

**DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE**

Non-price Effects of Mergers - Note by Orla Lynskey

6 June 2018

This paper by Orla Lynskey was submitted as background material for Item 4 of the 129th OECD Competition committee meeting on 6-8 June 2018.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

More documents related to this discussion can be found at www.oecd.org/daf/competition/non-price-effects-of-mergers.htm.

JT03432756

Considering Data Protection in Merger Control Proceedings

Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.

COMP/M.7217 - Facebook/Whatsapp, para 164.

1. Introduction

1. As is well documented, personal data lead a double life in digital society. Our personal data are, on the one hand, a digital reflection of our physical and spiritual selves. It is for this reason that privacy and data protection legislation seeks to provide individuals with effective control over their personal data, or ‘informational self-determination’. Such control over personal data is valuable in its own right but is also instrumental to individual freedom of expression, freedom of association and autonomy (including political autonomy). As a result of the informative insights that can be gleaned from personal data they also, on the other hand, have an economic life. Individuals therefore allow for the processing of their personal data in exchange for benefits, such as access to content and services online without monetary payment. This dual dignitary-economic role for personal data has prompted scholars and regulators to query what role, if any, privacy and data protection (hereafter ‘data privacy’) should play (as a non-price factor) in merger control.¹ This question has become more pertinent given the fast rise in M&A deals involving a technology target over the past decade.²

2. While there is an extensive literature published regarding the role of data (including personal data) in competitive assessments, this paper is concerned with the narrower question of whether data privacy is relevant to competitive assessments in merger control and, if so, how. The present paper suggests that, although data privacy matters remain primarily within the remit of data privacy regulators, there are circumstances in which data privacy should influence the competitive assessment of competition authorities.³ Two ways are identified. First, when making competitive

¹ While privacy and data protection are often referred to synonymously, in many legal systems they are distinct but overlapping rights. See further: Kokott and Sobotta, ‘The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law 222.

² For instance, in a 2015 Report on data-driven innovation, the OECD observed that in data-related sectors, ‘the number of mergers and acquisitions (M&A) has increased rapidly from 55 deals in 2008 to almost 164 deals in 2012’ (p 94). More recently, the 2017 M&A Report published by Boston Consulting Group indicated that technology takeovers represented 30% of the entire US M&A market in 2016. Boston Consulting Group, 2017 M&A Report – Chapter 2: The Resurgent High-Tech M&A Marketplace, 26 September 2017.

³ For general background on the synergies between data protection and competition law, and areas of potential intersection see: Costa-Cabral and Lynskey, ‘Family ties: the intersection between data protection and competition law in the EU’ 2017 Common Market Law Review 11. See also for a

assessments on a given market, competition authorities take into consideration the existing legal and regulatory framework as background to their assessments. As data privacy forms part of this legal landscape, it influences competitive assessments in this way. Second, it is suggested that the data privacy policy an undertaking offers to individuals is an element of a product or service's quality. The quality of the data privacy policy offered is therefore a competitive parameter on which undertakings can engage in competition.

3. By taking data privacy into account in this way, a problematic dynamic has nevertheless emerged. Competition authorities implicitly assume that the existence of data privacy regulation and oversight is, in itself, sufficient to ensure that markets involving personal data accurately reflect consumer data privacy preferences. This (erroneous) assumption can then underpin the finding that undertakings do not yet compete on the basis of data privacy as a dimension of quality. Concentrations are thus not scrutinised on this basis and further market concentration occurs thereby exacerbating the existing dysfunctional equilibrium in the markets concerned.

4. Two steps – each with their own challenges – are therefore required in order to break this cycle. First, competition authorities need to look ‘under the hood’ of data privacy regulation and gain a better understanding of the constraints on consumer decision-making. Second, should consumers value data privacy as a dimension of quality, it is necessary to prescribe criteria to identify a deterioration in quality. These will be considered in turn. Finally, this paper recalls the public good character of data protection that supports the claim that data privacy, like media plurality, could be subject to a contemporaneous non-competition assessment prior to the clearance of data-driven concentrations.

2. The Role of Data Protection in Merger Analysis

5. Data-driven mergers allow for the potential aggregation of the merging parties' data sets. The merged data set may then become a barrier to entry to the relevant market. For instance, the DOJ's action against the merger of Bazaarvoice and its leading rival Power-Reviews established that data can serve as a barrier to entry in the market for rating and reviewing platforms.⁴ However, this is an empirical question of whether an alternative source of a similar volume and variety of data is available to competitors. Competition authorities therefore examine whether competitors could access such data from data brokers, data analytics services, or by collecting and analysing the data themselves.⁵ For instance, in finding that the *Facebook/Whatsapp* transaction would not enable Facebook to improve its targeted advertising on Facebook's social networking (by integrating Whatsapp user data), the Commission held that post-merger there would

US perspective, Ohlhausen and Okuliar, ‘Competition, consumer protection, and the right (approach) to Privacy’ (2015) *Antitrust Law Journal* 121.

⁴ *USA v Bazaarvoice Inc.*, Case No. 13-cv-00133 WHO, Competitive Impact Statement, p 5. Available at: <http://www.justice.gov/atr/case-document/file/488826/download>.

⁵ Ocello, Sjödin and Subočs, ‘What's Up with Merger Control in the Digital Sector? Lessons from the *Facebook/Whatsapp* EU merger case’ *Competition Merger Brief* 1/2015, p 6.

continue to be a large amount of Internet user data, valuable for advertising purposes, that are not within Facebook's exclusive control.⁶

6. However, as cautioned by the German and French Competition Authorities in their joint report on Big Data, even though it may be theoretically possible to match an incumbent's data trove, 'this might not be possible in practice due to the quantity and quality of the established company's data set'.⁷ This is echoed by Stucke and Grunes who suggest that it is the variety of the data amassed by a concentration, rather than the volume, that may be critical.⁸ If a data-aggregating merger leads to the exclusion of competition, whether actively (if the merged entity refuses access to data, or provides differentiated access to this data) or passively (if the data is a barrier to entry) then this has the potential to increase the market power of the merged entity. In other words, the data could be a source of monopoly power. As the German *Monopolkommission* suggests:

It is conceivable that the concentration-related combination of data stocks on the platform of an acquirer enables its operator to prevail over competitors in its further competition conduct solely by virtue of permanently having superior knowledge e.g., of the user preferences. This can be used by a platform operator in order to expand into directly adjacent digital markets, as well as into other markets not previously belonging to the company's core business.⁹

7. Such consolidation of market power can be of relevance to data privacy if it enables the monopolist to exploit consumers by imposing unfair terms and conditions on them, or by exerting downward pressure on competition on the basis of data protection.

2.1. Data protection as a parameter of non-price (quality) competition

8. There is growing consensus behind the idea that 'competition on privacy', or 'competition on data protection', can constitute an element of competition for goods and services.¹⁰ As such, a concentration that reduces data privacy could be equated to a degradation in quality for these goods and services. This approach internalises data protection within a competition authorities' competitive assessment. This reduction in quality could arise in several ways, for instance, directly by merging the data sets or by altering the data protection policies post-merger; or, indirectly, by the removal of a maverick that is playing a disruptive role in the market to the benefit of consumers.

⁶ COMP/M.7217 - *Facebook/Whatsapp*, para 189.

⁷ Autorité de la Concurrence and Bundeskartellamt, 'Competition law and data', Joint Report, 10 May 2016, p 13. Available at: www.autoritedelaconcurrence.fr/doc/report_competitionlawanddatafinal.pdf.

⁸ Stucke and Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016), p 136.

⁹ Monopolkommission, Competition policy: the challenge of digital markets, Special Report No 68, 2015, p 111.

¹⁰ Kimmel and Kestenbaum, 'What's up with WhatsApp? A transatlantic view on privacy and merger enforcement in digital markets' *Antitrust* (Fall 2014), p 51; Ohlhausen and Okuliar, 'Competition, consumer protection, and the right (approach) to privacy' (2015) *Antitrust Law Journal*, p 37–38; Tucker, 'The proper role of privacy in merger review' (2015/2) *CPI Antitrust Chronicle*, p 2–4.

9. Of course, there is no empirical basis for ‘assuming in every case that a firm acquiring more data about customers is imposing the equivalent of a price increase or quality decrease’, such a finding is fact dependent.¹¹ Nevertheless, that data privacy constitutes a potential aspect of quality has been recognised by, for instance, the FTC in its *Google/DoubleClick* merger assessment when it investigated the possibility that the transaction ‘could adversely affect non-price attributes of competition, such as consumer privacy’ but found that the evidence did not support this conclusion.¹²

10. In *Facebook/Whatsapp* the European Commission acknowledged that, on the basis of its market investigation, consumer communications applications compete on the basis of functionality and their underlying network.¹³ ‘Privacy and security’ were recognised to be amongst the most important areas for functionality improvement.¹⁴ Moreover, the Commission noted that one of the differentiating features of Facebook Messenger and Whatsapp was their data privacy policies however it concluded that the two were not close competitors.¹⁵ Therefore, the Commission in its decision implicitly recognised data privacy as a parameter of competition but did not consider the impact of the transaction on this parameter as there was an ostensible lack of competition between the merging firms. Competition officials have subsequently reiterated that ‘data privacy as quality’ is most likely to be relevant where a merger involves a market in which data privacy is shown to be an important parameter in the eyes of (a significant number of) customers¹⁶, or a ‘key parameter of competition’.¹⁷

11. This conclusion exposes a blind spot in the Commission’s reasoning in *Facebook/Whatsapp*. As Stucke and Grunes note, the interesting dynamic was that a very high percentage of Whatsapp users were already using Facebook’s social network and could easily have used the integrated Facebook messenger yet they ‘opted for a texting app that afforded them significantly greater privacy protection than Facebook messenger’.¹⁸ Indeed, in its decision the Commission noted that privacy and data security are ‘becoming increasingly valued’.¹⁹ Yet, the fact that Facebook and Whatsapp had dissimilar data protection policies was used as a factor to conclude that they were not

¹¹ Bruce Hoffmann - Acting Director of Competition Bureau, FTC, ‘Competition Policy and the Tech Industry: What is at Stake?’, 12 April 2018, p 6. Available at: https://www.ftc.gov/system/files/documents/public_statements/1375444/ccia_speech_final_april30.pdf

¹² Statement of the FTC concerning Google/DoubleClick, FTC File No. 071-0170. Available at: https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf, p 2.

¹³ COMP/M.7217 - *Facebook/Whatsapp*, para 86.

¹⁴ Ibid, para 87.

¹⁵ Ibid, paras 102 and 106 respectively.

¹⁶ Ocello and Sjödin, *Microsoft/LinkedIn: Big data and conglomerate effects in tech markets*, Competition Merger Brief 1/2017, p 5.

¹⁷ Ocello, Sjödin and Subočs, ‘What’s Up with Merger Control in the Digital Sector? Lessons from the *Facebook/Whatsapp* EU merger case’ Competition Merger Brief 1/2015, p 6.

¹⁸ Stucke and Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016), p 132.

¹⁹ COMP/M.7217 - *Facebook/Whatsapp*, para 87.

competitors rather than that they competed, and could be distinguished, on the basis of these data privacy policies. This reasoning suffers from the same logical fallacies as that of the Office of Fair Trading (OFT) in *Google/Waze*. The OFT cleared that transaction on the basis that Waze, a digital mapping company operating on the basis of real-time data from users, did not exercise a competitive constraint on Google. As Stucke and Grunes highlight, pursuant to this logic ‘a monopolist could acquire the few nascent competitive threats, so long as these competitors have not reached scale and become disruptive forces in the marketplace’.²⁰

12. Shapiro has suggested that the application of applying ‘tougher standards to mergers that may lessen competition *in the future*, even if they do not lessen competition right away’ would improve merger enforcement.²¹ Indeed, he singles out the technology sector as a sector in which it is common for a large incumbent firm to acquire a ‘highly capable firm operating in an adjacent space’ thereby involving a loss of future competition.²² Stucke and Grunes suggest that by acquiring Whatsapp, Facebook was shielding itself from further competition on data privacy: ‘Whatsapp represented a moat to prevent inroads from rival, privacy-focused texting apps’.²³ Thus, the concentration by decreasing the quality of data privacy policies and removing a ‘data protection friendly’ option from the market, also decreased choice. In *Microsoft/LinkedIn* the Commission found that if the merged entity foreclosed access to Microsoft for LinkedIn competitors, this could impact the choice of consumers regarding the level of data privacy offered by professional services networks. Thus, LinkedIn competitor XING’s possible marginalisation as a result of Microsoft’s foreclosure strategy would also restrict consumer choice regarding data privacy.²⁴ The Commission thus obtained a number of commitments from Microsoft to preserve choice on the market, including consumer data privacy choice. Furthermore, the US Horizontal Merger Guidelines state that if ‘the merged firm would withdraw a product that a significant number of customers strongly prefer to those products that would remain available, this can constitute a harm to customers over and above any effects on the price or quality of a given product.’²⁵ In such circumstance, the relevant agency may assess whether the ‘reduction in variety is largely due to a loss of competitive incentives attributable to the merger’.²⁶

2.2. Data privacy legislation as part of the competitive backdrop

13. A further way in which data privacy can inform the application of the competition rules is through its place in the legal and regulatory landscape against which competitive assessments are made. Data protection regulation has a hybrid regulatory and rights-based

²⁰ Ibid, p 96.

²¹ Shapiro, ‘Antitrust in a time of populism’, p 23. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3058345

²² Ibid.

²³ Stucke and Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016), p 83.

²⁴ M.8124 *Microsoft/LinkedIn*, para 350.

²⁵ US DOJ and FTC, Horizontal Merger Guidelines, section 6.4.

²⁶ Ibid.

function.²⁷ It both ensures the protection of fundamental rights but can also be characterised as economic regulation as it seeks to tackle information and power asymmetries between individuals and those who process personal data, and control that processing. Indeed, in many legal systems data protection is treated solely as an instrument of economic regulation. Competition authorities proceed from the premise that this regulation corrects market failures and therefore that data-driven markets function effectively and reflect consumer preferences. This presumption then informs their decision-making. For instance, in *Sanofi/Google/DMI JV* the Commission held that the parties to the transaction would ‘lack the ability to lock-in patients by limiting or preventing the portability of their data given that, according to the draft General Data Protection Regulation (GDPR), users will have the right to ask for the data portability of their personal data’.²⁸

14. Similarly, in *Facebook/Whatsapp* the Commission did not interrogate the conclusion that competition on the basis of data protection does not yet exist, assuming that markets involving personal data function efficiently and reflect consumer preferences. As the UK Competition and Markets Authority (CMA) observes: the ‘presence of competition over privacy is a useful indicator, not only of firms’ willingness to adapt to consumers’ desires, but also consumers’ understanding of the use of their data in that market, and the effectiveness of competition in the market in question’.²⁹ Indeed, there are a number of reasons that might explain such a lack of data privacy competition. One of them is that consumer inactivity on data privacy means that they do not care about it, yet the so-called privacy paradox (a situation where consumers consistently claim to value data privacy but then do not act accordingly) must then be explained. A second explanation is that undertakings have already exercised market power to weaken data protection on the relevant market (the ‘cellophane fallacy’). As Stucke and Grunes put it, the ‘reason why market forces have not yielded the privacy protections that we desire is the *absence* of meaningful competition’.³⁰ A third is that there is market failure that has not been remedied by data privacy regulation.

15. Thus, it is suggested, competition authorities need to gain a better understanding of how markets involving personal data function in practice to inform their merger analysis. In the absence of such insights, a merger risks putting increasing pressure on a regulatory mechanism struggling to achieve its stated objectives.

3. Challenges of Incorporating Data Protection into Merger Analysis

16. Based on the above, there are two primary obstacles to incorporating data protection considerations into merger proceedings. The first is quantifying a decrease in data protection quality resulting from a transaction. The second is taking into consideration the mechanics of consumer decision-making on data-driven markets.

²⁷ See further, Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015), p 76-88.

²⁸ M.7813 - *Sanofi/Google/DMI JV*, para 69.

²⁹ CMA, ‘The commercial use of consumer data: Report on the CMA’s call for information’, CMA38, June 2015, p 80.

³⁰ Stucke and Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016), p 61.

3.1. Quantifying ‘data protection’ quality

17. The general challenges of taking decreases in quality into consideration in competition proceedings are reflected in this context. The first challenge is one of incommensurability. This raises a number of questions: can a decrease in price offset a decrease in data privacy quality, or what if, despite a decrease in data privacy quality, the merged entity offered a superior quality product overall? Perhaps most pertinently, can an ‘efficiency’ (namely more accurate targeted advertising) offset the decrease in quality that data aggregation entails? Hoffmann suggests that data transfers lead to an ‘immediate positive return’ for consumers: ‘[w]hen you give data to a tech firm, often that data is immediately used to improve the service that the firm is providing to you.’³¹

18. A second challenge is that there is internal differentiation in terms of how users value data protection. For instance, Hoffmann suggests that these issues are ‘more analogous to a differentiated product, where different consumers may have different values associated with each aspect of product available in the market, and each consumer makes a purchase choice based on his or her own utility’.³² While this may be true, in reality, consumers are offered ‘boilerplate’ data privacy terms and it is the impact of these terms on the marginal consumer that is most relevant for competitive assessments.

19. A third challenge is defining the benchmarks to be used to gauge a decrease in quality. One mechanism to do this might be quantitative, by applying a SSNDQ (small but significant non-transitory decrease in quality) test. To be accurate, this test would assume that decreases in quality are tangible for consumers in a similar way to decreases in price. However, a qualitative test, based on core data protection principles, might also be applied. In the European Union, such principles can be gleaned from the General Data Protection Regulation and include principles such as data minimisation; data security; and data accuracy. The recently modernised Council of Europe Convention No 108 also contains these principles in its Articles 5 and 7. These core principles are present in other national and transnational data protection and privacy protections. For instance, in the US the Fair Information Practice Principles, set out in the 1974 Federal Privacy Act, include ‘information protection’ and ‘information review and correction’. Thus, we are seeing increasing convergence around a set of core principles for data privacy and a growing body of legal guidance to inform their interpretation. In these instances, competition authorities could cooperate with data protection authorities, as proposed by the European Data Protection Supervisor in its ‘Digital Clearinghouse’ initiative, in order to gauge the impact a concentration would have on data protection as a dimension of quality.³³ Of course, as has been suggested in the context of media mergers, if quality is so tightly regulated through detailed rules, then competition authorities might justifiably assume

³¹ Bruce Hoffmann - Acting Director of Competition Bureau, FTC, ‘Competition Policy and the Tech Industry: What is at Stake?’, 12 April 2018. Available at: https://www.ftc.gov/system/files/documents/public_statements/1375444/ccia_speech_final_april30.pdf.

³² Ibid.

³³ For further information: EDPS, Big Data and Digital Clearinghouse: https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en

that mergers would leave factors such as quality unchanged, or even improved.³⁴ This is not the case at present, however, in the data privacy context.

3.2. Consumer decision-making in data-driven markets

20. Farrell has observed that there are particular reasons why the ‘standard commitment and information conditions for efficient contracting’ do not hold in the privacy context, leading to a dysfunctional equilibrium in data-driven markets.³⁵ This dysfunctional equilibrium persists despite decades of regulation in many countries. The reasons individuals have thus far failed to exercise control over their personal data are numerous. Solove points to several in his work. As he notes, even if individuals had the desire to micro-manage their data ‘there are simply too many entities that collect, use, and disclose people’s data for the rational person to handle’.³⁶ Furthermore, the ‘true consequences’ of data processing are ‘cumulative, and they cannot be adequately assessed in a series of isolated transactions’.³⁷ In many data-driven mergers individuals will have no direct contact with the merging parties and cannot therefore exercise data protection rights. Indeed, if the EU’s new data protection rules are strictly enforced, one consequence might be more stringent oversight of the activities of data brokers. This in turn would have competitive implications: data may become a more rare (and valuable) asset, if no longer available on such secondary markets. Finally, as Farrell cautioned, individuals may have already resigned themselves to the idea that companies do not offer adequate data protection.³⁸ For instance, the CMA observes that ‘many feel resigned to the inevitability of surveillance and the power of marketers to harvest their data’³⁹ and that the ‘feeling of loss of control appears to be a core theme, perhaps helping to explain consumers’ specific fears about how their data might be used’.⁴⁰ A competitive implication of this is as follows:

If firms believe that few consumers shift their demand in response to actual privacy policies, then the firm’s incentives are to make its policy noncommittal and/or non-protective, and to go for the biggest available V (additional profits per customer) – or, perhaps less dramatically to go for bigger [additional profits

³⁴ OECD – Policy Roundtable on Media Mergers, 9. Available at: <https://www.oecd.org/competition/mergers/17372985.pdf>.

³⁵ Farrell, ‘Can privacy be just another good?’ (2012) *Journal on Telecommunications and High Technology Law* 251, 261.

³⁶ Solove, ‘Privacy Self-Management and the Consent Dilemma’ (2013) 126 *Harvard Law Review* 1880, 1888.

³⁷ Ibid.

³⁸ Farrell, ‘Can privacy be just another good?’ (2012) *Journal on Telecommunications and High Technology Law* 251, p 258.

³⁹ CMA, ‘The commercial use of consumer data: Report on the CMA’s call for information’, CMA38, June 2015, p 116.

⁴⁰ Ibid.

per customer] over minimising H [the incremental harm to consumers caused by switching from a more protective to a less protective policy].⁴¹

21. Furthermore, as Fletcher suggests, demand-side interventions to change consumer behaviour are necessary but not sufficient to rectify market failings. As she notes, changing consumer behaviour involves ‘understanding what other inhibitors there might be to enhancing consumer decision-making’.⁴² Marsden makes a similar point highlighting that the fundamental driver of competition is ‘the process of consumers exercising their choice’.⁴³ While this thinking is embedded in market definition he claims that further focus on whether and how consumer choice is exercised, particularly analysing online activity, will allow authorities to better appreciate the actual mechanism at play in competition. Do consumers have a choice? How informed is it? Can they exercise their choice? How do they exercise it? How does a restraint affect consumer choice?⁴⁴ This suggests that merger analysis needs to look beyond the regulatory framework to examine the actual barriers to consumer choice in data-driven markets.

4. Conclusion

22. The foregoing analysis leads to two suggestions. First, that core data protection principles could serve as a normative benchmark for assessing quality of data privacy. As Stucke and Grunes note, a retrospective examination of consummated concentrations may lead to the conclusion that ‘what is quantifiable is not necessarily what is important, and what is important should be captured by legal presumptions’.⁴⁵ Second, competition analysis will need to come to grips with the realities faced by consumers on data-driven markets when exercising their rights. Increased cooperation between data protection and competition regulators would lead to institutional efficiencies in this regard.

23. Some further linked observations might however be made. In light of the complex economic, social and political ramifications of personal data aggregation, a more cautious approach to data-driven mergers might be advised. At its most extreme, this would amount to a moratorium on acquisitions by certain companies, as proposed by the Open Markets Institute.⁴⁶ More likely, this would mean increased use of the power to block mergers. As Shapiro suggests sound competition policy would tolerate some false positives in order to avoid some false negatives (i.e. allowing mergers that eliminate

⁴¹ Farrell, ‘Can privacy be just another good?’ (2012) *Journal on Telecommunications and High Technology Law* 251, p 258.

⁴² Fletcher, *Exploitation of Consumer Decision-Making and How to Address it: Lessons from Past Demand-Side Interventions* (2017)8 *Journal of European Competition Law and Practice*, p 519.

⁴³ Marsden, ‘Competition and exercising consumer choice in online markets’, February 2015, p 3. Available at: <https://www.oxera.com/Latest-Thinking/Agenda/2015/Competition-and-exercising-consumer-choice-in-onli.aspx> .

⁴⁴ *Ibid.*

⁴⁵ Stucke and Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016), p 313

⁴⁶ Open Markets Institute, ‘Open Markets Letter to FTC regarding Facebook’, 31 October 2017. Available at: <https://openmarketsinstitute.org/commentary/open-markets-letter-to-ftc-regarding-facebook/> .

targets that would indeed have grown to challenge the dominant incumbent’).⁴⁷ One assumption that could be embedded in merger analysis in data-driven markets is that this data can, and will, be merged post-merger. As Stucke and Grunes highlight, it is ‘hard to fathom under the Commission’s analysis why Facebook acquired Whatsapp’.⁴⁸ Indeed, subsequent developments revealed that data aggregation was technically feasible and that the merged entity intended to proceed on this basis.⁴⁹ Pledges to not aggregate data should be treated in the same way as pledges to not raise prices, and overlooked.

24. Finally, irrespective of whether consumers value data protection at an individual level, data protection has many ‘public good’ qualities. As such, an argument could be made for an assessment – contemporaneous to the competition assessment – of the impact of a merger on data protection. Media mergers may provide a useful comparator for these purposes.

⁴⁷ Shapiro, ‘Antitrust in a time of populism’, p 24. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3058345

⁴⁸ Stucke and Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016), p 82.

⁴⁹ COMP/M.8228 *Facebook/Whatsapp*.