Fairness and enforcement: bridging competition, data protection, and consumer law

Inge Graef*, Damian Clifford** and Peggy Valcke***

Key Points

- Since the notion of fairness underpins the regimes of competition, data protection, and consumer law, it can act as a connecting factor to align substantive protections and enforcement mechanisms in the three fields.
- While most attention has so far been devoted to how vigorous competition enforcement can render data protection rules more effective, the complementarity between the regimes also works the other way around.
- In particular, substantive data protection or consumer law principles can be integrated into competition analysis so as to strengthen the ability of competition authorities to tackle new forms of commercial conduct.
- At the same time, the competition concepts of market definition and market power can help to interpret the scale of obligations that data controllers and processors have to comply with under data protection law in line with the risk-based approach of the General Data Protection Regulation.

Introduction

Recent years have shown a surge of interest from various enforcement agencies to remedy commercial behaviour exploiting the increasing information and power asymmetries between consumers and firms. What is

- Tensions occur where competition enforcement favours sharing or merging of data sets for economic efficiency reasons against the spirit of the data protection rules, but there is also room for synergies by involving data protection or consumer authorities in merger investigations and by considering data protection or consumer interests more proactively in the design of merger remedies.

particularly notable about this rise in attention is that enforcement actions demonstrate clear interactions between different legal fields that are traditionally applied and enforced in isolation. The present article will focus in particular on the growing interaction between competition, data protection, and consumer law.

The Italian Competition, Communications and Data Protection Authority opened a joint ‘big data’ sector inquiry in May 2017 that not only aims to identify potential competition concerns but also to define ‘a regulatory framework able to foster competition in the markets of the digital economy, to protect privacy and consumers, and to promote pluralism within the digital ecosystem’.¹ The Bundeskartellamt (German competition authority) announced its preliminary assessment in the *Facebook* competition investigation in December 2017, reaching the view that Facebook’s collection and use of data from third-party sources is abusive. According to the Bundeskartellamt, Facebook’s terms of service violate data protection provisions and thereby constitute abuse of dominance under competition law as well.² On the basis of its new competence in the area

* Tilburg Institute for Law, Technology, and Society (TILT) and Tilburg Law & Economics Center (TILEC), Tilburg, Netherlands. E-mail: i.graef@uvt.nl.

** FWO Aspirant, KU Leuven Centre for IT & IP Law (CiTiP), Leuven, Belgium.

*** KU Leuven Centre for IT & IP Law (CiTiP), Leuven, Belgium.

1 Press release Autorità Garante della Concorrenza e del Mercato, “Big Data”: Italian Regulators Open A Sector Inquiry, 1 June 2017 <<http://www.agcm.it/en/newsroom/press-releases/2384-%E2%80%9CDig-data%E2%80%9D-italian-regulators-open-a-sector-inquiry.html>> accessed 31 August 2018.

2 Bundeskartellamt, ‘Preliminary Assessment In Facebook Proceeding: Facebook’s Collection and Use of Data from Third-Party Sources Is

of consumer protection,³ the Bundeskartellamt also opened two sector inquiries into online price comparison websites and smart TVs in October and December 2017, respectively. The sector inquiry into comparison websites aims to uncover possible violations of consumer law and to identify possible deficits in the enforcement of consumer rights that so far mainly takes place in individual private court proceedings.⁴ The sector inquiry into smart TVs investigates how producers of smart TVs handle user data. In particular, the Bundeskartellamt is looking to clarify to what extent smart TV manufacturers collect, use and pass on personal data, and whether individuals are appropriately informed of these practices in the contract terms.⁵

While the national authorities' awareness of these issues is a welcome development, it raises the question of how to create coherence in enforcement between Member States. Differences in the degree of enforcement create risks for the internal market both for companies that have to comply with distinct requirements throughout the European Union (EU) and for consumers who depend on the success of their national agencies to act. Moreover, as the behaviour of companies in digital markets is blurring the boundaries between legal regimes, a better coordination between enforcement authorities is necessary to adequately protect consumers. The various enforcement actions under competition, data protection, and consumer law following the update of WhatsApp's privacy policy in August 2016 form a good illustration of this overlap. Using its competition law competences, the European Commission imposed a 110 million euro fine on Facebook for providing incorrect or misleading information during the 2014 merger investigation. While Facebook had informed the

Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts, WhatsApp's updates to its terms of service in August 2016 included the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. On that basis, the Commission found that the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014 and that Facebook staff were aware of such a possibility.⁶ In addition, the update of WhatsApp's privacy policy attracted the attention of several national data protection authorities,⁷ resulting in a coordinated action by the Article 29 Working Party.⁸

In March 2018, two further developments occurred at the national level. The Hamburg Commissioner of Data Protection and Freedom of Information announced that the Higher Administrative Court of Hamburg had confirmed the administrative order prohibiting the data sharing between Facebook and WhatsApp⁹ and the UK Information Commissioner's Office succeeded in having WhatsApp sign an undertaking including a public commitment from WhatsApp not to share personal data with Facebook until data protection concerns are addressed in line with the General Data Protection Regulation (GDPR).¹⁰ National consumer authorities have also intervened. The Federation of German Consumer Organizations sought an injunction before the Berlin Regional Court in January 2017 to stop the data sharing with Facebook and the deletion of data already transferred to Facebook.¹¹ The Italian competition and consumer authority took two decisions in May 2017 imposing a fine of 3 million euro on WhatsApp for alleged unfair commercial practices and

Abusive', 19 December 2017 <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html?nn=3591568> accessed 31 August 2018.

- 3 The 9th amendment to the German Competition Act, promulgated on 8 June 2017, has provided the Bundeskartellamt with the capacity to conduct sector inquiries in order to detect consumer law infringements. See Press release Bundeskartellamt, 'New Decision Division for Consumer Protection - The 9th Amendment To The German Competition Act Confers New Competences Upon The Bundeskartellamt', 12 June 2017 <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/12_06_2017_Abteilung%20V.html?nn=3591568> accessed 31 August 2018.
- 4 Press release Bundeskartellamt, 'Bundeskartellamt Launches Sector Inquiry into Comparison Websites', 24 October 2017 <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/24_10_2017_Vergleichsportale.html> accessed 31 August 2018.
- 5 Press release Bundeskartellamt, 'Bundeskartellamt Launches Sector Inquiry into Smart TVs', 13 December 2017 <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/13_12_2017_SU_SmartTV.html?nn=3591286> accessed 31 August 2018.
- 6 Case No M.8228 *Facebook/WhatsApp*, 17 May 2017, C(2017) 3192 final.
- 7 For an overview, see Nicolo Zingales, 'Between a Rock and Two Hard Places: WhatsApp at the Crossroad of Competition, Data Protection and

Consumer Law' (2017) 33 Computer Law & Security Review 553, 554–5–55.

- 8 See for instance the letter of the art 29 Working Party to WhatsApp of 24 October 2017 <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47964> accessed 31 August 2018.
- 9 Press release Hamburg Commissioner of Data Protection and Freedom of Information, 'Higher Administrative Court Confirms the Prohibition of Data Sharing between WhatsApp and Facebook', 2 March 2018 <https://datenschutz-hamburg.de/assets/pdf/Press_Release_2018-03-02_Higher_Administrative_Court_Facebook.pdf> accessed 31 August 2018.
- 10 Press release UK Information Commissioner, 'A Win for the Data Protection of UK Consumers – Whatsapp Signs Public Commitment Not To Share Personal Data With Facebook Until Data Protection Concerns Are Addressed', 14 March 2018 <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/>> accessed 31 August 2018.
- 11 Statement von Klaus Müller, Vorstand des vzbv, 'vzbv verklagt WhatsApp: Verbraucher müssen Hoheit über Daten behalten', 30 January 2017 <<https://www.vzbv.de/pressemitteilung/vzbv-verklagt-what-sapp-verbraucher-muessen-hoheit-ueber-daten-behalten>> accessed 31 August 2018.

inclusion of unfair terms, including forcing users to subscribe to new terms and conditions by making them believe that otherwise they would not have been able to continue using the service.¹²

Despite all these efforts by competition, data protection, and consumer protection agencies in various Member States, no solution has surfaced that addresses the widely felt underlying concerns relating to the transparency of, the control over and the accountability for the use of personal data by key players in digital markets. Such concerns transcend the individual competences of the various authorities and require more coherent enforcement actions. Against this background, the article outlines concrete instances where competition, data protection, and consumer law can be applied more coherently and where the relevant authorities can collaborate more closely in order to achieve a better protection of consumer interests. By giving recommendations that can be implemented in investigations in practice, the article aims to contribute to existing work that analyses the relationship between, respectively, competition and data protection law¹³ as well as consumer and data protection law¹⁴ in more abstract terms. As such, the article fits with the spirit of the Digital Clearinghouse as initiated by the EDPS in September 2016¹⁵ and as endorsed by the European Parliament in March 2017.¹⁶ The Digital Clearinghouse is a voluntary network of authorities and aims to offer a platform to facilitate cooperation, dialogue, and exchange of best practices so as to achieve a coherent enforcement of legal regimes protecting the interests of individuals in digital markets.¹⁷

Building upon our previous work,¹⁸ we rely on the notion of fairness as a common feature across the three legal frameworks as a basis to create a more coherent enforcement and to align substantive protections in an effective way. After all, as noted by the European Data Protection Supervisor '[a] number of practices in digital markets may infringe two or more applicable legal frameworks, each of which is underpinned by the notion of "fairness".'¹⁹ While consumer law principles are considered where relevant, most of the analysis presented in this article relates to the interaction between competition and data protection law. After describing the role of fairness in the three regimes, attention is paid to substantive overlaps in terms of the underlying principles of each regime as well as enforcement synergies and tensions as regards interaction between the different enforcement mechanisms.

Fairness as an overarching principle

Naturally, the overlaps between the fields of competition, consumer and data protection as regards their substantive principles are particularly apparent in relation to practices involving the collection and use of personal data of individuals. The processing of personal data triggers the application of EU data protection rules including the GDPR.²⁰ At the same time, contract terms and commercial practices relating to the use of personal data have to be in conformity with EU consumer protection requirements as laid down in *inter alia* the Unfair Terms Directive²¹ and the Unfair Commercial Practices Directive.²² Furthermore, companies

- 12 Press release Autorità garante della concorrenza e del mercato, 'WhatsApp fined for 3 Million Euro For Having Forced Its Users To Share Their Personal Data with Facebook', 12 May 2017 <<http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html>> accessed 31 August 2018.
- 13 See in particular Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer Law International, Alphen aan den Rijn 2016); and Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11.
- 14 See in particular Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427; and Dan Jerker B Svantesson, 'Enter the Quagmire – The Complicated Relationship Between Data Protection Law And Consumer Protection Law' (2018) 34 Computer Law and Security Review 25.
- 15 European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016, 15 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf> accessed 31 August 2018.
- 16 European Parliament resolution of 20 February 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, recital R <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//EN>> accessed 31 August 2018.

- 17 For its activities, see <https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en> accessed 31 August 2018.
- 18 Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' in *Yearbook of European Law* (Forthcoming 2018) <<https://papers.ssrn.com/abstract=3013139>> accessed 31 August 2018; Damian Clifford, Inge Graef and Peggy Valcke, 'Pre-Formulated Declarations Of Data Subject Consent – Citizen-Consumer Empowerment And The Alignment Of Data, Consumer And Competition Law Protections' German Law Journal (Forthcoming 2019), CiTiP Working Paper 33/2017, 38–41 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126706> accessed 31 August 2018; and Damian Clifford, 'Data Protection and the Fairness of Commercial Practices', CiTiP Working Paper (Forthcoming 2018).
- 19 European Data Protection Supervisor (n 15) 3.
- 20 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 (GDPR), OJ 2016 L 119/1.
- 21 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Contract Terms Directive), OJ 1993 L 95/29.
- 22 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial

increasingly rely on information extracted about the profile and interests of individuals in order to provide services to consumers as a result of which data has become an economic asset needed to compete on the market. As such, the use of personal data by undertakings may also raise issues under competition law.²³

Defining fairness and the role of the respective notions across the frameworks

The three areas of law complement each other and protect different dimensions of consumer welfare. While data protection law aims to protect autonomous decision-making by data subjects but also more broadly includes the safeguarding of a secure and fair personal data processing environment, consumer protection law empowers individuals to make well-informed autonomous choices. Therefore, although consumer protection and data protection clearly overlap, as data protection applies whenever personal data are processed, it is distinct since it is not solely connected to the protection of an individual's decision making capacity and choices. Competition law, for its part, aims to keep markets competitive so to ensure that consumers have such choices. As such, competition enforcement is vital to protect consumers against distortions of competition but a precondition for the existence of a well-functioning market is that individuals are able to exercise a genuine and informed choice. To that end, the effective implementation and enforcement of information requirements in consumer protection law and conditions for valid consent in data protection law in particular, are key. Competition law thus aims to ensure the availability of choice whereas data protection and consumer protection law aim at effectively empowering individuals exercise such a choice. Hence, competition, data protection and consumer law have to go hand in hand in order to adequately protect consumer interests. This is the coherence that the present article envisages: an effective application and enforcement of the three regimes whereby substantive protections and enforcement actions build upon and strengthen each other, as such protecting the different dimensions of consumer welfare in a unified way.

While the outcome of each of the regimes relates to the various dimensions in which choice needs to be protected, the notion of fairness can be seen as an overarching principle connecting the three fields as to the way in which the protection of choice as the desired outcome is to be achieved. As such, the alignment of the different policy agendas could be based on the notion of fairness. As a starting point for interpreting fairness as a general overarching principle of the fields of competition, data protection, and consumer law, it is worth looking at its dictionary definition. The Oxford Dictionary defines 'fairness' as 'impartial and just treatment or behaviour without favouritism or discrimination'.²⁴ Similarly, the Cambridge Dictionary refers to 'the quality of treating people equally or in a way that is right or reasonable'.²⁵ While the use of open terms like 'discrimination', 'just', and 'reasonable' may not provide much clarity on the exact requirements for something to be fair, it is at least clear from these dictionary definitions that fairness consists of a number of facets. This already indicates that fairness requires different forms of protection and as such calls for the parallel application of several legal regimes. Although fairness plays a role in all three regimes, its relevance and interpretation is different in each.

The European Data Protection Supervisor (EDPS) has positioned the fairness principle in data protection as a 'core' principle alongside the lawfulness and transparency principles.²⁶ Despite this 'core' status however, fairness is often dealt with in somewhat of a shorthand manner. As suggested elsewhere,²⁷ a division can be made between procedural fairness and fair balancing. These elements run concurrently throughout the operation of the GDPR and owe their foundations to the Charter of Fundamental Rights of the EU. Accordingly, the procedural fairness and fair balancing elements of the fairness principle manifest themselves in the secondary framework of the GDPR as a system of fairness check and balances. As such, the procedural fairness element is comprised of three components; transparency, timeliness, and burden of care, whereas fair balancing is comprised of two; proportionality and necessity, owing their origins to the fundamental rights and freedoms balancing at the core of data protection law. Fair balancing manifests itself in the form of both *ex ante* (ie the

practices in the internal market (Unfair Commercial Practices Directive), OJ 2005 L 149/22.

23 Competition Commissioner Vestager argued in this regard: 'If a company's use of data is so bad for competition that it outweighs the benefits, we may have to step in to restore a level playing field.' See Speech Commissioner Vestager, 'Competition in a Big Data World', DLD 16 Munich, 17 January 2016 <https://ec.europa.eu/commission/commis-sioners/2014-2019/vestager/announcements/competition-big-data-world_en> accessed 31 August 2018.

24 See <<https://en.oxforddictionaries.com/definition/fairness>> accessed 31 August 2018.

25 See <<http://dictionary.cambridge.org/dictionary/english/fairness>> accessed 31 August 2018.

26 European Data Protection Supervisor (n 15) 8.

27 Clifford and Ausloos (n 18).

conditions for lawful personal data processing) and *ex post* (ie data subject rights) micro fair balancing mechanisms. In contrast, procedural fairness refers to the formal or process orientated requirements and, as argued elsewhere, is an indirect horizontal manifestation of the right to fair administrative procedure provided for in Article 42 of the Charter which requires that peoples' affairs are handled 'impartially, fairly and within a reasonable time'.²⁸ Given that impartiality is impossible in the context of personal data processing (ie due to the fact that it is the controller who determines the purpose and means of the processing), through the application of the accountability principle controllers are responsible for their own compliance, must provide evidence of their compliance and are thus left with the burden of proof to justify that their actions are in compliance with the fairness principle. The accountability principle is therefore an overarching principle vis-à-vis the practical operation of data protection. This is reflected in the effective implementation of the fairness principle given that controller accountability is essentially manifested in the burden of care component.

Similarly, fairness also has a central position in consumer protection law. Under the Unfair Terms Directive and the Unfair Commercial Practices Directive, fairness acts as the substantive standard against which the legality of contract terms and commercial practices are tested, respectively. In short, fairness in consumer protection focuses on the decision making capacity of consumers. In the Unfair Terms Directive unfairness consists of substantive elements (including 'good faith' and 'significant imbalance' components to be assessed at the national level) and formal elements (transparency and information provision) as contained in Articles 3–5 of the Directive.²⁹ As observed by Donnelly and White, '[a]lthough the first of these mechanisms has inevitably been the more high profile, it is arguable that the primary weighting of Directive 93/13 is toward the latter mechanism'.³⁰ In this regard, it is important to note that the substantive fairness level does not apply to the 'core' terms (eg such as the price) unless otherwise provided for by national law (see Article 4(2)). This reflects the minimum harmonization approach of the Unfair Terms Directive and

thus the role played by national law in the fairness assessment. In contrast the Unfair Commercial Practices Directive is a maximum harmonization instrument and therefore 'it is unfairness as variously defined in the Directive that determines national regulatory standards—nothing less, but also, nothing more'.³¹ Fairness in the Unfair Commercial Practices Directive is divided into three levels of fairness as provided for in Article 5 of the Directive. On the first level is the general clause which is then expanded into two small general clauses on the second level specifying unfairness protections for misleading and aggressive commercial practices, respectively. Finally, on the third level is a blacklist of practices that are deemed *de facto* unfair. Each of these levels focuses on the average consumer's capacity to make informed autonomous decisions.

Furthermore, Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), the two main EU competition law provisions, also contain references to fairness. One of the requirements under Article 101(3) TFEU to justify restrictive practices is that a 'fair share' of the benefit, namely an improvement in the production or distribution of goods or the promotion of technical or economic progress, resulting from the practice goes to consumers. Article 102(a) TFEU, in its turn, refers to the imposition of 'unfair purchase or selling prices' or 'other unfair trading conditions' as a form of abuse of dominance prohibited under that provision. However, what constitutes 'unfair' in this context remains unclear as the legality of practices under competition law is evaluated on the basis of their anticompetitive nature or effects in the specific circumstances of the case. In other words, there is no single way of defining fairness as it is interpreted differently in different contexts and there are no straightforward criteria to assess the fairness of conduct under competition law.³² Similarly, there are no general criteria against which to test the anticompetitiveness of behaviour considering that each form of abuse under Article 102 TFEU, as well as each type of restrictive practice under Article 101 TFEU for that matter, has its own line of decision making practice and case law setting out the applicable principles.

28 Ibid.

29 Hans-W Micklitz, 'Unfair Terms in Consumer Contracts' in Hans-W Micklitz and others (eds), *European Consumer Law* (2nd edn, Intersentia 2014) 142.

30 Mary Donnelly and Fidelma White, *Consumer Law: Rights and Regulation* (Thomson Round Hall 2014) 239.

31 Chris Willett, 'Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive' (2010) 33 *Journal of Consumer Policy* 247, 252.

32 For a good analysis, see Pinar Akman, *The Concept of Abuse in EU Competition Law: Law and Economic Approaches* (Hart Publishing 2012) 146–57. With regard to fairness of trading conditions in digital markets, see Harri Kalimo and Klaudia Majcher, 'The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace' [2017] *European Law Review* 210, 223–28.

As such, the role of fairness in competition law is less explicit than in the regimes of data protection and consumer law. Rather than a substantive benchmark, fairness can be regarded as an inherent objective or outcome of competition enforcement. By intervening against anticompetitive practices, EU competition law protects the competitive process in the internal market³³ to the benefit of consumers, competitors, and the economy as a whole. In this manner, competition enforcement thus contributes to a fairer society.³⁴ Fairness can also be regarded as constituting part of the notion of ‘competition on the merits’ that is used to distinguish ‘normal’ competitive behaviour on the basis of price, quantity, quality, choice, and innovation from conduct that restricts competition.³⁵ In this sense, when markets work fairly, businesses compete on the merits.³⁶ Apart from this more fundamental role of fairness in competition law, procedural fairness plays a role in the context of the right to good administrative procedure in the form of, for instance, an undertaking’s right to be heard, right to defence, right to protection of business secrets and right to judicial review that have to be respected by competition authorities while conducting competition investigations.³⁷

Interestingly however, despite its seemingly more implicit function, fairness is currently playing a key role in discussions about the objectives of competition policy. Competition Commissioner Vestager increasingly refers to the importance of markets working fairly in her public statements. In a September 2016 speech, she argued that: ‘competition enforcement also sends a message of fairness. That public authorities are here to defend the interests of individuals, not just to take care of big corporations.’³⁸ Similarly, in a March 2018 speech, she stated that ‘competition policy also reflects an idea of

what society should be like’, namely ‘the idea of a Europe that works fairly for everyone’.³⁹ In her view, competition policy helps to build a fair society:

Because we know that competition gives consumers the power to demand a fair deal. To shop around to find a better price, or a wider choice of products. To seek out better quality, whatever that means to them – whether it’s a more reliable car, or a social network that protects their private data better.⁴⁰

As such, the notion of fairness is mainly used to describe the underlying rationale of competition enforcement and its rise in competition policy discussions does not change the substance of the competition rules. In the words of the Commissioner:

We don’t need to replace the whole system of rules that lawyers and economists have developed over two generations. We don’t need a new rule of fairness in our system. Because fair markets are just what competition is about.⁴¹

Furthermore:

That doesn’t mean that we at the Commission see ourselves as superheroes, solving all unfairness, and righting every wrong. It doesn’t mean that just because something is unfair, it’s automatically also against the competition rules. All it means is that simply by doing our job – simply by enforcing the competition rules in our Treaty – we do our bit to make Europe a fairer place to live.⁴²

While these references to fairness thus do not expand the reach of the competition rules, an explicit recognition of fairness as an inherent objective or outcome of competition enforcement does emphasize that competition law is about protecting consumers and needs to be applied alongside other regimes to achieve its objective to create a fairer society.

33 As Protocol 27 on the internal market and competition makes clear: ‘the internal market as set out in Art 3 of the Treaty on European Union includes a system ensuring that competition is not distorted’.

34 Alfonso Lamadrid de Pablo, ‘Competition Law as Fairness’ (2017) 8(3) *Journal of European Competition Law and Practice* 147, 147–48.

35 See for instance *Post Danmark I*, Case C209/10, [2012] ECLI:EU:C:2012:172, para 25: art 102 TFEU ‘prohibits a dominant undertaking from, among other things, adopting pricing practices that have an exclusionary effect on competitors considered to be as efficient as it is itself and strengthening its dominant position by using methods other than those that are part of competition on the merits’.

36 See the quote of Commissioner Vestager referred to in the speech of Director General Laitenberger, ‘EU competition law in innovation and digital markets: fairness and the consumer welfare perspective’, MLex / Hogan Lovells event Brussels, 10 October 2017, 5 <http://ec.europa.eu/competition/speeches/text/sp2017_15_en.pdf> accessed 31 August 2018.

37 For a good overview, see the contributions in Paul Nihoul and Tadeusz Skoczny (eds), *Procedural Fairness in Competition Proceedings* (Edward Elgar 2015).

38 Speech Commissioner Vestager, ‘Competition for a Fairer Society’, 10th Annual Global Antitrust Enforcement Symposium Georgetown, 20 September 2016 <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-fairer-society_en> accessed 31 August 2018.

39 Speech Commissioner Vestager, ‘Fair markets in a Digital World’, Danish Competition and Consumer Authority, Copenhagen, 9 March 2018 <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/fair-markets-digital-world_en> accessed 31 August 2018.

40 Speech Commissioner Vestager, ‘Fairness and Competition’, GCLC Annual Conference, Brussels, 25 January 2018 <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/fairness-and-competition_en> accessed 31 August 2018.

41 Speech Commissioner Vestager (n 39).

42 Speech Commissioner Vestager (n 40).

Fairness and accountability—bolstering decision making capacity and the enforcement lacuna

The fact that fairness also plays a role in competition law, be it more implicit as underlying rationale of competition enforcement rather than a substantive benchmark, shows the normative commonalities of the regimes of competition, data protection, and consumer law. As such, the notion of fairness may form the basis for a better alignment of substantive requirements as well as enforcement actions between the three fields as illustrated below. This is all the more important in practice where market players often operate at the interface of competition, data protection, and consumer law, and their commercial practices blur the boundaries between these distinct but related regimes.

Moreover, data protection, consumer, and competition law enforcement authorities are clearly conscious of the need for broader citizen-consumer protection given the increasing overlap in the enforcement remit of the relevant authorities. As analysed elsewhere,⁴³ this overlap is specifically evident in the explicit reference to the Unfair Terms Directive in Recital 42 GDPR which specifies that pre-formulated declarations of data subject consent should not contain unfair terms. In addition to the possible role of the Unfair Terms Directive in data protection, there is increasing discussion in relation to the application of the Unfair Commercial Practices Directive in the context of personal data processing. However, in contrast to the Unfair Terms Directive there is no explicit reference to the Unfair Commercial Practices Directive in the GDPR. That being said (and as highlighted in the ‘Introduction’ section), national consumer protection authorities are increasingly relying on the application of the Unfair Commercial Practices Directive to assess the fairness of personal data gathering in terms of the legitimacy of consumer consent. Aside from these consent-focused enforcement actions, there is also a growing body of literature suggesting the potential application of the Unfair Commercial Practices Directive to mitigate the effects of personalization and thus to bolster the *ex post* protections provided for in the GDPR by focusing on the effects on the decision making capacity of the average consumer.⁴⁴

As regards the role of competition enforcement in the context of personal data processing, the use of competition principles seems particularly promising in interpreting the scale of controller and processor obligations under data protection law. Competition concepts of market definition and market power could be applied in line with the risk-based approach of the GDPR. The stronger the market position of a data controller or processor, the more risk the processing activities can be regarded to entail for the individual’s fundamental right to data protection. Unlike competition law, data protection law is not concerned with scale as such in the sense that a breach of data protection rules can be equally damaging to the interests of individual data subjects irrespective of the market position of the firm and the size of the data set or the processing activities. However, the GDPR does take into account the level of risk of a certain form of processing in such a way that more detailed obligations will apply to controllers where the risk of processing is higher. For example, ‘the risks of varying likelihood and severity for the rights and freedoms of natural persons’ play a role in determining to what extent the controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the applicable rules under Article 24(1) GDPR. While no formal distinction is made on the basis of scale or size under EU data protection law, the risk that particular processing activities may bring about can thus be considered as a relevant factor in establishing, respectively, the scale of its obligations under the GDPR and the impact of its processing activities on the rights of the data subject. This resembles, at least to a certain extent, the well-established principles of market definition and market power in competition law. As such, data protection authorities could draw upon assessments of competition authorities that determine the strength of particular data controllers on the market in order to implement a proper risk-based approach to data protection.

Reference can also be made to the special responsibility of a dominant firm under Article 102 TFEU. This concept entails that irrespective of how it has obtained its dominant position, the undertaking has a ‘special responsibility not to allow its conduct to impair genuine

43 Clifford, Graef and Valcke (n 18).

44 See for instance Gianclaudio Malgieri and Giovanni Comandè, ‘Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation’ (2018) 7 International Data Privacy Law 23; Damian Clifford, ‘Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?’ <<https://papers.ssrn.com/abstract=3037425>> accessed 31 August 2018; Damian

Clifford and Valerie Verdoodt, ‘Integrative Advertising: The Marketing “Dark Side” or Merely the Emperor’s New Clothes?’ (2017) 8 European Journal of Law and Technology <<http://ejlt.org/article/view/547>> accessed 31 August 2018; Valerie Verdoodt, Damian Clifford and Eva Lievens, ‘Toying with Children’s Emotions, the New Game in Town? The Legality of Advergaming in the EU’ (2016) 32 Computer Law and Security Review 599.

undistorted competition on the common market'.⁴⁵ The Bundeskartellamt also seems to incorporate the special responsibility that dominance brings about in its reasoning underlying the *Facebook* investigation. The authority is of the view that when operating its business model Facebook 'as a dominant company, must consider that its users cannot switch to other social networks'.⁴⁶ More specifically, the president of the Bundeskartellamt stated that: 'Dominant companies are subject to special obligations. These include the use of adequate terms of service as far as these are relevant to the market.'⁴⁷

Competition law reasoning could thus be used to interpret key data protection concepts like fairness and accountability. In this sense, the stronger the position of the data controller or processor and thus the less chance for data subjects to rely on another controller or processor, the stricter the principles of fairness and accountability would need to be applied to adequately protect the interests of data subjects.⁴⁸ With regard to the interpretation of the concept of consent, this logic would imply that the existence of market power in a competition law sense may act as an indicator challenging the validity of consent as a legitimate ground for processing of personal data. After all, one can doubt whether consent is to be considered freely given in the presence of market power pointing to, following the wording of recital 43 GDPR, 'a clear imbalance between the data subject and the controller'.⁴⁹ An analogy with competition analysis is useful as one must acknowledge that it is hard to imagine situations without any imbalance in a B2C context. Indeed, data protection law is inherently founded on the premise of redressing power asymmetries and therefore, the enforcement of data protection law may increasingly incorporate the market strength of controllers and processors when deciding on the scale of the obligations incumbent on them.

However, despite the above moves towards alignment, there are clear question marks regarding the precise significance of the separation between the policy agendas and how this differentiation manifests itself in terms of substantive requirements. This is particularly significant *vis-à-vis* the data protection-consumer protection overlaps. Indeed, as discussed elsewhere, it is

questionable whether much of the alignment discussion is in fact fuelled by an apparent enforcement lacuna rather than a lack of substantive requirements *per se*.⁵⁰ In this regard it is significant to note that the standard of protection appears to be higher in data protection. Here one can refer to the seemingly stronger protections provided for in Article 7 GDPR, which stipulates the conditions for consent, to be contrasted with the average consumer standard at the root of consumer protection, but also to the fact that the GDPR's protections apply beyond the operation of the assessment of the fairness of consent. To clarify, data protection applies whenever personal data are processed. As such, the GDPR aims to ensure a fair personal data processing environment through the fair balancing of the rights and interests of the data subject, the controller and third parties via a series of checks and balances. In this manner the GDPR aims to provide a higher level of protection, less focused on transparency and more on a secure personal data processing ecosystem. Moreover, the proposed reform of the consumer acquis also arguably gives rise to apparent inconsistencies with the GDPR and in this regard it is significant to refer to the proposed Digital Content Directive.⁵¹ This proposal presents a number of concerns from a data protection and privacy perspective given the (ie either explicit or implicit depending on the version) positioning of personal data as counter-performance and the distinction between 'active' and 'passive' personal data provision. As a consequence, it is suggested that consumer protection policy and enforcement authorities are in fact responding to a societal need that is not being met by data protection authorities. Accordingly, these enforcement actions are not being driven by a substantive lacuna but rather an apparent enforcement one.

In particular, the effective implementation of the fairness principle in the data protection context, and thus the correct operation of the fairness components (ie necessity and proportionality and timeliness, transparency and burden of care), is dependent on effective enforcement. It is arguable that the shift to a risk-based approach and the resulting increased focus on the accountability of the data controller in the GDPR may be

45 See for instance *NV Nederlandsche Banden Industrie Michelin tegen Commissie (Michelin I)*, Case 322/81, [1983] ECLI:EU:C:1983:313, para 57.

46 Bundeskartellamt (n 2).

47 Press Release Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules', 2 March 2016.

48 See also Zingales (n 7) 553, 557–58 for a discussion of how two decisions taken by the *Autorità garante della concorrenza e del mercato* (Italian

competition and consumer authority) in May 2017 imposing a fine of 3 million euro on WhatsApp for alleged unfair commercial practices indicate the relevance of competition and data protection considerations in consumer law.

49 For a more elaborate analysis, see Clifford, Graef and Valcke (n 18).

50 Clifford (n 18).

51 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final.

problematic.⁵² The increased importance placed on risk and the accountability principle reflects the finite nature of regulatory resources and the reliance on industry (ie the implementation of self- and co-regulatory mechanisms), enforcement agencies as well as individuals in order to hold companies to account. Such an approach however, assumes that (i) businesses will act fairly with adequate enforcement and (ii) individuals are capable of 'control' and thus playing the role of the active market participant.⁵³ The first assumption reflects the positioning of industry in the implementation of the data protection requirements and presents clear concerns in terms of their capacity or indeed willingness to adequately cater for the intangible harms targeted by the data protection framework. The second assumption is based on the premise that individuals are capable of playing the active market participant and thus holding businesses to account. However, behavioural law and economics research indicating bounded data subject rationality raises clear concerns in this regard. Information overload, or rather the failure of privacy policies to inform data subjects effectively, the multiplicity of requests for consent and the 'stickiness' of defaults dilute the value of data subject participation.⁵⁴ Fairness acts as an overarching principle (and arguably a collective notion of control)⁵⁵ aimed at ensuring more effective individual control (ie via fair balancing and procedural fairness). Given the difficulties in terms of adequately appreciating risk and enforcement, the assumption that individuals are capable of control may not hold up, thereby further undermining the reliance on rationality. Therefore, it is clear that the effective implementation of the fairness principle in the GDPR rests in the hands of controllers.

Similar concerns are valid in the consumer protection context given the focus on the average consumer standard and thus the autonomous decision making capacity of individuals. Indeed, as argued elsewhere, such concerns may even be accentuated in consumer

protection given that the GDPR via the fairness and accountability principles seemingly imposes higher standards of protection.⁵⁶ This is also illustrative of the differentiation between the fundamental rights foundations of the GDPR and the more economically driven consumer protection framework. Irrespective of such substantive requirement comparisons however, it also is questionable whether consumer protection in its current form is truly capable of filling the apparent enforcement gap. Indeed, with reference to the decisions taken by the Italian competition and consumer authority in relation to the fallout from the *Facebook/WhatsApp* merger, it is highly debateable whether a 3 million euro fine is really sufficient to propagate meaningful change. However, in this regard one can also refer to similar actions taken by data protection authorities at the national level and thus their potentially negligible effect. Moreover, although both consumer and data protection authorities have illustrated the capacity to present a united front in the form of the Article 29 Working Party and the Consumer Protection Cooperation Network,⁵⁷ fragmentation is still problematic. Indeed, one should note that the determination of the applicability of the Unfair Commercial Practices Directive to personal data gathering *vis-à-vis* the validity of consent as well as the positioning of personal data as the payment for the provision of the service depends on national law interpretation thereby facilitating divergences.⁵⁸

Despite the fact that the German Courts have accepted that issues relating to the processing of personal data come within the scope of consumer protection (ie as consideration is not required for the formation of a contract), the Berlin Regional Court found that this does not prevent Facebook from positioning itself as a 'free' service. The Court thus found that the Unfair Commercial Practices Directive (as a maximum harmonization Directive) required the payment of a tangible price. In short therefore, the Berlin Court concluded that by advertising itself as 'free', Facebook does not fall

52 For a discussion see generally: Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law* 3.

53 Clifford and Ausloos (n 18).

54 The readiness of data subjects to consent to the surrender their personal data without being aware of the specific purpose indicated (or indeed of the data gathering in the first place) is a good illustration of this point. Despite the fact that reliance on consent as a grounds for personal data processing is questionable (a critique well-founded in literature), there is a continuing move towards empowerment at a policy level. See, Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250, 251.

55 Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12 *SCRIPTed* <<http://script-ed.org/?p=1927>> accessed 31 August 2018.

56 Clifford (n 18).

57 For example, see the March 2017 coordinated action of EU consumer authorities within the Consumer Protection Cooperation Network, under the leadership of the French consumer authority and with the support of the European Commission, urging social media companies Facebook, Twitter and Google+ to comply with EU consumer rules shows the potential of joint efforts to effectively enforce consumer protection law against corporate giants. Press release European Commission, 'The European Commission and Member States Consumer Authorities Ask Social Media Companies to Comply with EU Consumer Rules', 17 March 2017 <http://europa.eu/rapid/press-release_IP-17-631_en.htm>.

58 See, *verbraucherzentrale bundesverband (vzbv) v Facebook* [2018] Landgericht Berlin (Berlin Regional Court) Case no 16 O 341/15. See press release by vzbv, 'Facebook Verstößt Gegen Deutsches Datenschutzrecht | VZBV' <<https://www.vzbv.de/pressemitteilung/facebook-verstoest-gegen-deutsches-datenschutzrecht>> accessed 31 August 2018.

foul of the requirement to identify commercial communications (see point 20 of Annex 1 to the Unfair Commercial Practices Directive) as contracts for such services do not involve the payment of a tangible ‘price’. Therefore, this judgment seemingly precludes the application of protections as the Court refused to recognize that personal data have an economic value within the meaning of the Directive. This case illustrates an interesting distinction and the important role played by the national courts and indeed national contract law. In this regard, it is interesting to refer to common law jurisdictions where consideration or some form of value exchange is necessary for the formation of a valid contract. EU consumer protection is therefore clearly linked to contract and contract is strongly linked to national traditions.⁵⁹

Building on the above, it is important to note that the GDPR aims to respond to concerns relating to the effectiveness of data protection enforcement via *inter alia* the provision of the availability of higher fines, the one-stop-shop enforcement mechanism and the establishment of the European Data Protection Board (which aims to provide a more cohesive enforcement landscape—see a discussion of Article 56(6) GDPR in Section ‘Enforcement synergies and tensions’). Therefore, stating that data protection enforcement is inadequate before the GDPR actually comes into effect is perhaps pre-mature. That being said, data protection enforcement has been clearly challenging and it is this enforcement gap which certain consumer protection authorities have aimed to fill. However, given the substantive delineations such moves should be viewed with caution albeit there is nothing preventing concurrent application and enforcement. Moreover, although outside the focus of this article, it is important to note the

recent proposed reforms of the EU consumer protection acquis and in particular the proposal for a Directive on representative actions for the protection of the collective interests of consumers.⁶⁰

A similar development has arguably taken place as regards the interaction of data protection with competition enforcement. In its 2014 Preliminary Opinion on ‘Privacy and competitiveness in the age of big data’, the EDPS called upon the European Commission to enforce the competition rules strictly in order to increase the level of data protection offered by market players.⁶¹ In this regard, it is mainly the strength of competition enforcement rather than its substantive principles that has caused this attention. Indeed, in recent years the European Commission has shown itself capable of forcing big market players like Microsoft,⁶² Apple,⁶³ Intel,⁶⁴ Google,⁶⁵ and Qualcomm⁶⁶ to comply with the competition rules. Competition law can be regarded as one of the strongest branches of EU law considering *inter alia*, the possibility of imposing relatively high fines amounting to a maximum of 10 per cent of a company’s worldwide turnover,⁶⁷ the wide range of investigation powers of competition authorities including the competence to conduct inspections of private homes⁶⁸ and the national transpositions of Directive 2014/104⁶⁹ that aims to ensure that anyone who has suffered harm from a competition law infringement by an undertaking can effectively exercise the right to claim full compensation from that undertaking under national law.

From an institutional perspective, the main difference of the enforcement of data protection and consumer law with that of competition law is that for the first two regimes there is no authority at the EU level that has the competence to take action and adopt measures having an effect on the EU territory as a whole.

59 For more see, Clifford (n 18).

60 Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, Brussels, 11.4.2018 COM(2018) 184 final 2018/0089(COD).

61 Preliminary Opinion of the European Data Protection Supervisor, ‘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 <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf> accessed 31 August 2018.

62 Case COMP/C-3/37.792—*Microsoft*, 24 March 2004 (prohibition decision involving a refusal to share interoperability information with competitors and the tying of Windows Media Player to the Windows operating system); Case COMP/C-3/39.530—*Microsoft (Tying)*, 16 December 2009 (commitment decision involving the tying of Microsoft Internet Explorer to the Windows operating system); and Case AT.39530—*Microsoft (Tying)*, 6 March 2013 (fining Microsoft for not complying with the 2009 commitment decision).

63 In 2012 and 2013, the Commission accepted commitments from Apple and a number of publishers to address concerns arising from a concerted practice aimed at raising retail prices for e-books. See the case

file on http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39847.

64 Case COMP/37.990—*Intel*, 13 May 2009 (prohibition decision involving conditional rebates and payments in the market for x86 central processing units). In September 2017, the Court of Justice set aside the 2014 judgment of the General Court upholding the Commission decision and referred the case back to the General Court to examine in the light of Intel’s arguments whether the rebates at issue are capable of restricting competition (*Intel*, Case C-413/14 P, [2017] ECLI:EU:C:2017:632).

65 Case AT.39740—*Google Search (Shopping)*, 27 June 2017.

66 Press release European Commission, ‘Antitrust: Commission Fines Qualcomm €997 Million for Abuse of Dominant Market Position’, 24 January 2018 <http://europa.eu/rapid/press-release_IP-18-421_en.htm> accessed 31 August 2018.

67 Art 23(2) of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in arts 81 and 82 of the Treaty (Regulation 1/2003), OJ 2003 L1/1.

68 Art 21 of Regulation 1/2003.

69 Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the EU, OJ 2014 L 349/1.

Unlike the competition enforcement mechanism which consists in joint application and enforcement of the EU competition rules by the European Commission and national competition authorities,⁷⁰ the enforcement of data protection and consumer law solely takes place at the national level which leads to additional complexities in terms of coordination and cooperation. All of this may explain why data protection advocates like the EDPS have started to look at competition law as a source of inspiration for creating stronger enforcement of data protection law as well.⁷¹ In terms of substantive principles, competition and data protection law can equally complement each other as discussed in the next section.

Substantive overlaps and inspiring competition law enforcement

Despite the partial overlap in objectives of the regimes of competition, data protection, and consumer law, their respective rules and principles are typically still applied in isolation from each other even though a particular type of behaviour may raise issues under more than one legal framework. As a result, there is room to apply the different regimes in a more coherent way to achieve a better protection of consumers. The overlap that has so far received most attention is how competition enforcement can render data protection rules more effective by increasing competition in concentrated markets and by facilitating genuine consumer choice.⁷² However, one should note that a high level of concentration in itself is not a reason for competition authorities to intervene in a market. After all, it is the abuse of a dominant position that is prohibited under Article 102 TFEU, not the existence of dominance itself. The application of competition law is thus only triggered in the presence of actual, proven competition problems. As such, the role of competition enforcement is not to change market structures, to decide on the best business model or to impose particular products or services on consumers. To the contrary, it is the task of competition

authorities to maintain competitive conditions on the market thereby enabling consumers to make such choices themselves and to transact with the companies of their own liking. This does not mean that there are no substantive overlaps between competition and data protection law, but it needs to be emphasized that there are limits to what can be achieved by way of competition enforcement. Furthermore, competition enforcement can also benefit from incorporating principles from data protection and consumer law into its analysis.

Data protection and consumer law principles as benchmarks for exploitative abuse

Most of the debate on the interface between competition and data protection law has so far focused on how data protection interests can be integrated into competition analysis and how competition enforcement may thereby strengthen compliance with data protection law.⁷³ However, the use of data protection principles in competition cases can also boost competition enforcement. The *Facebook* investigation of the Bundeskartellamt illustrates the complementarity of the two regimes that is based on the unfairness of conditions as a form of exploitative abuse of dominance under Article 102(a) TFEU.

Strengthening data protection consent through the regime of abuse of dominance

In March 2016, the Bundeskartellamt launched an investigation into Facebook's terms of service to examine whether consumers are sufficiently informed about the type and extent of personal data collected. The Bundeskartellamt suspects that Facebook's terms of service are in violation of data protection law and could thereby also constitute abuse of dominance under competition law by representing an abusive imposition of unfair conditions on users.⁷⁴ The investigation forms a first attempt by a competition authority to integrate data protection interests into competition analysis. The investigation seems to be premised on the view that

70 Art 3(1) of Regulation 1/2003 provides that national competition authorities should also apply arts 101 and 102 TFEU to, on the one hand, agreements, decisions by associations of undertakings or concerted practices which may affect trade between Member States and, on the other hand, abuses prohibited by art 102 TFEU. With respect to the cooperation between the European Commission and the national competition authorities, art 11(6) of Regulation 1/2003 states that the initiation of a competition law proceeding by the Commission relieves the competition authorities of the Member States of their competence to apply arts 101 and 102 TFEU. In addition, art 13(1) of Regulation 1/2003 lays down that once one competition authority is dealing with a particular competition issue under art 101 or 102 TFEU, this shall be sufficient grounds for the others to suspend proceedings or to reject a complaint against the same agreement, decision of an association or practice.

71 As initiated by the Preliminary Opinion of the European Data Protection Supervisor (n 61).

72 See for instance Christopher Kuner, Fred H Cate, Christopher Millard and others, 'When Two Worlds Collide: The Interface Between Competition Law And Data Protection' (2014) 4(4) *International Data Privacy Law* 247, 247.

73 See in particular the Preliminary Opinion of the European Data Protection Supervisor (n 61).

74 Press Release Bundeskartellamt (n 47). <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568> accessed 31 August 2018.

principles from data protection law can be used as benchmarks for assessing whether certain exploitative behaviour of a dominant firm should be considered anticompetitive under Article 102 TFEU.

In December 2017, the Bundeskartellamt reached the preliminary assessment that Facebook's collection and use of data from third-party sources is abusive. According to the Bundeskartellamt, Facebook is abusing its dominant position by making the use of its social network conditional on it being allowed to collect every kind of data generated by using third-party websites and merge it with the user's Facebook account. Considering that users are only given the choice of either accepting the 'whole package' or not being able to use Facebook, the Bundeskartellamt takes the view that it cannot be assumed that users effectively consent to this form of data collection and processing. The Bundeskartellamt qualifies the terms of service of Facebook as inappropriate and a violation of data protection provisions. In the authority's assessment, consumers must be given more control over processes whereby data are transmitted from websites and apps to Facebook, and Facebook needs to provide consumers with suitable options to effectively limit this collection of data.⁷⁵

As such, a possible intervention by the Bundeskartellamt on the basis of competition law could help alleviate data protection concerns. The specific benchmark relied upon by the Bundeskartellamt to establish anticompetitive conduct under the abuse of dominance regime seems to be the validity of consent under data protection law. In particular, the main focus of the investigation seems to be whether the consent given by Facebook users is sufficiently informed as required by Article 4(11) GDPR. Depending on how the investigation will evolve, the Bundeskartellamt may set a new precedent under which competition enforcement also has a role to play in preventing exploitation of consumers by dominant firms through the imposition of unfair conditions regarding the processing of personal data. As the investigation seems to focus on the requirement of consent to be informed, a possible competition intervention of the Bundeskartellamt may result in a welcome strengthening of this key data protection principle.

Boosting competition enforcement by incorporating data protection principles

At the same time, the use of principles from data protection law as benchmarks for analysing whether abuse of dominance under competition law exists can also bolster the enforcement capabilities of competition authorities. Currently, competition authorities rarely challenge behaviour that directly harms individuals and instead focus on addressing conduct of dominant firms leading to the foreclosure of competitors.⁷⁶ Within abuse of dominance, a distinction is made between exclusionary and exploitative abuse. Exclusionary abuse consists of conduct that drives competitors from the market thereby indirectly harming consumers through higher prices, limitations of quality or reduced choice. Exploitative abuse involves direct harm to consumers in the form of, for instance, excessive prices and is based on Article 102(a) TFEU that prohibits the imposition of 'unfair purchase or selling prices or other unfair trading conditions'. The cautious approach towards addressing exploitation under competition law can be explained by the belief in the self-correcting nature of the market that may mitigate harmful effects of exploitative behaviour by dominant firms in the longer term. The idea is that as long as markets remain competitive, consumers can switch suppliers and choose an offer that provides them with a fairer deal.

In the words of Competition Commissioner Vestager, 'sometimes, a company is dominant simply because it's better than its competitors. And when that's the case, it's only fair that it should get the reward of its efforts'. There is a need to prevent 'competition authorities taking the place of the market' as a regulator, 'deciding on the right price' in the context of possible competition interventions against excessive pricing. As such, '[t]he best defence against exploitation remains the ability to walk away' and consumers can often be protected 'just by stopping powerful companies from driving their rivals out of the market.'⁷⁷ However, due to markets becoming increasingly concentrated and new technologies giving businesses unprecedented possibilities to track and monitor individual preferences, exploitative practices that enable companies to increase profits at the expense of consumers are on the rise. As a

⁷⁵ Bundeskartellamt (n 2).

⁷⁶ The Guidance Paper on enforcement priorities under art 102 TFEU focuses only on exclusionary abuse. See Communication from the Commission—Guidance on the Commission's enforcement priorities in applying art 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (Guidance Paper), OJ 2009 C 45/7, para 7.

⁷⁷ Speech Commissioner Vestager, 'Protecting Consumers from Exploitation', Chillin' Competition Conference Brussels, 21 November 2016 <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/protecting-consumers-exploitation_en> accessed 31 August 2018.

result, there is a need for more proactive approaches to address anticompetitive effects of consumer exploitation under competition law. By incorporating principles from other regimes such as data protection and consumer protection law into competition analysis, difficulties to establish at what point a certain type of exploitative behaviour becomes anticompetitive can be overcome.⁷⁸ Such an approach would then also strengthen the ability of competition authorities to address new forms of anticompetitive behaviour in digital markets. As exploitative abuses are inherently linked to 'fair' prices and other trading conditions under Article 102(a) TFEU, the incorporation of benchmarks from data protection law to determine the anticompetitiveness of such practices under competition law could be based on the notion of fairness as a normative underpinning for more coherent enforcement approaches between the two regimes.

Excessive pricing and personal data

In a 2016 speech, Competition Commissioner Vestager argued that while the main focus of competition enforcement is on protecting consumers indirectly by keeping markets competitive, there can be reasons for competition authorities to intervene in cases 'where competition hasn't been enough to provide a real choice' and 'dominant businesses are exploiting their customers, by charging excessive prices or imposing unfair terms'.⁷⁹ As such, one may wonder whether these statements lead to increased attention of the European Commission to exploitative abuses in its enforcement work. Here it is worth noting that the Commission in May 2017 opened its first investigation into concerns about excessive pricing practices in the pharmaceutical industry against the company Aspen Pharma.⁸⁰ However, as consumers typically do not pay a monetary price for online services the question is what could form the basis for claims of exploitative abuse in these markets. In this regard, Competition Commissioner Vestager stated that:

Consumers use search engines that produce incredibly accurate results. Social networks let people keep in touch with friends, wherever they are in the world. And they don't pay a single penny for those services. Instead, they pay with their data. That doesn't have to be a problem, as long as

people are happy that the data they share is a fair price to pay for the services they get in return. Personal data has become a valuable commodity.⁸¹

In line with the positioning of data as a counter performance in the proposal for a Digital Content Directive⁸² (ie either explicitly or implicitly depending on the version), this statement forms another recognition of data operating as an indispensable currency used to compensate providers for the delivery of their services to consumers. Since personal data replaces price as a type of currency in the digital environment, one may wonder whether exploitative abuse could relate to the excessive collection of information about consumers instead of to the monetary price charged for a product or service.⁸³ In other words, if the data shared by individuals with a dominant firm is not 'a fair price to pay for the services they get in return', this might point to the excessiveness of data collection and thus an exploitative abuse under Article 102 TFEU.

In line with the Facebook investigation of the Bundeskartellamt, data protection principles could also be used here to test the excessiveness of a dominant firm's data collection. By extracting personal data beyond what is allowed under data protection law, the firm may try to get more insight into consumer preferences to the detriment of the exploited individuals. For instance, if a firm extracts personal data beyond what is necessary to achieve a particular purpose or keeps it for a period longer than necessary to fulfil this purpose, it is violating the data minimization and purpose limitation principles. Such an infringement of data protection law may in turn also form an indication of whether the extraction of data is excessive and could qualify as exploitative abuse under competition law. This way, substantive data protection principles are used to determine at what point a practice results into unfair competition under Article 102(a) TFEU. Again, the concept of fairness as an overarching principle can constitute the normative underpinning for such complementarity between the two fields.

Misleading privacy policies and consumer law

A similar analogy can be made with regard to the substantive principles used in consumer protection law. In

78 In the data protection context, see also Costa-Cabral and Lynskey (n 13) 33–37.

79 Speech Commissioner Vestager (n 77).

80 Press release European Commission, 'Antitrust: Commission Opens Formal Investigation into Aspen Pharma's Pricing Practices for Cancer Medicines', 15 May 2017 <http://europa.eu/rapid/press-release_IP-17-1323_en.htm> accessed 31 August 2018.

81 Speech Commissioner Vestager, 'Making Data Work For Us', Data Ethics event on Data as Power Copenhagen, 9 September 2016 <<https://ec.eu>

ropa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-work-us_en> accessed 31 August 2018.

82 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final.

83 See Kalimo and Majcher (n 32) 210, 229–31. See also Aleksandra Gebicka and Andreas Heinemann, 'Social Media & Competition Law' (2014) 37(2) *World Competition* 149, 165 who argue that 'an undue increase in the use of personal data may very well be compared to excessive prices'.

speeches, the head of the European Data Protection Supervisor Buttarelli also referred to non-negotiable and misleading privacy policies as constituting a potential form of abuse of dominance.⁸⁴ Here again, it is hard to determine at what point a (change in) privacy policy should constitute exploitative abuse under Article 102(a) TFEU. Article 6(1) of the Unfair Commercial Practices Directive may be of assistance in this regard. According to this provision, a commercial practice has to 'be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct' in relation to one or more of the elements specified in subsections (a) to (g) such as the nature of the product or its main characteristics.

Interestingly, the Court of Justice recognized in *AstraZeneca*, a case targeting the provision of misleading information by a dominant undertaking, that the breach of one area of law can be a factor in deciding that there has been a violation of competition law as well. The *AstraZeneca* case involved a pharmaceutical group which was fined by the European Commission for having provided misleading representations to patent offices which was alleged to form part of an overall strategy designed to prevent or delay market entry of competing generic products. The Court of Justice endorsed the finding of the General Court that representations designed to unlawfully obtain exclusive rights constitute an abuse if it is established that they are actually liable to lead the public authorities to grant the exclusive right applied for.⁸⁵ In this way, the *AstraZeneca* judgment makes clear that the misuse of regulatory procedures is to be regarded as abuse of dominance where such conduct has a potential anticompetitive effect.⁸⁶ In analogy, consumer protection principles could be used to identify misleading privacy policies that restrict competition and thereby constitute abuse of dominance.

This is particularly relevant in Member States where the competition and consumer protection rules are enforced by the same authority like in Italy (Autorità Garante della Concorrenza e del Mercato), the Netherlands (Authority for Consumers & Markets),

Ireland (Competition and Consumer Protection Commission), the UK (Competition & Markets Authority), and Poland (Office of Competition and Consumer Protection—UOKiK). The fact that the two regimes are enforced by one authority implies that the relevant expertise is present to rely on consumer protection principles in order to establish a violation of competition law in cases where this is desirable to enhance the effectiveness of the competition regime.⁸⁷ As misleading privacy policies would constitute exploitative abuse in the form of the imposition of unfair conditions on consumers, the notion of fairness as an underlying principle in both consumer and competition law can again form the normative underpinning to create these synergies between the two regimes.

Use of data protection principles in merger review

Apart from their use as benchmarks to establish the unfairness of conditions as an exploitative abuse under competition law as evidenced by the German *Facebook* investigation, data protection principles are also becoming apparent in merger decisions of the European Commission. Attention is paid here to the role of data protection as a non-price parameter of competition and its potential as a limit on commercial conduct that can preclude competition concerns from arising. While data protection principles are not used here as substantive benchmarks against which to test the anticompetitiveness of practices of dominant undertakings, data protection should in these instances rather be seen as a factor setting the boundaries of the market within which the fairness of competition between market players has to be determined.

Data protection as a non-price parameter of competition

In the *Facebook/WhatsApp* merger decision, the Commission recognized data protection as a potential dimension of competition. According to the Commission, the market investigation showed that the main drivers of competitive interaction between

84 With respect to non-negotiable privacy policies, see speech Buttarelli, 'Privacy and Competition in the Digital Economy', Privacy Platform event: The Digital Economy, Competition and Privacy Brussels, 21 January 2015, 5 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-01-21_speech_GB_EN.pdf> accessed 31 August 2018. As regards misleading privacy policies, see speech Buttarelli, 'Keynote Speech At Joint ERA-EDPS Seminar', workshop Competition Rebooted: Enforcement and personal data in digital markets Brussels, 24 September 2015, 3 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-09-24_ERA_GB_EN.pdf> accessed 31 August 2018.

85 *AstraZeneca AB and AstraZeneca plc v European Commission*, Case C-457/10 P, [2012] ECLI:EU:C:2012:770, paras 106–113.

86 *AstraZeneca AB and AstraZeneca plc*, *ibid* para 112.

87 See also Inge Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets' in Mark-Olivier Mackenrodt and others (eds), *Personal Data in Competition, Consumer Protection and IP Law. Towards a Holistic Approach?* (Springer, Forthcoming 2018), 16–17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881969> accessed 31 August 2018.

consumer communications apps appear to be the functionalities offered and the underlying network or user base.⁸⁸ The Commission noted that a key innovation driver in the context of consumer communications apps is the improvement of the functionalities in order to gain the largest user base. Apart from the reliability of the communications service, an important area of improvement includes privacy and security. Although the importance of privacy and security varies from user to user, these notions are becoming increasingly valued as, in the Commission's view, was shown by the introduction of consumer communications apps specifically addressing privacy and security issues.⁸⁹

In a number of other instances, the Commission also referred to the role of privacy. As regards closeness of competition between Facebook Messenger and WhatsApp, one of the differences between the two consumer communications services that the Commission pointed out related to the privacy policy of Facebook Messenger. Contrary to WhatsApp, Facebook Messenger enables Facebook to collect data regarding its users for the purposes of its advertising activities.⁹⁰ In the context of an assessment of the strength of network effects, the Commission noted that competing consumer communications apps are able to grow despite the existence of network effects, both over time and following disruptions in the market.⁹¹ In this regard, the Commission referred to the outcry after the announcement of WhatsApp's acquisition by Facebook when thousands of users downloaded different messaging platforms because of privacy concerns.⁹² The Commission also found that even though Facebook would in theory be able to introduce targeted advertising on WhatsApp, it might not have the incentive to do so as this 'could create dissatisfaction among the increasing number of users who significantly value privacy and security'.⁹³ Reference is made to Telegram's successful entry in the market (with 35 million monthly active users reached just six months after the launch of the app) which is believed to be primarily due to its new feature of message encryption and to the high number of German users who switched from WhatsApp to

Threema in the 24 hours following the announcement of Facebook's acquisition of WhatsApp.⁹⁴

Despite these multiple references to privacy in its decision, the Commission did not specifically analyse the *Facebook/WhatsApp* transaction in this light, since privacy was only regarded as one of the many parameters of competition applicable to the case along with price, reliability of the communications service, the user base and perceived trendiness of the app.⁹⁵ This was different in the *Microsoft/LinkedIn* merger where the Commission concluded that privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction. The Commission identified a risk that the market for professional social networks would tip in favour of LinkedIn after the transaction.⁹⁶ To the extent that such foreclosure effects would lead to the marginalization of an existing competitor offering a greater degree of privacy protection than LinkedIn, the merger would in the Commission's view 'restrict consumer choice in relation to this important parameter of competition'.⁹⁷ According to the Commission, the results of the market investigation indeed revealed that privacy was an important parameter of competition and driver of customer choice in the market for professional social networks, in line with its findings as regards consumer communications services in *Facebook/WhatsApp*.⁹⁸ Microsoft entered into a number of commitments⁹⁹ to address the competition concerns in the market for professional social networks that were also linked to the impact on privacy as a non-price parameter of competition.

Both the *Facebook/WhatsApp* and *Microsoft/LinkedIn* merger decisions acknowledge the role of privacy or data protection as a dimension on the basis of which market players may compete. A market investigation has to point out whether firms are indeed competing with one another on the level of privacy protection offered or on a more traditional parameter of competition such as price. Apart from a restriction of consumer choice as the Commission relied upon in *Microsoft/LinkedIn*, a lowering of the level of privacy protection

88 Case No COMP/M.7217—*Facebook/WhatsApp*, 3 October 2014, para 86.

89 Ibid para 87.

90 Ibid para 102.

91 Ibid para 132.

92 Ibid fn 79, p 24.

93 Ibid para 174.

94 Ibid paras 174 and 116.

95 Ibid paras 87–90.

96 Case M.8124—*Microsoft/LinkedIn*, 6 December 2016, para 347.

97 Ibid para 350.

98 Ibid fn 330, 77.

99 Microsoft committed: (i) to ensure that PC manufacturers and distributors were free not to install LinkedIn on Windows and to allow users to remove LinkedIn from Windows when preinstalled; (ii) to allow competing providers of professional social networks to maintain current levels of interoperability with Microsoft Office through the Microsoft Office Add-in Program and Office application programming interfaces; (iii) to grant competing providers of professional social networks access to Microsoft Graph, a unified gateway that enables developers to build applications and services that can, subject to user consent, access data (such as contact information, calendar information, email and files) from Microsoft's cloud services. See para 5–16 of Annex I to Case M.8124—*Microsoft/LinkedIn*, 6 December 2016.

can also be regarded as a degradation of quality in line with the *TomTom/Tele Atlas* merger decision. In *TomTom/Tele Atlas*, the Commission assessed the incentives of the merging parties to protect confidential information of customers and noted that ‘confidentiality concerns can be considered as similar to product degradation’.¹⁰⁰ Although the merger dealt with sensitive information of commercial entities and not with personal data of end consumers, the Commission did recognize that the value of a product may decrease due to concerns relating to how customer information is used. The confidentiality concerns assessed in *TomTom/Tele Atlas* concerned information provided by customers of Tele Atlas who purchased the latter’s navigable digital maps in the upstream market in order to integrate the maps into their portable navigation devices which were competing with those of TomTom in the downstream market. During the market investigation, concerns had been expressed that certain categories of confidential information, such as information on future competitive actions and technical information that manufacturers of navigation devices provided to Tele Atlas could be shared with TomTom after the merger.¹⁰¹ The Commission argued that the perceived value of the digital maps for manufacturers of navigation devices would be lower if they feared that their confidential information could be revealed to TomTom.¹⁰² Similarly, a decrease in the level of personal data protection can be regarded as an aspect of product or service quality in the competition analysis.

Data protection as a limit precluding competition concerns from arising

A second and more remarkable way in which data protection principles are being integrated in competition analysis is as legal restrictions that market players have to abide by and thereby limit their ability to engage in anticompetitive behaviour. When assessing the competitive impact of a possible post-merger combination of the data sets relating to online advertising in *Microsoft/LinkedIn*, the Commission as a preliminary remark noted that ‘any such data combination could only be implemented by the merged entity to the extent it is allowed by applicable data protection rules’.¹⁰³ The

relevant data held by each of the merging parties consisted in personal data as it comprised, in the Commission’s words, ‘information about an individual’s job, career history and professional connections, and/or her or his email or other contacts, search behaviour etc. about the users of their services’¹⁰⁴ as a result of which data protection law applied.

In this context, the Commission noted that Microsoft and LinkedIn were at the time of the merger decision (dating from December 2016) subject to relevant national data protection rules, namely those applicable in Ireland where both Microsoft and LinkedIn either had their registered seat or were processing personal data.¹⁰⁵ The applicability of the GDPR from 25 May 2018 would in the Commission’s view ‘further limit Microsoft’s ability to have access and to process its users’ personal data in the future’ since the new rules would strengthen existing rights of data subjects and empower individuals with more control over their personal data through for instance easier access to personal data and the new right to data portability.¹⁰⁶ The Commission then continued its competition analysis on the assumption that a combination of the data sets of Microsoft and LinkedIn would be allowed under the applicable data protection rules.¹⁰⁷ The exact same approach and wording has been used in the *Verizon/Yahoo* merger where a potential combination of data sets relevant for online advertising purposes was also one of the competition concerns investigated by the Commission.¹⁰⁸

In *Microsoft/LinkedIn*, the Commission took the applicability of data protection law into account in two other instances where the ability of the merged entity to foreclose competing providers of both customer relationship management software solutions as well as productivity software was at issue. As regards both relevant markets, the applicability of data protection law was argued to limit Microsoft’s ability to access and undertake any treatment of LinkedIn full data after the merger.¹⁰⁹ As such, the Commission relied on data protection law in order to substantiate its reasoning that the combination of data sets of the two merging parties did not raise competition concerns.¹¹⁰ This belief in the effectiveness of data protection law is probably most apparent in footnote 332.¹¹¹ Even though concerns were raised

100 Case No COMP/M.4854—*TomTom/Tele Atlas*, 14 May 2008, para 274.

101 Ibid paras 253 and 269.

102 Ibid para 274.

103 Case M.8124 (n 96) para 177.

104 Ibid para 176.

105 Ibid para 177.

106 Ibid para 178.

107 Ibid para 179.

108 Case M.8180—*Verizon/Yahoo*, 21 December 2016, para 90.

109 Case M.8124 (n 96) paras 254–255 and 375.

110 For a discussion of such pitfalls, see also O Lynskey, ‘Considering Data Protection in Merger Control Proceedings’, OECD roundtable on non-price effects of mergers, June 2018, paras 13–15 <[https://one.oecd.org/document/DAF/COMP/WD\(2018\)70/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)70/en/pdf)> accessed 31 August 2018.

111 Case M.8124 (n 96) fn 332, 77:

during the market investigation that companies based outside the EEA might be able to try to circumvent the European data protection rules, the Commission argued that it sufficed to say that both LinkedIn and Microsoft remained subject to national laws implementing the European data protection rules after the transaction. As regards LinkedIn to which Irish data protection law applied, the Commission noted that in cases where Irish data protection rules were less restrictive than those in other Member States, the 'newly adopted GDPR is directly applicable and therefore the scope for divergence between Member States' national data protection laws will be reduced, including in their enforcement'.¹¹² This illustrates the strong faith in a future regime that would only start applying about 1.5 years after the merger was approved.

The Commission relied on an even more presumptuous reasoning in its *Google/Sanofi* merger decision. The decision dealt with a joint venture offering services for the management and treatment of diabetes using an integrated digital e-medicine platform. A competitor raised the concern that the joint venture would be able to lock-in patients to its services by limiting or preventing the portability of their data to other platforms.¹¹³ However, the Commission concluded that 'the risk of the JV locking-in patients to the Services appears unlikely to materialize in the foreseeable future'.¹¹⁴ According to the Commission, the parties would lack the ability to lock-in patients by limiting or preventing the portability of their data, given that users will have the right to ask for portability of their data under the, at that time still, draft GDPR:

The draft GDPR states that data subjects have a right to receive a copy of their data in a structured and commonly used machine-readable format. Moreover, they have the right to transmit their data to another controller or to request the controller to transmit their data directly to another controller.¹¹⁵

For completeness, the Commission notes that, in the course of the market investigation, concerns were raised that companies based outside the EEA may be able to try to circumvent European data protection rules (either by not fully complying with such rules or by interpreting them in their favour), while European competitors need to fully comply with EU data protection rules. In this respect, it suffices to say that LinkedIn post-Transaction remains subject to European data protection rules, in particular to Irish data protection law with respect to the data collection, processing and usage of European users. Moreover, in the case where Irish data protection rules were less restrictive than those in other Member States, the Commission notes that the newly adopted General Data Protection Regulation is directly applicable and therefore the scope for divergence between Member States' national data protection laws will be reduced, including in their enforcement. Finally, if Microsoft were to transfer and process personal data of LinkedIn' members outside of the EEA, the rules of the national laws implementing the Data Protection Directive and, as of 25 May 2018, the General Data Protection Regulation will still apply.

One needs to realize that the merger decision was thus taken even before the final version of the Regulation was adopted on 27 April 2016, let alone before it started applying from 25 May 2018. Even though merger review is forward-looking by nature, the reliance on a new right in a draft legislative proposal as a way to preclude relevant competition concerns from occurring is problematic. This is especially the case as the scope of the right to data portability is not clear even after the adoption of the GDPR. The Article 29 Working Party published guidelines in April 2017 that aim to clarify the conditions under which the new right is applicable.¹¹⁶ However, market players have expressed disagreement with the approach put forward by the Article 29 Working Party.¹¹⁷ The most contentious issue is the scope of the data that data subjects are entitled to port. While Article 20 GDPR speaks about personal data concerning a data subject 'which he or she has provided to a controller', the Article 29 Working Party put forward a broad interpretation of the concept of 'provided data' including not only data actively and knowingly provided by the data subject but also observed data provided by the data subject by virtue of the use of the service or the device.¹¹⁸ Another relevant question is to what extent data controllers can legitimately reject requests for data portability by invoking intellectual property rights in the data assets at stake. In this regard, Article 20(4) GDPR states that the right of data portability 'shall not adversely affect the rights and freedoms of others'. It remains to be seen how this balancing of the interest of the data subject in porting his or her personal data with the intellectual property rights of the data controller will play out.¹¹⁹

With such crucial questions about the scope and implementation of the right to data portability still unanswered, it is hard to justify the weight that the Commission attached to the ability of a new right in precluding any lock-in of patients to the services to be

112 Ibid.

113 Case M.7813—*Sanofi/Google/DMI JV*, 23 February 2016, para 67.

114 Ibid para 69.

115 Ibid.

116 Art 29 Working Party, 'Guidelines on the Right to Data Portability', 5 April 2017, 16/EN WP 242 rev.01.

117 See for instance the Legal memo submitted by the European Telecommunications Networks Operators' Association to the WP29 with regard to the guidelines on the right to data portability, 16 February 2017 <<https://etno.eu/home/positions-papers/2017/367>> accessed 31 August 2018.

118 Art 29 Working Party (n 116) 10.

119 For a discussion see, Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', TILEC Discussion Paper No 2017-041, s 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071875> accessed 31 August 2018.

provided by the joint venture. As many uncertainties still surround the right to data portability today, the Commission's reasoning dating from more than two years before the, at that time even, draft GDPR would start applying is highly speculative. This does not even take into account that there are a number of differences in the personal and material scope of the right to data portability in the GDPR and the competition law remedy of data portability.¹²⁰ As such, the new right may not take away all competition concerns of a lack of data portability in causing user lock-in.

If analysed correctly, the integration of data protection principles into merger review as a parameter of competition is a welcome development to create a more coherent application of different regimes. As regards the potential of data protection law to prevent competition concerns from arising, a cautious approach is necessary to ensure that the data protection rights and duties relied upon are in fact capable of restricting the scope for market players to engage in anticompetitive behaviour.

Enforcement synergies and tensions

In terms of enforcement overlaps, it is instructive to note that the GDPR seems to take competition enforcement mechanisms as inspiration to improve some procedural elements of EU data protection law. As regards its geographic scope of application, the GDPR brings EU data protection law in line with the approach of EU competition law. To establish whether a certain practice falls within the geographic scope of application of the EU competition regime, either the behaviour has to be implemented in the EU or have an immediate and substantial effect in the EU.¹²¹ While the Data Protection Directive applied only to processing of personal data carried out in the context of a controller's EU establishment or, in case the controller was not established in EU territory, through the use of equipment situated in the EU,¹²² the GDPR can also be applicable if neither

the controller, nor its equipment is situated in the EU. The processing of personal data of data subjects who are in the EU is caught by the GDPR as soon as the processing activities are related to the offering of goods or services to such data subjects, irrespective of whether a payment of the data subject is required, or to the monitoring of their behaviour as far as their behaviour takes place within the EU.¹²³ As a result, firms active in the EU are now subject to EU data protection rules even though they are based outside the Union, just like under the EU competition rules.

Another procedural novelty of the GDPR is the one-stop-shop mechanism applicable to cases where the controller or processor is established in more than one Member State. In accordance with Article 56(1) GDPR, the national data protection authority of the main establishment or of the single establishment of the controller or processor is competent to act as lead supervisory authority for the cross-border processing of this controller or processor.¹²⁴ The lead supervisory authority will, in the wording of Article 56(6) GDPR, be 'the sole interlocutor of the controller or processor for the cross-border processing carried by that controller or processor'.¹²⁵ As a result, one single national data protection authority will thus in principle become competent under the GDPR for monitoring the processing of personal data and for taking the related decisions as far as the cross-border processing of personal data is concerned. An analogy can be found here with merger review where a one-stop-shop system is applied that gives the European Commission the exclusive competence to assess concentrations with a Community dimension.¹²⁶ This implies that Member States cannot apply their national competition rules to any concentration that has a Community dimension.¹²⁷

Despite these new procedural strengths, the main difference with the enforcement of EU competition law persists under the GDPR, namely that there is no body at the EU level that has the competence to take action

120 See Inge Graef, 'Mandating Portability And Interoperability In Online Social Networks: Regulatory And Competition Law Issues In The European Union' [2015] Telecommunications Policy 502, 508–509; and Orla Lynskey, 'Aligning Data Protection Rights With Competition Law Remedies? The GDPR Right to Data Portability' [2017] European Law Review 793, 801–02.

121 See in particular *Intel Corp. v European Commission*, Case T-286/09, [2014] ECLI:EU:T:2014:547, paras 235–244 as confirmed by *Intel Corp. v European Commission*, Case C413/14 P [2017] ECLI:EU:C:2017:632, paras 40–46.

122 Art 4(1)(a) and (c) of the Data Protection Directive.

123 Art 3(2)(a) and (b) of the GDPR.

124 As art 4(23)(a) and (b) makes clear, cross-border processing of personal data means either 'processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or

processor is established in more than one Member State' or 'processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State'.

125 However, one should note that each national data protection authority is still competent to deal with a complaint lodged with it or to deal with a possible infringement of the Regulation in case the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State under art 56(2) of the GDPR.

126 Art 1(2) of Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (EU Merger Regulation) [2004] OJ L 24/1 lays down the turnover thresholds that have to be met in order for a concentration to have a Community dimension.

127 Art 21(3) of the EU Merger Regulation.

and adopt measures under EU data protection law. This also explains the calls to consider data protection interests in devising competition law remedies as a way to improve compliance with data protection law throughout the EU.¹²⁸ However, in addition to synergies, there are also situations in which tensions are apparent between the regimes of competition and data protection law.

Linking merger review with data protection and consumer law compliance

One of the main strengths of merger review is the scope for prospective and structural remedies. While merger analysis is forward-looking by nature and the EU Merger Regulation explicitly provides for the possibility to block mergers which are incompatible with the common market, consumer and data protection authorities can only impose behavioural remedies and sanction companies after they have infringed the rules by requiring changes in the way they deal with consumers or process personal data. It should be noted that the GDPR does give data protection authorities the ability to act in a more proactive way, in particular via the principle of accountability that requires data controllers to take responsibility for and to demonstrate compliance with EU data protection rules.¹²⁹ The principle of accountability implies that, upon request of a data protection authority, controllers have to be able to show that adequate measures are in place to ensure that their processing activities comply with EU data protection law. As such, this enables data protection authorities to monitor compliance before an actual breach of the data protection rules needs to be established. Apart from such limited possibilities, EU data protection and consumer law do not provide for structural measures to prevent possible future data protection or consumer issues from emerging. Because of the relative strength of merger review in this respect, the question rises whether data protection and consumer issues should be considered in the merger analysis to be conducted by competition authorities.

Data protection and consumer protection as public interests beyond merger review

The European Commission has persistently expressed the view in the context of its merger decisions in *Google/DoubleClick*, *Facebook/WhatsApp* and *Microsoft/LinkedIn* that privacy-related concerns do not fall within the scope of EU competition law but within the scope of the EU data protection rules.¹³⁰ Similarly, the Court of Justice noted in *Asnef-Equifax* 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’.¹³¹ However, one should note that the approval of a transaction under the EU Merger Regulation does not preclude national data protection or consumer authorities from starting their own inquiry in parallel with or after the merger investigation. After all, merger review is without prejudice to the obligations of the merging parties under these regimes. As already put forward elsewhere,¹³² the role of Article 21(4) of the EU Merger Regulation in creating better coordination between the European Commission as a competition authority and the national data protection or consumer authorities is instructive in this regard. On the basis of this provision, Member States are entitled to take appropriate measures to protect legitimate interests other than those taken into account under the EU Merger Regulation. The legitimate interests that are specified by Article 21(4) include public security, plurality of the media and prudential rules.¹³³ Any other public interest must be communicated to the Commission by the Member State concerned after which its compatibility with the general principles and other provisions of Community law will be assessed by the Commission.

If a new public interest such as data protection or consumer protection will indeed be accepted by the Commission as a legitimate basis to adopt measures protecting other considerations at the national level, the Member State may, on the basis of national law, subject a merger to additional conditions and may even block it

128 See Preliminary Opinion of the European Data Protection Supervisor (n 61) para 64 where the EDPS criticized the Commission’s ‘purely economic approach’ to the *Google/DoubleClick* merger that ‘neglected the longer term impact on the welfare of millions of users in the event that the combined undertaking’s information generated by search (Google) and browsing (DoubleClick) were later processed for incompatible purposes’ under data protection law.

129 See art 5(2) of the GDPR in the context of the data quality requirements.

130 Case No COMP/M.4731—*Google/DoubleClick*, 11 March 2008, para 368; Case No COMP/M.7217 (n 88) para 164 and Press release European Commission, ‘Mergers: Commission Approves Acquisition Of LinkedIn By Microsoft, Subject To Conditions’, 6 December 2016 <http://europa.eu/rapid/press-release_IP-16-4284_en.htm> (no similar statement was made in the *Microsoft/LinkedIn* decision) accessed 31 August 2018.

131 *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios*, Case C-238/05, [2006] ECLI:EU:C:2006:734, para 63.

132 The analysis presented here is based on Graef (n 13) 349–52; and Graef (n 87) 17–18 and 20–21.

133 A recent case in which the UK invoked art 21(4) of the EU Merger Regulation to conduct a media plurality review of a merger after it gained approval by the European Commission is Fox’s acquisition of Sky. See Press release European Commission, ‘Mergers: Commission Clears 21st Century Fox’s Proposed Acquisition of Sky under EU Merger Rules’, 7 April 2017 <http://europa.eu/rapid/press-release_IP-17-902_en.htm> accessed 31 August 2018.

if prohibiting the transaction altogether is proportionate in order to protect the public interest concerned. However, it needs to be emphasized that the analysis conducted by the Member State after invoking Article 21(4) takes place on the basis of national law and outside the framework of EU merger review. Since EU data protection as well as consumer law do not provide the relevant authorities with the possibility to adopt prospective or structural measures, it does not seem possible for a national data protection or consumer authority to subject a merger to any conditions, let alone block it, if it does not give rise to data protection or consumer issues at the time the merger is approved by the Commission under the EU Merger Regulation.¹³⁴

A data protection or consumer authority would thus only be entitled to impose conditions to a merger under Article 21(4) of the EU Merger Regulation if the transaction in and of itself infringes data protection or consumer rules. If the authority merely anticipates that any relevant issues might occur at some point in the future after the merger has been finalized, its only option is to monitor whether the merged entity continues to comply with its data protection or consumer law obligations. Once there are indications that the merged entity is breaching the relevant rules, the authority can start an investigation on its own initiative on the basis of either consumer or data protection law and thus outside the framework provided by Article 21(4) of the EU Merger Regulation.

Devising merger remedies that also further data protection interests

Apart from these possibilities to apply data protection and consumer law alongside merger review, the question can be raised as to whether there is scope to integrate data protection and consumer law interests into merger analysis more proactively, irrespective of the hesitant attitude of the European Commission and the Court of Justice. As already argued in other places,¹³⁵ opportunities to do so seem particularly present in situations where mergers raise competition concerns. When a proposed transaction is found to significantly impede effective competition, the merging parties

typically offer remedies to the Commission to address the identified competition concerns in order to render the concentration compatible with the common market. Since the merging parties are dependent on the discretion of the Commission to prevent the merger from being blocked, the Commission has scope to require remedies that not only address the competition concerns but at the same time also guarantee the effectiveness of data protection or consumer law.¹³⁶ Because of the normative commonalities between the regimes and the role of fairness as an overarching principle, there is room to develop more coherent enforcement approaches in these situations.

Inspiration of how merger remedies may be used to further data protection interests can be drawn from the dissenting statement of former US Federal Trade Commissioner Pamela Jones Harbour in *Google/DoubleClick*. She suggested that it may have been desirable to mandate a firewall between the data of Google and DoubleClick for some period of time to prevent any anticompetitive effects.¹³⁷ In such cases where the combination of data sets is considered to strengthen the position of the merged entity in a particular relevant market so as to significantly impede effective competition, there is reason to require the merging parties to keep their databases separate because of competition concerns. Although the suggestion of Pamela Jones Harbour was solely based on the impact of the merger on competition in the market, the establishment of a firewall between the data sets of the merging parties would also prevent personal data from being used for incompatible purposes under data protection law. To ensure that the merged entity indeed keeps the data sets separate as committed to the Commission, the competent national data protection authority could be put in charge of monitoring whether personal data is not exchanged between previously distinct services. As such, the data protection authority will assist the Commission in monitoring compliance with the merger decision, but at the same time is able to require the merged entity to take pre-emptive measures that also prevent personal data from being combined and, as a consequence, used for incompatible purposes beyond its usual competences.

134 For another view on the possibilities offered by art 21(4) of the EU Merger Regulation, see Costa-Cabral and Lynskey (n 13) 46–47.

135 The analysis presented here is based on Graef (n 13) 352–54 and Inge Graef (n 87) 21–23.

136 A parallel can be made here with commitment decisions as regards which the Court of Justice has made explicit in *Alrosa* that undertakings offering commitments ‘consciously accept that the concessions they make may go beyond what the Commission could itself impose on them’ in an infringement decision (*Alrosa*, Case C441/07 P, [2010] ECLI:EU:C:2010:377, para 48).

137 Dissenting Statement of Commissioner Pamela Jones Harbour, *Google/DoubleClick*, FTC File No 071-0170, 20 December 2007, fn 23, 9 <https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf> accessed 31 August 2018. ‘For example, the Commission might have mandated a firewall between the Google and DoubleClick data for some period of time, consistent with the parties’ representations that they do not intend to merge the datasets. Such a firewall would need to be carefully crafted to avoid gamesmanship, permit auditing, and the like.’

With hindsight, such a remedy may have been appropriate in *Facebook/WhatsApp* in light of the developments that have taken place after the Commission approved the merger in October 2014 as described in the introduction. In particular, one can raise the question of whether the Commission has not been too optimistic by approving the merger without even opening an in-depth investigation and exploring possible merger remedies.¹³⁸ Had the Commission taken a more proactive stance towards the data concentration concerns in *Facebook/WhatsApp*, it could have prevented or at least restricted Facebook from unilaterally deciding to alter WhatsApp's privacy policy. The scope for merger remedies relating to the use of personal data after the merger was present considering that the use by Facebook of data from WhatsApp also raised potential competition concerns. In the absence of any merger remedies, the only option for the various national data protection and consumer authorities involved is to monitor *ex post* whether Facebook is complying with the relevant rules.

An interesting question is whether the new requirements that the GDPR introduces relating to risky processing activities will enable data protection authorities to monitor data controllers more proactively. Under Article 35(1) GDPR, controllers must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk for the rights and freedoms of individuals. Article 36(1) GDPR requires the controller to consult the competent national data protection authority prior to the processing of personal data in situations where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller. The obligation to conduct a data protection impact assessment can be argued to apply in merger cases that give rise to a combination of previously separate data sets which contain personal data. Because of the risk that personal data will be processed for incompatible purposes after the merger, the merged entity may have to take mitigation measures and consult the national data protection authority before the start of the processing activities. In this way, the data protection authority can closely

monitor how personal data are processed after the merger and advise the controller even though no violation of EU data protection law is identified at the time of notification of the merger to the European Commission under the EU merger regime.

Tensions between competition enforcement and data protection

While there are a number of instances where clear synergies can be identified between competition enforcement and data protection, there is also room for tensions to occur. Two types of tensions are discussed here: the imposition of a duty to share data under Article 102 TFEU and the existence of data-driven efficiencies under merger review.¹³⁹ In these scenarios, what is required to establish fair competition may go against the spirit of data protection.

Data protection as an objective justification for refusing to give access to data

As data has become an important input for the development of products and services, it can also form a bottleneck for market players that are dependent on third parties to get access to the data needed to compete on the market. In certain circumstances, competition law can be relied upon to address such data access issues on a case-by-case basis. On the basis of Article 102 TFEU, an incumbent can be required to give access to a particular data set if (i) it holds a dominant position on the relevant market and (ii) the refusal to give access amounts to an abuse of that dominant position. Refusals to deal by dominant undertakings constitute a form of exclusionary abuse as prohibited under Article 102 TFEU. There is a string of case law at the EU level which deals with the requirements under which the legality of refusals to deal has to be assessed.¹⁴⁰ Previous cases relate to physical infrastructures such as railways and ports but also to intangible, intellectual property protected assets.¹⁴¹ In literature, the requirements that need to be met for establishing competition law liability for a refusal to deal have been referred to as the 'essential facilities doctrine'. This doctrine forms an important and at the same time controversial part of EU

138 The *Facebook/WhatsApp* merger was approved on the basis of art 6(1)(b) of the EU Merger Regulation. See Case No COMP/M.7217 (n 88) para 191.

139 The analysis presented here is based on Graef (n 13) 315–22.

140 Relevant cases at the EU level include: *Telefís Eireann and Independent Television Publications Ltd v Commission of the European Communities (Magill)*, Joined cases C-241/91 and C-242/91, [1995] ECLI:EU:C:1995:98; *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs*, Case C-7/97, [1998] ECLI:EU:C:1998:569; *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG*, Case C-418/01, [2004]

ECLI:EU:C:2004:257; *Microsoft*, Case T-201/04, [2007] ECLI:EU:T:2007:289.

141 In the 1990s, the Commission took a number of decisions involving access to port and railway infrastructures:

Case IV/34.174—*B&I Line PLC v Sealink Harbours Ltd. & Sealink Stena Ltd.* [1992] 5 CMLR 255; Case IV/34.689—*Sea Containers v Stena Sealink* [1994] OJ L 15/8; Commission Decision 94/119/EC—*Port of Rødby* [1994] OJ L 55/52; Commission Decision 94/894/EC—*Eurotunnel* [1994] OJ L 354/66.

competition law as its application interferes with the generally recognized principles of freedom to contract and freedom to dispose of one's property. After all, as soon as a refusal to deal qualifies as abuse of dominance, the dominant undertaking is forced to enter into a business relationship with the access seeker and has to share access to its assets. As a result, the EU courts have consistently held that refusals to deal are only to be considered abusive under Article 102 TFEU in 'exceptional circumstances'. In fact, the essential facilities doctrine carries the highest burden of proof under EU competition law.¹⁴²

A relevant question when applying the essential facilities doctrine to personal data is to what extent a dominant undertaking can objectively justify its refusal to deal by invoking its obligations under data protection law. The provider could argue that it will not be able to comply with data protection rules anymore, since it cannot vouch for an adequate level of data protection if it is forced to share personal data with third parties. In fact, such a case has already occurred in the USA, where LinkedIn attempted to terminate hiQ's ability to access otherwise publicly available information on profiles of LinkedIn users. hiQ is a company providing information to businesses about their workforces based on a statistical analysis for which it is wholly dependent on LinkedIn's public data. To defend itself against hiQ's motion for a preliminary injunction to stop LinkedIn from terminating access to the latter's public data, LinkedIn asserted before the District Court of the Northern District of California that to hiQ's access to LinkedIn's data violated LinkedIn users' privacy. However, the Court did not accept this argument on the ground that LinkedIn does allow other third parties to access user data without the knowledge or consent of its users. Furthermore, while hiQ would likely be driven out of business and thus face irreparable harm in the absence of an injunction, the Court argued that LinkedIn had presented no evidence of harm resulting from hiQ's activities despite the fact that the company has been aggregating LinkedIn's public data for five years with LinkedIn's knowledge. As to the asserted harm tied to LinkedIn users' expectations of privacy, the Court stated that 'LinkedIn's own actions do not appear to have zealously safeguarded those privacy interests'.¹⁴³

While a finding like the latter is unlikely to prevail in Europe due to higher data protection standards, the dispute does show the need to analyse the extent to which data protection interests of users are a legitimate reason for refusing to share data with third parties.

As a result, when imposing a duty to deal that would require a dominant undertaking to give access to information relating to identified or identifiable natural persons, competition authorities, and courts have to take into account data protection law. The French Autorité de la concurrence has already dealt with such a case when it imposed interim measures on *GDF Suez* in September 2014 ordering it to give other market players with government authorization to supply natural gas access to certain information about its customers. This duty concerned the customers who had a contract for the supply of gas with *GDF Suez* under the regulated tariffs which were only provided by *GDF Suez* as a result of its public service obligation. For these customers, *GDF Suez* was ordered to provide its competitors with personal data such as names, addresses, fixed telephone numbers and consumption profiles in order to enable them to contact potential new customers. Awaiting the investigation on the merits, the Autorité de la concurrence found *GDF Suez* capable of abusing its dominant position in the market for natural gas by using customer information it had obtained within the framework of its former monopoly status to launch offers at market prices outside the scope of its public service obligation.¹⁴⁴ In line with the recommendations made by the Commission Nationale de l'Informatique et des Libertés (CNIL),¹⁴⁵ the French data protection authority, the Autorité de la concurrence laid down in the operative part of its decision how *GDF Suez* had to comply with its obligation to share customer information with rivals.¹⁴⁶

The Autorité de la concurrence imposed an opt-out system on *GDF Suez* whereby customers had to take action themselves to prevent other gas suppliers would get access to their personal data. This approach seems in line with EU data protection law, as a duty to share personal data with third parties imposed on the basis of competition law would amount to a legal obligation in line with the legitimate ground of processing provided by Article 6(1)(c) GDPR.¹⁴⁷ In principle, a competition law remedy to share personal data can thus not lead to a

142 For an extensive discussion of the application of the essential facilities doctrine to data, see Graef (n 13) 249–80.

143 *hiQ Labs, Inc. v LinkedIn Corporation*, No 17-cv-03301-EMC (ND Cal August 14, 2017).

144 Autorité de la concurrence, Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité, paras 169–174

<<http://www.autoritedelaconcurrence.fr/pdf/avis/14mc02.pdf>> accessed 31 August 2018.

145 Autorité de la concurrence, Décision No 14-MC-02 du 9 Septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité, paras 289 and 294.

146 Ibid 52–53.

conflict with data protection rules as it forms a legitimate ground for processing in itself. Nevertheless, considering that the *GDF Suez* case concerned interim proceedings, one could argue that consent would have constituted a more appropriate ground for processing. If the finding of abuse had not been upheld in the proceedings on the merits, the legal obligation for processing would be deemed to have never existed. In that situation, the personal data of the customers of *GDF Suez* was already shared with third parties in the absence of any legal obligation to that end. It should also be noted that in addition to having a legitimate ground for processing, the other data quality requirements of Article 5(1) GDPR have to be met. In particular, in accordance with the notion of purpose specification, data subjects need to be informed that their personal data is shared with third parties and is thus processed for a new purpose.

GDF Suez illustrates that it is possible for a dominant undertaking to prevent a breach of data protection law as long as the right safeguards as required under the latter field are applied. In cases where it is not appropriate to rely on the competition law obligation as a legitimate ground for processing, a dominant firm may preclude a violation of data protection law by obtaining consent from customers to share their personal data with competitors or by anonymizing personal data before third parties are granted access to it. One should note that anonymization cannot form a solution in situations where competitors have to be granted access to the personal details of users, such as in the *GDF Suez* case where competitors needed certain specific information about individuals in order to contact potential new customers. Furthermore, because of ever stronger technological possibilities and the ability to identify a natural person indirectly by combining anonymous information with data held by a third party, it seems hard to claim that data sets can still be truly anonymous.¹⁴⁷

Data-driven efficiencies as a defence in merger review

Another instance where the regimes of competition and data protection law may conflict is in the context of data-driven efficiencies in merger cases. During the *TomTom/Tele Atlas* and *Microsoft/Yahoo* merger

investigations, the parties put forward data-driven efficiencies as a defence to justify potential anticompetitive effects to which the respective transactions would give rise. In *TomTom/Tele Atlas*, the parties claimed that the acquisition of Tele Atlas by TomTom would bring about significant efficiencies due to the integration of feedback data from TomTom's large customer base to improve the map databases of Tele Atlas. In this light, the parties stated that the rationale of the merger was to allow the merged entity to produce better maps faster. While the Commission argued that end-customers would certainly benefit from the more frequent and comprehensive map database updates made possible by the merger, it also made clear that such efficiencies are difficult to quantify. In the end, the Commission did not estimate the magnitude of the likely efficiencies because it concluded that the transaction lacked anticompetitive effects irrespective of the existence of efficiencies.¹⁴⁹

In *Microsoft/Yahoo*, Microsoft argued that its strategic rationale in pursuing the transaction lay in the notion that success in search advertising and internet search is dependent on scale. By acquiring Yahoo, Microsoft expected to become a more credible alternative to Google because of the increased scale which, in its view, would have a positive effect on both users and advertisers. Microsoft argued, for instance, that the user and advertiser experience would improve because of the more relevant search results and better ad targeting possibilities resulting from a larger volume of search queries. While the Commission did not find conclusive evidence that higher scale is beneficial to users and advertisers, respondents to the market investigation confirmed that the merger would have procompetitive effects and would lead to more advantages than disadvantages. In addition, the large majority of advertisers and media agencies included in the market investigation believed that post-merger the new entity would be a stronger competitor to Google.¹⁵⁰

Mergers giving rise to data-driven efficiencies may be incompatible with data protection law as such if personal data is involved. Although the integration or combination of data from previously separate entities can be beneficial from the perspective of economic efficiency, it is likely to raise data protection issues because, for instance, personal data is further processed for a purpose

¹⁴⁷ As regards examples of cases in which a legal obligation has been accepted as a legitimate ground for processing, European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (2014) 82 makes reference to the legal duty of employers to process data about their employees for reasons of social security and to businesses to process data about their customers for reasons of taxation.

¹⁴⁸ See art 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques', WP 216, 10 April 2014.

¹⁴⁹ Case No COMP/M.4854 (n 100) paras 245–250.

¹⁵⁰ Case No COMP/M.5727—*Microsoft/Yahoo! Search Business*, 18 February 2010, paras 160–176.

different than the original one. In such a situation, the new purpose must be specified and a legitimate basis for the new processing activities must be found. In case the lawfulness of the initial processing was based on consent, this consent must be renewed for every data subject that will be affected by the new processing activities. In order to comply with EU data protection rules, additional data protection measures thus may need to be implemented by the merged entity when data-driven efficiencies relate to personal data.¹⁵¹ A similar tension occurs where, as a potential remedy to address data-related competition concerns, the parties to a merger are demanded to duplicate the relevant data to enable competitors to develop competing or complementary services on this basis.¹⁵² Precedent for such a remedy can be found in the context of the acquisition of Reuters by Thomson in 2008 where the Commission approved the merger on the condition that the merging parties would divest copies of their databases containing financial information. This remedy would allow purchasers of the databases to quickly establish themselves as a credible competitive force in the marketplace in competition with the merged entity.¹⁵³ If personal data is included in the data sets, the same measures as discussed in the context of data-driven efficiencies need to be taken in order to ensure that the merger remedy does not raise data protection issues.

Conclusion

A number of overlaps between the regimes of competition, data protection, and consumer law have been outlined that would in our view benefit from a better coordination, both in terms of substantive principles and enforcement mechanisms. As an overarching principle that plays a role in each of the regimes (albeit in a different way), the notion of fairness can act as the normative underpinning for such more coherent approaches that would improve the protection of consumer interests.

Our belief is that a more consistent application and enforcement of existing regimes will help to address

increasing power and information asymmetries. Before considering the introduction of new legal frameworks to remedy concerns caused by digitization in line with calls for, for instance, the regulation of online platforms or algorithmic accountability, attention should be paid to how existing regimes can be applied to cope with new forms of commercial behaviour. Often, not the scope of the available rules causes problems, but rather the effectiveness with which the rules are enforced. Instead of investing time and effort in the development of new regimes that may again suffer from a lack in adequate enforcement capabilities, attention should be directed to an analysis of the possibilities of existing regulatory frameworks. It should be noted that this is not a plea against any new regime, but a call for a nuanced approach whereby novel rules are only considered when existing regimes leave actual regulatory gaps. This article has aimed to provide a starting point by outlining recommendations for strengthening synergies between competition, data protection and consumer law on the basis of existing substantive principles and enforcement mechanisms.

Apart from such synergies, scope for tensions remain in particular between competition enforcement and data protection. Such tensions can be put in the wider context of ongoing debates about the regulation of the data-driven economy in which different policy objectives are being reconciled.¹⁵⁴ On the one hand, there is a strong interest in incentivizing the development of new data-enabled products and services by opening up privately held data sets. On the other hand, the exchange of data between market players should not erode the fundamental right to data protection. As such, a policy dilemma of continued interest is how to strike a balance between data innovation, facilitated through data access and reuse, and data protection, to be guaranteed through compliance with principles like data minimization and purpose limitation.

doi:10.1093/idpl/ipy013

151 Similar considerations also play a role in the context of art 101 TFEU where agreements by which competitors cooperate and share personal data may be considered to give rise to efficiencies under art 101(3) TFEU. Furthermore, such an agreement may not even be anticompetitive under art 101(1) TFEU if it does not have an anticompetitive object or leads to anticompetitive effects, while the sharing of personal data with third parties is problematic from a data protection law perspective.

152 See Nils-Peter Schepp and Achim Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (2016) 7 *Journal of European Competition Law and Practice* 120, 123.

153 Case No COMP/M.4726—*Thomson Corporation/Reuters Group*, 19 February 2008.

154 For ongoing policy discussions, see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Building a European Data Economy', 10 January 2017, COM(2017) 9 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a common European data space', 25 April 2018, COM/2018/232 final.