015).

110 Council Regulation (EC) No. 139/2004 of 20 January 2004 on the Control of Concentrations Between Undertakings, art. 21(4), 2004 O.J. (L 24) 1, 17. 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.

nondiscriminatory. This provision does not therefore, as Jones and Davies observe, confer new 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."[111]

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 noncompetition analysis, with a negative impact on media plurality treated as a separate rationale for market intervention.[112] Data-driven mergers that may enhance data power could therefore similarly be subject to a noncompetition assessment running in parallel to the competitive assessment, an option hinted at by the European Data Protection Board in its statement on economic concentration.

Such a regulatory response does, however, beg a number of questions 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 supports 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.[113] 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 be weighed against increased efficiency?

---

111 Alison Jones & John Davies, *Merger Control and the Public Interest: Balancing EU and National Law in the Protectionist Debate*, 10 Eur. Competition J. 453, 488 (2014).

112 For a discussion of how this operates in the UK, see Rachael Craufurd Smith & Damian Tambini, *Measuring Media Plurality in the United Kingdom: Policy Choices and Regulatory Challenges*, 4 J. Media L. 35 (2012).

113 For further information and access to the 2016 report, see Ctr. Media Pluralism Media Freedom, Monitoring Media Pluralism in Europe: Application of the Media Pluralism Monitor 2016 in the European Union, Montenegro and Turkey. http://cmpf.eui.eu/download/621/?uid=cd83592de0 (2017).

Such incommensurability abounds even within the "objective" economics-based framework of competition law.

Conclusion

As the French 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 recent events have illustrated that current practices do not make it possible to reach these goals.[114] 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 minimization and disaggregation and their attempts to curtail the implications of power for individuals, provide a solid normative foundation for such additional measures. The challenge is, however, to identify practical regulatory responses to such data power. This Article has identified three potential options that have been mooted to tackle such data power: namely, to move to a more vigorous enforcement of data protection law (a process already afoot under the GDPR); to treat data as a common good and/or technology giants as public utilities; and to limit artificial data aggregation through data-driven mergers.

114 CNNum, *supra* note 20, at 6.