THE INTERSECTION BETWEEN DATA PROTECTION AND COMPETITION LAW: HOW TO INCORPORATE DATA PROTECTION, AS A NON-ECONOMIC OBJECTIVE, INTO EU COMPETITION ANALYSIS

LOUISE O'CALLAGHAN*

Introduction

The digital economy is marked by the exponential growth in the collection of personal data which is analysed and exploited by businesses for commercial purposes. While companies encourage the perception that their online services are provided free of charge, in reality there is 'no such thing as a free search'.[1] Individuals who use online services are in fact surrendering their personal data as an extremely valuable form of payment to companies.

By the employment of a two-sided business model,[2] companies monetise personal data by exploiting indirect network effects. On the one side they offer free services to attract as many users as possible and, on the other side, they sell user data to advertisers. The more details a service provider can collect about its users, the more precise information it can sell to its advertisers. This benefits advertisers who can then better target their advertising.[3] Therefore, it is no wonder that personal data has been coined the 'new currency'[4] for the digital economy. However, while personal data is of economic value, it also encompasses intrinsic privacy concerns for individuals.

* LLB and Scholar, Trinity College Dublin, LLM, Leiden University. The author would like to thank Dr. Ben Van Rompuy, Leiden University, and Nina Milosavljevic for their helpful comments and suggestions on an earlier draft of this article.

[1] Alec J Burnside, 'No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals' (2015) CPI Antitrust Chronicle, May 2015, 2.

[2] A two-sided business model is a platform which connects two distinct groups of users seeking a mutual benefit, thus permitting both bodies of customers to obtain value from one another – Aleksandra Gebicka and Andreas Heinemann, 'Social Media & Competition Law' (2014) 37(2) World Competition 149, 154.

[3] Inge Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38(4) World Competition 473, 473.

[4] Commissioner Vestager, 'Competition in a big data world', 17 January 2016, <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en> accessed 11 February 2018.

While Mark Zuckerberg is quoted as saying that privacy is 'no longer a social norm,'[5] the ubiquitous nature of information sharing has raised concerns over the acquisition and processing of personal data by large companies. These concerns are bolstered by the existence of significant information and power asymmetries between users and service providers in that consumers are largely unaware of the information being collected about them and how this information is subsequently being used. In reaction to mounting concern, it has been suggested that the data protection framework is inadequate to address the privacy concerns arising in the digital market.

Although, the General Data Protection Regulation (GDPR)[6] seeks to address the challenges of the evolving digital economy, it remains focused on the notion of individual control. However, due to the concentrated nature of online markets, the fostering of individual control is considered to be inadequate to ensure the effectiveness of data protection, as ultimately, consumers have little or no choice.[7] Thus, advocates contend that in order to ensure the effectiveness of data protection in the digital market a holistic approach should be adopted with competition enforcement taking privacy considerations into account.[8] This article focuses on this proposition for a holistic approach, as it is examined whether there is a legal basis within the EU legal order by which data protection concerns could be incorporated into competition policy.

I. Data Protection and Competition Law

The proposition that data protection concerns should be taken into account in the application of competition law has not been unanimously welcomed. On the one hand, those advocating for the incorporation of data protection into competition law focus on the common objectives which exist between the two fields in order to advance the opinion that the policies should be applied in a holistic manner.[9] These common objectives are identified as seeking to protect

[5] The Guardian, 'Privacy is no longer a social norm, says Facebook founder' <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 11 February 2018.

[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 [2016] OJ L119/1.

[7] Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4(4) IDPL 250, 251.

[8] European Data Protection Supervisor (EDPS), Preliminary Opinion, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014.

[9] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersections Between Data Protection and Competition Law in EU Law' (2017) 54 Common Market Law Review 11; Inge Graef, 'Blurring boundaries of consumer welfare, how to create synergies between competition, consumer and data protection law in digital markets' (2016)

individuals and tackling power asymmetries. Firstly, in relation to the protection of individuals, the 'basic assumption' of competition law is that a competitive market enhances consumer welfare. In terms of data protection, data subjects, also being consumers, are the direct beneficiaries of the data protection framework.[10] Secondly, in relation to power asymmetries, competition law seeks to protect consumers against undertakings' market power while data protection seeks to protect the individual within the data processing cycle.[11] These common objectives are highlighted in order to demonstrate that data protection and competition law share the same underlying normative concerns which therefore justifies integrated enforcement.

On the other hand, those against the incorporation of data protection concerns into competition analysis predominantly address the issue from the perspective of institutional choice.[12] From this perspective, it is contended that competition law is focused on economic efficiency and if used to remedy normative concerns about privacy, its specialised nature would be contradicted and it would be at risk of being distorted.[13] This adheres to the view that the role of competition law is maintaining an environment within which products may compete, and not addressing non-efficiency goals such as privacy concerns. In the same vein, it is contended that the inclusion of privacy considerations into competition analysis would open the floodgates for other fundamental rights or public policy goals. In the words of Lamadrid and Villiers, this would have the result of turning competition law into 'a law of everything, which would not only entirely deform the discipline but would also provide a great starting point for a dystopian novel'.[14]

However, if it is established that there is a legal basis for incorporating data protection concerns into competition analysis, it is disputed that any obligation conferred by such a legal basis could be overridden by the fact that

---

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881969> accessed 11 February 2018; EDPS (n 8).

[10] Costa-Cabral and Lynskey (n 9), 21.

[11] ibid 21.

[12] See D Daniel Sokol and Roisin E Comerford, 'Antitrust and Regulating Big Data' (2016) 23 Geo Mason L Rev 1129; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) Antitrust L J 121; Alfonso Lamadrid, 'On Privacy, Big Data and Competition Law (2/2) On the nature, goals, means and limitations of competition law' (June 2014) <https://chillingcompetition.com/2014/06/06/on-privacy-big-data-and-competition-law-22-on-the-nature-goals-means-and-limitations-of-competition-law/> accessed 11 February 2018.

[13] Ohlhausen and Okuliar (n 12), 152-153.

[14] Alfonso Lamadrid and Sam Villiers, 'Big Data, Privacy and Competition Law: Do Competition Authorities Know How To Do It?' CPI Antitrust Chronicle, January 2017, 4.

this might result in the incorporation of other fundamental rights or public policy goals.[15]

Moreover, any obligation established is not suggesting that the Directorate General ('DG') Competition should pursue data protection infringements as competition law infringements due to the mere fact of there being either an agreement, an undertaking in a dominant position, or a concentration. Any obligation to take data protection issues into account is constrained by the principle of legality which prevents the Commission from using its powers to consider data protection concerns in the absence of a competition law infringement.

However, the proposition for such a holistic approach has not been well received by either the Court of Justice ('the Court') in Luxembourg or in the practice of the European Commission ('the Commission'). In fact, both EU case law and the Commission's decisional practice abide by the view that there is a strict delineation between the data protection and competition frameworks and concerns regarding data protection are excluded from the application of competition law.

In 2006, in *Asnef-Equifax*,[16] the Court established that 'any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection.'[17] This was affirmed by the Commission in the *Google/DoubleClick*[18] and again in *Facebook/WhatsApp,*[19] when the Commission stated that 'any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.'[20] This was again reiterated in *Microsoft/LinkedIn*[21] where the Commission proceeded by discussing the competition issues raised by the transaction 'assuming such data combination is allowed under the applicable data protection legislation.'[22]

Notably, the Commission has acknowledged that consumers may see privacy as a significant factor affecting the quality of goods and that privacy may constitute a competitive lever where firms compete in providing more or less privacy-friendly products and services.[23] However, it must be borne in

[15] Costra-Cabral and Lynskey (n 9) 48.
[16] Case C-238/05, *Asnef-Equifax*, EU:C:2006:734.
[17] ibid [63].
[18] Case COMP/M.4731, *Google/Double/Click* (2008).
[19] Case COMP/M.7217, *Facebook/WhatsApp* (2014).
[20] ibid [164].
[21] Case COMP/M.8124, *Microsoft/LinkedIn* (2016).
[22] ibid [179].
[23] *Facebook/WhatsApp* (n 19) [87]; *Microsoft/LinkedIn* (n 21) [330].

mind that this is purely a theoretical scenario since, to date, privacy has not emerged in practice as a parameter of competition.[24]

Against this backdrop, this article examines whether there is a legal basis according to which data protection, as a non-economic objective, could be incorporated into competition law. By looking at the current legal framework governing EU competition policy, three such gateways have been identified: the Treaty on the Functioning of the European Union ('the TFEU'),[25] the Charter of Fundamental Rights ('the Charter'),[26] and Article 21(4) of Regulation No. 139/2004 ('the EUMR').[27]

This article contends that within each of these gateways there is scope to incorporate data protection concerns into competition analysis. Firstly, it will be established that upon a holistic reading of the TFEU, competition law cannot be taken as an isolated policy and therefore has to take other EU objectives into consideration, including data protection concerns. Secondly, it will be contended that as the right to data protection is enshrined in the Charter, the Commission is obliged to respect that right. Finally, it will be established that there is potential scope for data protection to constitute a notifiable public interest under Article 21(4) EUMR.

II. The TFEU

The EU competition provisions are found within the TFEU, as opposed to being contained in competition-specific legislation. This holds particular importance as it means that the provisions are not aimed at isolated goals, but form part of a web of inter-related Treaty articles.[28] Therefore, the structure of the EU Treaties demands consideration of non-economic goals in competition policy as, upon a holistic reading of the Treaty, it is impossible to exclude such concerns.[29] In this regard, there are two provisions within the TFEU by which data protection, as a non-economic goal, could be integrated into competition analysis, namely Article 12 or 16 TFEU.

Article 12 TFEU provides that '[c]onsumer protection requirements shall be taken into account in defining and implementing other Union policies and

---

[24] Autorité de la concurrence and Bundeskartellamt, 'Competition Law and Data', 10 May 2016, 25 <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> accessed 11 February 2018.

[25] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/47.

[26] Charter of Fundamental Rights of the European Union [2016] OJ C202/389.

[27] Regulation (EC) 139/2004 of 20 January 2004 on the control of concentrations between undertakings [2004] OJ L24/1.

[28] Townley, *Article 81 EC and Public Policy* (Hart Publishing 2009), 48.

[29] ibid 50; for contrary view see Okeoghene Odudu 'The Wider Concerns of Competition Law' (2010) 30(3) Oxf J Leg Stud 599.

activities.' While Article 16 TFEU provides that '[e]veryone has the right to the protection of personal data concerning them.'

Starting from the premise that the competition provisions cannot be read in isolation, it will be examined whether either of the aforementioned articles could be invoked as a legal basis for incorporating data protection considerations into competition policy.

A. Article 12 TFEU

Article 12 TFEU is one of the numerous policy-linking clauses provided for in the TFEU,[30] which require the EU institutions either to take into account, or integrate, policy interests in other EU policies. Competition law is not immune from this obligation, and the Commission and the Court have recognised the impact of these policy-linking clauses. For example, in *Association belge*, in which the Court considered the standing of a consumer association to challenge a merger decision, the Court explicitly noted the requirement to take consumer protection requirements into account when implementing competition policy in accordance with Article 12 TFEU.[31]

Parallels can be drawn between consumer protection and data protection. Firstly, in relation to their common aim of advancing consumer welfare, consumer protection aims to empower consumers and protect their interests. Similarly, as already recognised, data protection enhances consumer welfare as data subjects, also being consumers, are the direct beneficiaries of the data protection framework. Secondly, the notion of fairness is common to both.[32] Fairness is one of the most fundamental criteria for lawful trading practices in consumer law and, in Article 5(1)(a) of the GDPR, fairness is established as a core principle of data processing.

i. Scope of Consumer Protection

The consumer interests protected by Article 12 TFEU are those that fall within the scope of the stipulated interests in Article 169 TFEU.[33] Article 169 TFEU defines the specific objectives of consumer protection as the protection of health, safety and the economic interests of consumers and the promotion of

[30] See environmental protection (Article 11 TFEU), equality between men and women (Article 8 TFEU), discrimination (Article 10 TFEU), consumer protection (Article 12 TFEU), animal welfare (Article 13 TFEU), employment, social protection, and exclusion (Articles 9 and 147(2) TFEU), culture (Article 167(4) TFEU), public health (Article 168(1) TFEU), industrial policy (Article 173(3) TFEU), regional policy (Article 175 TFEU) and development cooperation (Article 208(1) TFEU).
[31] Case T-224/10, *Association belge des consommateurs test-achats ASBL*, EU:T:2011:588, [43].
[32] European Data Protection Supervisor (EDPS), Opinion 8/2016, EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, September 2016, 8.
[33] Geiger, Khan, and Kotzur (eds), *European Union Treaties - A Commentary* (Hart 2015) 224.

the right to consumer information, education and the formation of consumer interest groups.[34]

While the TFEU does not contain any explicit definition of the term 'consumer', the notion has been defined as a natural person acting on the market for his or her personal, private but not commercial purpose.[35] A 'data subject' is a natural person identified or identifiable by personal data.[36] As already noted, the use of online services is not free, rather individuals surrender their personal data in exchange for such services, with the result that their personal data is conferred an economic value. Article 169(1) TFEU encompasses protection for consumers' economic interests. Therefore, if a data subject is also a consumer, and it is the personal data that carries the economic value, then privacy concerns, which are an intrinsic element of personal data, could fall within the scope of 'economic interests' protected under Article 169(1) TFEU.

ii. Duty to Take Consumer Protection Requirements into Account

If accepting that data protection and privacy concerns fall within the scope of consumer protection and thus within Article 12 TFEU, it is necessary to consider the impact of the duty to take consumer protection requirements into account on competition analysis. What weight do consumer protection requirements demand in practice? Does Article 12 TFEU impose a limited obligation, which is easily satisfied by a superficial examination of consumer protection requirements or does it require a more stringent consideration of such matters?

While all of the policy-linking clauses demand some form of integration, the exact wording of each is different with the result that, in terms of legal force, some are more powerful than others. Article 12 TFEU calls for consumer protection requirements to be taken into account. The legal force attached to this duty is ambiguous. Weatherill is unconvinced that Article 12 TFEU could prove to be an influential tool. In relation to its legal force, it is commented that Article 12's policy-framing character makes it an inadequate basis for judicial review of the substance of measures.[37] Moreover, it is submitted that the provision is deficient in both legal precision and institutional specificity and leans more towards political aspiration than constituting an independently enforceable legal norm.[38]

---

[34] Article 169 TFEU.
[35] Geiger, Khan, and Kotzur (n 33), 223-224.
[36] Article 4(1) GDPR.
[37] Weatherill, *EU Consumer Law and Policy* (Edward Elgar Publishing 2013), 16.
[38] ibid 72.

The only competition case in which Article 12 TFEU has been explicitly referred to is *Association belge*. Unfortunately, the reliance on Article 12 TFEU in the judgment offers little guidance on the strength of the obligation. The Court merely referenced Article 12 TFEU to buttress the argument that Article 11(c), second indent, of Regulation No. 802/2004[39] concerning mergers, cannot be interpreted in restrictive terms,[40] and did not consider the Article in substantive terms.

In terms of legal force, the case law concerning Article 167(4) TFEU and cultural diversity is instructive as it provides for an identical obligation to that found in Article 12 TFEU: '[t]he Union shall take cultural aspects into account in its action under other provisions of this Treaty'. In *Stim v Commission*,[41] the Court reviewed the Commission's decision in *CISAC*[42] in which the Commission was faced with the claim that an anticompetitive agreement should be exempted for reasons of cultural protection. In *CISAC*, the Commission had explicitly carried out an assessment of the case from the perspective of cultural diversity in accordance with Article 167(4) TFEU and had concluded that the decision did not harm cultural diversity.[43] The Court concluded that the applicants had not demonstrated to the requisite legal standard that the Commission had failed to take the protection of cultural diversity into account. However, the Court did not enunciate what such a requisite legal standard might require.

Unfortunately, neither *Association belge* in relation to Article 12 TFEU nor *Stim* in relation to Article 167(4) address the situation where requirements of consumer protection/cultural diversity conflict with competition concerns. Therefore, neither judgment offers any instruction on how the two interests would be balanced. In this situation, prioritisation is inevitable and it is doubtful that the obligation in Article 12 TFEU is sufficiently strong to enable consumer protection requirements to trump competition considerations.[44]

Ultimately, the obligation contained in Article 12 TFEU does not appear to be particularly instrumental, with consensus being that the obligation is merely formal, most likely amounting to a duty to state the reasons, why and how, or why not, the interests of consumers were or were not taken into account.[45] Therefore, while Article 12 TFEU does provide a legal basis by

[39] Regulation (EC) 802/2004 of 7 April 2004 implementing Council Regulation (EC) 139/2004 on the control of concentrations between undertakings [2004] OJ L133/1.
[40] *Association belge* (n 31), [43].
[41] Case T-451/08, *Stim v Commission*, EU:T:2013:189.
[42] Case COMP/C2/38.698, *CISAC* (2008).
[43] ibid [93-9].
[44] Jules Stuyck, 'European Consumer Law after the Treaty of Amsterdam: consumer policy in or beyond the internal market' (2000) 37(2) Common Mark Law Rev 367, 386.
[45] ibid 386.

which data protection concerns could be taken into account, the strength of the obligation is ambiguous and thus undermines its effectiveness.

B. Article 16 TFEU

The wording of Article 16 TFEU is undisputedly different from that of Article 12 TFEU. Article 16 TFEU does not contain integrationist language, but simply affirms that 'everyone has the right to the protection of personal data concerning them.' Article 16 TFEU consists of an affirmation of a right as opposed to a mandate to take data protection concerns into account. Therefore, data protection concerns cannot be incorporated into competition analysis by virtue of Article 16 TFEU alone.

However, it remains to be considered whether Article 16 TFEU, read in conjunction with Article 7 TFEU, which mandates for consistency between the EU's policies and activities, could provide a legal basis for consideration of data protection concerns within competition law.

i. Article 7 TFEU and the Principle of Consistency

Article 7 TFEU stipulates that the EU 'shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers.'

Article 7 TFEU is one of several consistency requirements contained in the Treaty on European Union ('the TEU') and the TFEU.[46] In order to differentiate the legal demands of such requirements, Franklin provides a detailed methodological approach to categorising the consistency requirements found in the EU Treaties.[47] According to this methodology, Article 7 constitutes an explicit consistency requirement as it is provided for in the TFEU. The requirement is horizontal in nature, demanding that the EU as a whole achieves consistency. In terms of subject-matter, Article 7 TFEU refers to consistency being achieved between all EU policies, thereby also applying to internal policies, such as data protection and competition law. In relation to its potential impact, Article 7 TFEU refers to both 'policies' and 'activities', which encompasses both policy-making and further implementation. Moreover, Article 7 TFEU falls under the Court's direct jurisdiction, rendering it directly enforceable in practice.[48]

---

[46] Articles 13(1), 17, 18 and 21(3) TEU and articles 181(1) and 212(1) TFEU.

[47] Christian NK Franklin, 'The Burgeoning Principle of Consistency in EU Law' (2011) 30 YEL 42, 53-58.

[48] The Court of Justice's only jurisdictional limits in relation to the EU Treaties are provided in articles 24 TEU and articles 275 and 276 TFEU.

However, the imperative question concerns what type of consistency is to be achieved by taking all EU objectives into account, as this goes to the heart of whether Article 16 TFEU, in conjunction with Article 7 TFEU, could be invoked to incorporate data protection concerns into competition analysis.

ii. Interpretation of Consistency

The interpretation of the principle of consistency is far from clear. It is contended that consistency, in its narrow sense, refers to the 'absence of contradiction', whereas, in a broad sense can be interpreted as coherence which relates to 'positive connections'.[49] The interpretation of consistency is particularly pertinent to the present discussion concerning the potential impact that Article 7 TFEU could have on incorporating data protection concerns into competition law as the different understandings differ immensely in terms of their potential instrumentality. The reason for this being that coherence is a matter of degree, whereas consistency is a static notion in the sense that concepts of law can be more or less coherent but cannot be more or less consistent.[50] As such, a narrow construction of consistency would appear to be inherently instrumental as a legal standard.[51] Thus, whether the consistency requirement is to be interpreted in a narrow or broad sense is of particular importance as it could result in different legal obligations being imposed in practice.

On the one hand, defining consistency as an 'absence of contradictions' would necessitate that data protection concerns be taken into account to the extent that no contradictions would arise with the principles provided for within the data protection framework, for instance the principle of consent.[52] Under this interpretation, Article 16 TFEU, read in conjunction with Article 7 TFEU would require the Commission to actively consider whether its actions contradict any established principles of data protection law.

However, Franklin is of the opinion that duties to take account of policy considerations do not appear to be designed so as to ensure that consistency in a narrow sense is achieved in practice.[53] As discussed above, by its nature, a duty to take into account is a flexible obligation as matters need only be taken into account, as opposed to adhering to a more stringent standard. Moreover, Franklin submits that were the Court to interpret consistency under Article 7 TFEU as requiring an absence of contradictions, it might prove 'absurdly

[49] Christophe Hillion, 'Tous pour un, un pour tous! Coherence in the External Relations of the European Union' in Marise Cremona (ed), *EU External Relations Law, Collected Course of the Academy of European Law* (OUP 2008) 10, 14.
[50] ibid 14.
[51] Franklin (n 47) 47.
[52] Article 7 GDPR.
[53] Franklin (n 47) 66.

difficult - if not practically impossible - to avoid breaches from occurring in practice.'[54] While, it may be clear to envisage how the Commission could alter its practice in order to ensure an absence of contradictions with data protection, it must be remembered that Article 7 TFEU requires such consistency to be achieved between all the EU's policies which when contemplated, gives force to Franklin's conclusion that it would be 'absurdly difficult' to abide by such a consistency requirement in practice.

On the other hand, applying consistency as interpreted akin to the notion of coherence, is problematic. Trying to decipher what the standard demands in practice, brings to mind the quotation, 'it is easier to write ten volumes of philosophy than to put a single precept into practice.'[55]

First and foremost, coherence is open to two interpretations. Under the first understanding it is found that consistency in the sense of an absence of contradictions will always be necessary for achieving any degree of coherence, although even then, more may be required.[56] Thus, this first understanding, in requiring an absence of contradictions, would amount to a similar obligation as discussed above. However, according to the second understanding, coherence may be established even in the face of contradiction so long as there are other justifying factors.[57]

While coherence in this second sense could allow for data protection concerns to be taken into account in the application of competition law, it lacks the equivalent legal force of an 'absence of contradictions' standard as it would allow the existence of contradiction to be justified. Franklin provides two examples of what could justify a contradiction: firstly, the practical impossibility of seeking to take into account all policy objectives; and secondly, arguments that the objectives were taken into account, yet subsequently disregarded.[58] In this regard, it is not inconceivable that the Commission could justify its position for leaving the data protection concerns to the relevant authorities on the basis of, for instance, expertise or avoiding duplication. Therefore, while coherence in a broad sense could act as a legal basis for taking data protection concerns into account, it could also be used to justify the Commission's current position.

---

[54] ibid 70.
[55] R F Christian, *Tolstoy's Diaries, Volume I: 1847-1894 (Diary Entry on 17th March 1847),* (Athlone Press, 1985).
[56] Franklin (n 47), 49.
[57] ibid 49.
[58] ibid 74.

C. Effectiveness

From the foregoing analysis it is established that both Article 12 TFEU and Article 16 TFEU, read in conjunction with Article 7 TFEU, have the potential to integrate data protection considerations into competition analysis. However, the parameters of these obligations remain undefined and ambiguous which leaves the effectiveness of these gateways inconclusive.

Moreover, apart from the question regarding the extent of the obligation imposed by the provisions of the TFEU, there are other factors which may undermine the effectiveness of these gateways, namely, the position in the assessment under the respective provisions and the standing requirements under Article 263 TFEU.

i. Position in Assessment

While it is found that data protection considerations may be taken into account, their position in the assessment differs in each of Article 101 TFEU, Article 102 TFEU and mergers which in turn impacts the extent of the influence of data protection concerns.

In relation to Article 101 TFEU, the bifurcated structure of the provision has triggered debate as to the position of public policy objectives in the analysis under Article 101 TFEU. On the one hand, the position of the Commission is that non-competition concerns are admissible, provided that they can be subsumed under the four conditions of Article 101(3) TFEU.[59] Following this line of reasoning, data protection considerations could only function as a justification against the finding of an infringement under Article 101(1) TFEU but could not be taken into account in order to establish an infringement of Article 101(1) TFEU. On the other hand, this view is contested on the basis that it is inconsistent with both the Court's case law and the Commission's decisional practice in which there is evidence of non-efficiency considerations being taken into account under Article 101(1) TFEU.[60] Under this view, data protection concerns could be taken into account in the finding of an infringement, for example, undertakings colluding on terms of privacy policies. Evidently, adherence to the second view provides more scope for data protection considerations to be taken into account.

Under Article 102 TFEU the potential role of data protection concerns is more expansive. In assessing whether conduct has abusive effects under Article 102 TFEU, there is a distinction between firstly, exclusionary abuses

[59] Guidelines on the application of article 81(3) of the Treaty [2004] OJ C101/97, [42].

[60] See: Van Rompuy, *Economic Efficiency: The Sole Concern of Modern Antitrust Policy? Non-efficiency Considerations under Article 101 TFEU* (Wolters Kluwer Law & Business 2012), 229-252.

which are those capable of having, and are likely to have, a foreclosure effect on the market, and secondly, exploitative abuses, those which are directly exploitative of consumers. In the discussion of data protection and competition law, the potential role of data protection concerns in relation to exploitative abuses has been flagged. Notably, the German Competition Authority ('Bundeskartellamt') has initiated proceedings against Facebook on the allegation that Facebook's use of unlawful terms and conditions could represent an abusive imposition of unfair conditions on users.[61] This provides an example of how data protection concerns could be taken into account in establishing harm under Article 102 TFEU.

Moreover, data protection considerations could be relevant in establishing an objective justification under Article 102 TFEU. While the parameters of accepted justifications are not completely defined, three categories may be distinguished: efficiencies; objective necessity and protecting an undertaking's own commercial interests. Most relevant to data protection concerns is the category based on objective necessity which the Commission defines as 'factors external to the undertaking'.[62] For example, this justification has been previously invoked, albeit unsuccessfully, to argue that the behaviour of the dominant undertaking was necessary in order to make sure that nail guns were used safely.[63] On similar reasoning, data protection considerations could be invoked in order to justify *prima facie* abusive behaviour, for instance, data protection concerns could be invoked in order to justify a refusal to supply by a dominant undertaking. Therefore, under Article 102, there is scope for data protection to be taken into account in both establishing harm and justifying infringements.

In relation to merger control, there is limited scope for taking data protection considerations into account in the substantive assessment of a merger's effect on competition. Under the EUMR, the substantive test is whether a concentration would significantly impede effective competition (SIEC test).[64] This test remains heavily focused on the creation or strengthening of a dominant position which is based solely on the increase of market power, thus leaving little scope for taking data protection considerations into account. However, in accordance with both Article 2(b) EUMR and the requirement to take efficiencies into account,[65] proportionate

[61] 'Bundeskartellamt initiates proceedings against Facebook on suspicion of having abused its market power by infringing data protection rules' <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html> accessed 11 February 2018.

[62] Guidance on the Commission's enforcement priorities in applying article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009] OJ C45/7, [28].

[63] Case T-30/89, *Hilti*, EU:T:1991:70, [118].

[64] Article 2(3) EUMR.

[65] Recital 29 EUMR.

data protection benefits or restrictions which are likely to flow from a proposed transaction could be taken into account under the SIEC test in the context of assessing whether 'technical and economic progress' would occur to the benefit of consumers. Similar to the Commission's view regarding Article 101 TFEU, such an efficiency analysis could only operate to justify a concentration and not to establish an infringement.

ii. Standing Requirements

The standing requirements for judicial review undermine the effectiveness of the TFEU as a means of incorporating data protection concerns into competition analysis. The main avenue for those wishing to challenge the validity of an EU act is through a direct action for annulment under Article 263 TFEU. As a competition decision does not constitute a regulatory act, according to the rules on *locus standi* under Article 263 TFEU, in order to challenge a competition decision on the basis of infringement of Treaty articles an individual would have to establish individual concern. In order to demonstrate individual concern it must be shown that a decision affects an individual by reason of certain attributes which are peculiar to him or her or by reason of circumstances in which he or she is differentiated from all other persons and by virtue of these factors distinguishes him or her individually just as in the case of the person addressed.[66] It would be extremely onerous for an individual who wanted to challenge a competition decision on the basis of failure to take data protection considerations into account to meet this standard. Thus, the narrow possibility for judicial review ultimately undermines the effectiveness of these provisions as gateways for incorporating data protection concerns.

Upon a holistic reading of the TFEU, both Article 12 TFEU and Article 16 TFEU, read in conjunction with Article 7 TFEU, in principle, have the potential to integrate data protection considerations into competition analysis. However, the effectiveness of such incorporation is impacted by the lingering question regarding the extent of the obligation imposed, and furthermore by the position in the assessment under each respective competition provision and the standing requirements under Article 263 TFEU.

III. Charter of Fundamental Rights

With the entry into force of the Lisbon Treaty in 2009, the Charter, which was first drafted and adopted in 2000, became a legally binding instrument on

[66] Case 25/62, *Plaumann*, EU:C:1963:17.

equal footing with the TEU and the TFEU.[67] Pertinently, the Charter provides for a stand-alone data protection provision with Article 8 recognising that 'everyone has the right to the protection of personal data concerning him or her.'

The scope of application of the Charter is established in Article 51(1):

> [t]he provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

Accordingly, all EU institutions and organs are bound by the Charter, and can be challenged for failure to respect its terms. To take one example, in *Digital Rights Ireland*[68] the Court, for the first time, declared an EU instrument - the Data Retention Directive[69] - entirely invalid, because it interfered with the fundamental right of data protection as provided for in the Charter.

Since the Charter has been given binding legal effect, it has gained widespread application in competition cases. The Charter has been invoked in order to question the standard of judicial review of Commission decisions in light of Article 47.[70] Similarly, parties have appealed to the Charter in the context of the Commission's practice of unannounced inspections or 'dawn raids',[71] to the extent that it is said that it is 'more or less standard procedure' for companies targeted by cartel investigations to invoke infringement of either one of several Charter provisions.[72]

Therefore, bearing this precedent in mind, the right to data protection provided for in Article 8 has the potential to constrain the application of competition law and demand that the Commission takes data protection concerns into account when applying competition policy. In this regard, both the principles governing the processing of personal data and the standard of

---

[67] Article 6(1) TEU.

[68] Joined Cases C-293/12 and 594/12, *Digital Rights Ireland*, EU:C:2014:238.

[69] 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] OJ L/281.

[70] Case C-389/10, *P KME Germany and Others v Commission*, EU:C:2011:816.

[71] Joined Cases T-289 and 290/11 and T-521/11, *Deutsche Bahn and Others v Commission*, EU:T:2013:404.

[72] Helene Andersson, 'Dawn Raids in Competition Cases: Do the European Commission's Dawn Raid Procedures Stand the Test of the Charter' in Sybe de Vries, Ulf Bernitz and Stephen Weatherill (eds) *The EU Charter of Fundamental Rights as a Binding Instrument* (Hart Publishing 2015), 321.

judicial review in relation to data protection has the potential to impact the application of competition law.

A. Processing of Personal Data

The principles governing the processing of personal data has the potential to influence the application of competition law. In order to comply with Article 8, any decision by the Commission, which involves the processing of personal data,[73] must comply with the principles established within the data protection framework. Article 8(2) states that data must be processed 'fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.' Thus, encompassed within Article 8 are both the requirement of a lawful basis for processing and the principle of purpose limitation.

The requirement of a lawful basis for processing could constitute a significant constraining factor in the application of competition law. Notably, the sharing of personal data is often suggested as a remedy to claims of market power where one entity has control over a large dataset. However, the sharing of personal data falls within the definition of data processing and therefore, any order requiring the disclosure of personal information must, in order to not infringe Article 8, be in compliance with principles governing data processing. The GDPR provides that the processing of personal data is lawful if at least one of the following legal bases applies: consent, contractual necessity, compliance with legal obligations, vital interests, public interest or legitimate interests.[74]

In order to illustrate the potential influence of the necessity for a legal basis for processing, experience can be drawn from the practice of both the French and British national competition authorities ('NCAs'). Firstly, the actions of the French Competition Authority ('Autorité de la concurrence') in their legal action against GDF Suez, demonstrate compliance with the principle of consent. As part of an investigation, the Autorité de la concurrence instructed GDF to disclose part of its customer database to competitors, mostly made up of personal data relating to identified individuals.[75] Therefore, the disclosure raised data protection concerns. In order to address such concerns, GDF Suez was ordered to obtain consent for the data sharing from all of the affected data subjects.

---

[73] Article 4(2) GDPR defines data processing as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'.

[74] Articles 6(1)(a)-(f) GDPR.

[75] Décision n° 14-MC-02 du 9 sep 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité.

Secondly, in August 2015, the UK Competition and Market Authority ('the CMA') was seeking to revitalise competition in the energy market and proposed to make customers' details available to rival suppliers on a database. The CMA considered the potential data protection issues concerning the sharing of personal data and implemented provisions to comply with principles including consent.[76] These actions of the NCAs demonstrate how the requirement for a lawful basis for data processing could condition the implementation of competition law.

Moreover, the principle of purpose limitation may have consequences for data sharing under competition law. Article 5(1)(b) GDPR provides that personal data must be 'collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.'[77] While further processing for a secondary purpose is not forbidden, the secondary purpose must not be 'incompatible' with the purposes for which the data have been collected. The potential impact of purpose limitation on competition law would be if the data sharing was demanded between two companies who were considered competitors but who used data for different purposes. In this regard, Costa-Cabral and Lynskey consider that, for example, where personal data is to be collected by a social networking site, it might not be possible to transfer it to the provider of a mobile phone application. This would apply even if both were considered competitors from a competition law perspective, as from the perspective of the individual, the purposes of the data processing may be incompatible.[78] Therefore, in order to comply with the principle of purpose limitation, personal data could not be transferred without consent for the new purpose.

B. Standards of Judicial Review

The Commission's obligation to respect the right to data protection has the potential to impact the standard of review of competition decisions. Notably, this is an area which has previously felt the impact of the Charter, namely in relation to the right to an effective remedy under Article 47. The addition of data protection, as a fundamental right, has the potential to further influence the current standard of judicial review.

Judicial review of competition law is complicated due to the intricate relationship between application of the law, which falls under the mandate of

---

[76] Competition & Markets Authority, 'Energy market investigation, Summary of final report' June 2016, [235] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/531157/Energy-final-report-summary.pdf> accessed 11 February 2018.

[77] Article 5(1)(b) GDPR.

[78] Francisco Costa-Cabral and Orla Lynskey, 'The Internal and External Constraints of Data Protection on Competition Law in the EU' *LSE Legal Studies Working Paper* 25 (2015), 35.

judicial review, and underlying economic analysis, which falls within the discretionary mandate of the Commission.[79] Where the Treaties have vested the Commission with a margin of discretion, the Courts are confined to 'checking whether the rules on procedure and on stating reasons have been complied with, whether the facts have been accurately stated and whether there has been any manifest error of assessment or a misuse of powers'.[80] Therefore, as regards complex economic assessments, the Court exercises a deferential standard of review.

In contrast, the Court takes a strict approach to privacy and data protection. In a series of judgments the Court has established a strict standard of review of acts of EU institutions which impact Articles 7 and 8 of the Charter.[81] In *Digital Rights Ireland* and *Schrems* it was explicitly established that the nature of the rights to privacy and data protection played an important role in determining the Commission's reduced discretion and the test's strictness.[82]

Evidently, there is an inherent dichotomy between the standards of 'manifest error of assessment' and 'strict scrutiny'. This results in an obvious tension with regard to judicial review of decisions taken by the Commission which also engage data protection rights. As the Court's strict approach to privacy and data protection applies to acts of all EU institutions, thus encompassing decisions of DG Competition, this could impact the standard of judicial review applied to competition decisions.

From the foregoing analysis, it is evident that the Charter of Fundamental Rights provides significant opportunity for data protection to be taken into account in competition policy. However, there is one limiting factor. In order to challenge a Commission decision on the basis of infringement of a Charter right, an individual would have to satisfy the stringent standing requirements outlined in section 3.3.2. Ultimately, this has the potential to undermine the effectiveness of Article 8 as a gateway by which to incorporate data protection concerns into competition law.

IV. Public Interest Considerations in Merger Control

Merger control has been at the centre of the debate regarding the intersection between data protection and competition law due to a series of cross-border

---

[79] Firat Cengiz, 'Judicial Review and the Rule of Law in the EU Competition Law Regime after Alrosa' (2011) 7(1) ECJ 127, 128.

[80] Case T-201/04, *Microsoft v Commission*, EU:T:2007.

[81] Case C-362/14, *Schrems v Data Protection Commissioner*, EU:C:2015:650; *Digital Rights Ireland* (n 68); Case C-131/12, *Google Spain and Google Inc*, EU:C:2014:317; Joined Cases C-92/09 and C-93/09, *Schecke and Eiffert*, EU:C:2009:284.

[82] *Schrems* (n 81), para 78; *Digital Rights Ireland* (n 68) [48].

transactions, such as *Facebook/WhatsApp.*[83] Due to the realisation that possession of Big Data generates significant advantages, mergers and acquisitions in digital markets have become more frequent for undertakings wishing to obtain datasets in situations where the target company may not always have a big turnover, but is regarded as valuable due to its dataset.[84] This was evident in the *Facebook/WhatsApp* merger where Facebook bought the messaging application WhatsApp for $19 billion while it was estimated that the company only had a revenue of $20 million. However, with 315 million active daily users, it is clear that the value of the company lay in its dataset.

Data protection and privacy issues represent 'the other side of the coin'[85] of data-driven mergers. While online platforms such as Google and Facebook use personal data to enhance users' experiences and provide more personally relevant services, the accumulation of vast amounts of data about consumer behaviour combined with the expansion of targeted advertising imposes costs in the form of the loss of privacy on consumers.[86] Therefore, mergers and acquisitions in digital markets have become a focal point for data protection concerns. However, the relationship between non-competition concerns and merger control is uneasy.

Merger control within the EU is governed by Regulation No. 139/2004[87] ('the EUMR'). While, the EUMR is predominantly based on competition interests, it does provide for limited evaluation of public interest concerns under Article 21(4). Therefore, it is proposed to examine whether data protection could be considered a public interest within this provision.

A. Article 21(4) EUMR

Article 21(4) provides that even where the Commission has exclusive jurisdiction,[88] Member States may take appropriate measures to protect legitimate interests other than those taken into consideration by the EUMR

---

[83] *Facebook/WhatsApp* (n 19).

[84] Hanna Stakheyeva and Fevzi M Toksoy, 'Merger control in the big data world: to be or not to be revisited?' (2017) 38(6) ECLR 265, 265.

[85] In the matter of Google/DoubleClick FTC File No. 071-0170, Dissenting Statement of Commissioner Pamela Jones Harbour, 9 <www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf> accessed 11 February 2018.

[86] OECD, Big Data: Bringing Competition Policy to the Digital Era, DAF/COMP(2016)14, 17 <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf> accessed 11 February 2018.

[87] Regulation (EC) No 139/2004 on the control of concentrations between undertakings [2004] OJ L24/1.

[88] Pursuant to Article 21(2) and (3), the Commission has exclusive jurisdiction to assess the competitive impact of concentrations with a Community dimension as defined in articles 1 and 3 EUMR.

which are compatible with the general principles and other provisions of EU law.

The provision operates by allowing non-competition concerns to be invoked by Member States for jurisdictional purposes i.e. Member States can seek to remove certain aspects of the transaction from the Commission's exclusive jurisdiction. Therefore, under Article 21(4) the Commission assesses the effect of a merger on competition, while Member States are permitted to intervene on public interest grounds. This is distinguished from the invocation of non-competition concerns for substantive purposes, i.e influencing the Commission's assessment of a merger's effect on competition, as was considered in section 3.3.1.

Article 21(4) distinguishes between two types of public interest, firstly, specified 'recognised interests' which are considered *prima facie* legitimate, and secondly, 'other public interests' which, in order to ensure the *effet utile* of the EUMR, require *ex ante* review by the Commission. Article 21(4) stipulates that public security, plurality of the media, and prudential rules, are considered to be 'recognised' public interests. Therefore, Member States may adopt measures to protect these interests without prior communication to, and approval from, the Commission. It is evident, and therefore unnecessary to elaborate, that data protection could not fall within the scope of any of these recognised interests.

Member States may invoke other legitimate public interests under Article 21(4) other than those considered 'recognised interests'. Notably, this catch-all provision in Article 21(4) is rarely invoked and the Commission tends to reject requests from Member States to adopt measures to protect non-recognised interests. That being said, the possibility does exist. In order for an interest to be recognised, it must, firstly, be considered a 'public interest' and secondly, be compatible with the general principles and other provisions of EU law, including proportionality and non-discrimination, as well as to provisions of primary and secondary EU law. Of particular significance to mergers and acquisitions are the rules regarding free movement of capital and freedom of establishment, Articles 49 and 63 TFEU.

B. Data Protection as a Legitimate Public Interest

The internet permeates every aspect of our lives, thus changing our society in a fundamental way, and along with it our values and interests. With the exponential growth of information sharing, protecting our privacy online has become a vitally important interest in society. The concept of public interest is both expansive and relative as it can encompass various values shared by a

respective state and also varies depending on the time and the state.[89] This dynamic nature of the concept of public interest is illustrated by the justification standard employed in free movement law which, accordingly, does not require a static conception of public interest.[90] Therefore, it is contended that data protection could satisfy the first requirement and be considered a 'public interest'.

As data protection has, to date, not been raised as a public interest justification within free movement law, it is proposed that an analogy could be drawn to consumer protection which has been recognised as constituting an overriding reason in the general interest.[91] The Court has been willing to accept that certain groups of consumers require enhanced protection, for instance, protecting the interests of particularly vulnerable consumers. This is focused - targeted - consumer protection.[92] For instance, in *Citroën Belux,*[93] the Court found that 'financial services are, by nature, complex and entail specific risks with regard to which the consumer is not always sufficiently well informed.'[94] The protection of consumers in the realm of Internet use necessitates a similar approach. As in the financial service industry, significant information asymmetries exist between Internet users and service providers. For instance, it has been estimated that it would take the average Internet user 76 days to read every privacy policy he or she encountered online in a year.[95] These information asymmetries combined with the harm to the consumer in the form of loss of privacy justifies a similar approach to that which already exists in the Court's analysis of consumer protection. Therefore, on the same reasoning that consumer protection has been recognised as a legitimate public interest, data protection could be accepted by the Court.

One of the greatest obstacles in establishing a legitimate public interest justification is an evidentiary obstacle.[96] The Court has emphasised that in

---

[89] Mateusz Blachucki, 'Public interest considerations in merger control assessment' (2014) 35(8) ECLR 380, 383.

[90] Niamh Nic Shuibhne, 'Primary Laws: Judging Free Movement Restrictions After Lisbon' in Panos Koutrakos, Niamh Nic Shuibhne and Phil Syrpis (eds) *Exceptions from EU Free Movement Law* (Hart Publishing 2016), 297.

[91] Case C-225/15, *Politanò*, EU:C:2016:645, [39].

[92] Stpehen Weatherill, 'Justification, Proportionality and Consumer Protection' in Panos Koutrakos, Niamh Nic Shuibhne and Phil Syrpis (eds) *Exceptions from EU Free Movement Law* (Hart Publishing 2016) 250.

[93] Case C-265/12, *Citroën Belux*, EU:C:2013:498.

[94] ibid [39].

[95] Madrigal, 'Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days' <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/> accessed 1 June 2017.

[96] See: Niamh Nic Shuibhne and Marsela Maci, 'Proving Public Interest: The Growing Impact of Evidence in Free Movement Case Law' (2013) 50 CML Rev 965.

order to successfully rely on a public interest claim, the Member State must adduce appropriate evidence.[97] In relation to data protection and mergers, as noted above, there is a consensus that the accumulation of vast amounts of data about consumer behaviour combined with the expansion of targeted advertising raises concerns regarding the privacy of consumers.[98]

Moreover, any conditions attached to a merger would have to satisfy the requirements of proportionality. An oft-cited example of how merger conditions could be used to address data protection concerns is a mandated firewall between the merging entities datasets. It is contended that such a firewall would be proportionate under free movement law as it is suitable for elevating privacy concerns due to the accumulation of large datasets and it is considered to be the least restrictive. To take the *Facebook/WhatsApp* decision as an example; despite the assurances from Facebook at the time of the acquisition that they would be unable to establish automated matching between Facebook users' accounts and WhatsApp users' accounts, it unfolded that this was not the case when, in August 2016, it was announced that WhatsApp's privacy policy was to be altered in order to enable Facebook to start using data from the messaging application.[99] This could have been avoided by the imposition of a firewall, which would adequately address the concerns regarding the potential concentration of data and resulting harm to consumers' privacy.

C. Challenges

While *prima facie* Article 21(4) seemingly provides a suitable gateway by which to incorporate data protection concerns into merger control, there are numerous practical challenges that could impact the provision's effectiveness, namely, the interaction with national law and national institutional arrangements and the potential measures that could be implemented pursuant to Article 21(4).

i. National Law and Institutional Arrangements

As demonstrated above, in order for data protection to be invoked as a legitimate interest under Article 21(4) it must not breach EU law. However, provision must also exist under national law for such a public interest criteria to be invoked. The frameworks across the Member States diverge regarding

---

[97] Case C-543/08, *Commission v Portugal (Golden Shares)*, EU:C:2010:669, [87]; Case C-319/06, *Commission v Luxembourg*, EU:C:2008:350, [51].

[98] OECD (n 86) 17.

[99] WhatsApp Blog, 'Looking ahead for WhatsApp' <https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp> accessed 11 February 2018.

the intersection between merger control and public interest factors. Three different models can be distinguished: firstly, the governing framework in some Member States is open-ended allowing for data protection to be easily included; secondly, some frameworks provide for non-exhaustive list of specified interests which can be expanded following a certain procedure; finally, in some Member States the framework is restrictive providing either an exhaustive list of public interest factors or no provision at all.

Firstly, the provision for public interest criteria in both the German and Spanish frameworks is open-ended. The German Act against Restraints of Competition (GWB) references overriding public interests which justify restraints of competition but does not define any specific criteria in order to constitute a public interest consideration.[100] Similarly in Spain, Law 15/2007 sets outs a non-exhaustive list of public interest grounds. Under such flexible frameworks, it is conceivable that data protection could be invoked as a legitimate public interest.

Secondly, in the UK, provision is made under the Enterprise Act, 2002 allowing for intervention in mergers on certain specified public interest grounds.[101] The Enterprise Act recognises the possibility that these grounds for intervention could be supplemented. A public interest consideration can only be adopted by way of adopting a statutory instrument approved by Parliament through an affirmative procedure. This has happened once previously in relation to the Lloyds TSB and HBOS merger. In order to allow the Lloyds merger on public interest grounds, the Secretary of State had to create a new public interest ground - stability of the financial system - with the consent of Parliament.[102] Therefore, while provision for data protection as a legitimate interest is possible, the procedure to be followed is stringent.

Thirdly, in Ireland, provision only exists for intervention to protect the plurality of the media.[103] While, in Belgium the Government's power to overturn merger decisions on public interest grounds was withdrawn in 2013.[104] Therefore, the possibility of data protection being considered as a public interest in these jurisdictions is limited due to the constraints imposed by national legislation.

Furthermore, the relationship between national competition and data protection authorities would hold particular practical relevance, pertinently in relation to the issue of which authority would conduct the public interest assessment. As data protection is not currently considered a public interest in

---

[100] S 42, Act against Restraints of Competition (GWB).

[101] S 58, Enterprise Act, 2002.

[102] S 2, SI 2008/2645, The Enterprise Act 2002 (Specification of Additional Section 58 Consideration) Order 2008.

[103] Part 3A, Competition and Consumer Protection Act, 2014.

[104] Alison Jones and John Davies, 'Merger control and the public interest: balancing EU and national law in the protectionist debate' (2014) 10(3) ECJ 453, fn45.

any Member State, there is no formal provision for consultation between national competition and data protection authorities. However, a parallel can be drawn between the systems in place for consultation with, *inter alia*, communication or energy regulators. For example, in the UK, provision is made for the CMA and OFCOM (UK communications regulator) to submit a report to the Secretary of State regarding public interest considerations.[105] Therefore, it is foreseeable that if data protection is considered a public interest, provision could be made for consultation with the Information Commissioner's Office (UK data protection regulator). Such provision would be preferable if data protection was to be effectively protected within the merger framework.

ii. Potential Measures under Article 21(4)

The successful invocation of Article 21(4) allows the Member State, on the basis of national law, to subject a merger to additional conditions or to block it altogether, provided this is proportionate in order to protect the interest concerned.

The ability of Member States to impose conditions on a merger under Article 21(4) is governed by national law. As data protection is a harmonised field, the scope for measures is dependent on the EU framework. In this regard, under EU data protection law, national authorities can only impose behavioural remedies and sanction companies after they have infringed the rules. Crucially, the framework does not provide national authorities with the possibility of adopting prospective or structural measures. Therefore, in relation to potential measures imposed pursuant to Article 21(4) it does not appear possible for a national data protection authority to either subject a merger to any conditions or block it, if it does not give rise to data protection issues at the time the merger is approved by the Commission under the EUMR.[106]

This extremely limits the potential effectiveness of Article 21(4) as a gateway to incorporating data protection concerns into merger control. Due to this limitation a national data protection authority would only be capable of imposing conditions on a merger under Article 21(4) if the transaction in and of itself infringes data protection rules. However, if it is merely anticipated that certain data protection issues may arise at some point in the future, the only option would be to monitor whether the merged entity continues to comply with its data protection obligations. If indications arise at a later date that the merged entity is in breach of the relevant rules, an investigation may be initiated under data protection law outside the framework of Article 21(4).

[105] Ss 44(3)(b) and 44A, Enterprise Act, 2002.
[106] Graef (n 9) 20.

Thus, the procedure under Article 21(4) is only relevant for mergers which at the time of their notification to the Commission already raise data protection concerns.[107]

Merger control is at the forefront of the discussion regarding data protection concerns and competition policy. From the preceding analysis it is established that Article 21(4) could be invoked by Member States in order to allow for national measures to be taken in order to protect personal data in these large data-driven mergers. However, successful invocation is dependent on a provision existing within the national framework for data protection to constitute a public interest. Moreover, the potential relationship between national competition and data protection authorities will be of practical relevance to an effective data protection assessment. Furthermore, the effectiveness of Article 21(4) is diminished by the constraints on the potential measures which could be imposed on mergers.

Conclusion

This article has explored and considered the possible legal bases for the incorporation of data protection, as a non-economic concern, into competition policy. While the Commission and the Court have consistently abided by the view that there is a strict delineation between the two fields, it has been established herein that, within the EU legal order, there is scope for incorporation of data protection concerns into competition enforcement. Firstly, upon a holistic reading of the TFEU, both Article 12 TFEU and Article 16 TFEU, read in conjunction with Article 7 TFEU, provide a legal basis for competition enforcement to take data protection considerations into account. Secondly, by virtue of the right to data protection being enshrined in the Charter of Fundamental Rights, the Commission is obliged to respect that right in the application of competition law. Finally, pursuant to Article 21(4) EUMR there is scope for Member States to invoke data protection as a public interest factor in mergers. While each gateway is faced with challenges regarding its potential effectiveness, in principle, the legal basis exists.

Therefore, in conclusion, competition law is not a 'lonely portfolio'[108] and against the fast evolving backdrop of the digital economy, it is considered that in order to ensure the effectiveness of data protection, a more holistic approach should be adopted with competition enforcement taking privacy considerations into account.

---

[107] ibid 21.

[108] Hearing of the European Commission for Competition Margrethe Vestager before the European Parliament, 2 October 2014 <http://www.europarl.europa.eu/hearings-2014/en/schedule/02-10-2014/margrethe-vestager> accessed 1 June 2017.