5. Privacy-as-a-Quality Parameter of Competition

Samson Y. Esayas*

Published in Björn Lundqvist and Michal Gal (eds.), *Competition Law for the Digital Economy* (Edward Elgar, 2019) pp. 126-172.

Key words: Privacy competition; data concentration; privacy as a quality parameter; competition in privacy; data protection and competition law; role of privacy in mergers.

1. Introduction

With the growing importance of data for commercial purposes, privacy has attracted considerable attention in competition law discussions, particularly when companies in data-rich industries seek a merger or acquisition. Prime examples of such mergers include Google/DoubleClick, Facebook/WhatsApp and the acquisition of LinkedIn by Microsoft. Such mergers are primarily driven by the desire to acquire and combine new data assets viewed as a key source of competitive advantage in developing and providing digital services.[1] In turn, this development raises novel regulatory questions in competition law, including whether, and to what extent, privacy is a relevant consideration in merger assessments.

One emerging approach, shared both by the European Commission (EC) and the US Federal Trade Commission (FTC), is to factor in privacy-as-a-quality (non-price) competition parameter. This approach treats privacy as a quality component of the product or service offered to consumers and privacy harms as reductions in the quality of the product or service that needs to be accounted for in the competition analysis. Despite the emerging consensus on how to incorporate privacy into a competition

* This work is financed by the University of Oslo and partly supported by the SIGNAL project (Security in Internet Governance and Networks: Analysing the Law), which is jointly funded by the Norwegian Research Council and UNINETT Norid AS. The author is grateful to Lee A. Bygrave and Inger B. Ørstavik for their valuable comments on earlier drafts. However, the usual disclaimer applies.

[1] For example, in the proposed merger of Microsoft/Yahoo!, the merging parties put forth efficiency gains resulting from access to large pools of search data, which was accepted by the European Commission. See Case M 5727 *Microsoft/Yahoo! Search Business* decision of 18 Feb 2010, para 163.

analysis, there is much uncertainty and scepticism on what constitutes reduction in privacy, the incentive to reduce privacy and the ultimate anti-competitive effect of such a reduction. This chapter identifies and reflects on some of these uncertainties and scepticisms surrounding the privacy-as-a-quality parameter, including the lack of a link between privacy harms and accumulation of too much information; the lack of economic incentive to reduce privacy; and the alleged trade-off between privacy harms and other quality improvements. Finally, the chapter examines the role that data privacy law can play in understanding the degradation of privacy in competition law.

2. Privacy-as-a-Quality (Non-Price) Competition Parameter

At its core, competition policy is concerned with a market power that may harm 'consumer welfare'. According to the Commission Guidelines on the abuse of a dominant position, consumer welfare is determined regarding price and other factors, such as quality and consumer choice.[2] When a market is effectively competitive, it benefits consumer welfare in the form of lower prices, high quality and a wide range of choices.[3] In contrast, competition is harmed when a transaction or a conduct results in a significant increase in market power, defined as the ability of a firm or group of firms 'to profitably increase prices, reduce output, choice or quality of goods and services, diminish innovation, or otherwise influence parameters of competition'.[4] Thus, traditional competition law concerns are primarily related to price increase, output or quality reduction, with little or no attention paid to privacy considerations and the treatment of personal data.[5] However, this has been changing in recent years due to

[2] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (Text with EEA relevance) [2009] OJ C45/02, para 19.

[3] See Case C-209/10 *Post Danmark AS v Konkurranceradet* EU:C:2012:172, para 22 (indicating that competition on merits leads to the exclusion of competitors that are 'less efficient and so less attractive to consumers from the point of view of, among other things, price, choice, quality or innovation').

[4] See Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004] OJ C 031/03, para 8.

[5] For example, the terms 'personal data' and 'privacy' have not featured in the Guidelines on abuse of dominant position nor in the Guidelines on horizontal mergers. See also, Commissioner Harbour's dissenting opinion on the Google/Double Click merger, noting that '[t]raditional competition analysis fails to capture the interests of all the relevant parties,' particularly 'consumers whose privacy is at stake'. See In the matter of Google/DoubleClick F.T.C. File No. 071-0170 Dissenting Statement of Commissioner Pamela Jones Harbour, <link>.

the growing value of personal data for commercial purposes and as a key source of competitive advantage.[6]

The digital economy is marked by a vast information collection that is analysed and exploited by businesses for their commercial ends; this has led to the coining of the term 'big data'.[7] Increasingly, massive amounts of data about consumers—where they are, what devices they use, what they purchase and the different categories of their online behaviours and interests—are collected every day. Personal data being referred to as the 'new currency' and the 'new oil' is only a confirmation of the paramount importance of personal data in the digital economy.[8] At the heart of the business model for companies, such as Google or Facebook, both considered global information giants,[9] is a detailed collection and analysis of consumer data that are often gathered without the individuals' knowledge or consent. Such information is used to target advertisements to specific groups that might be most interested in buying certain products or services. Thus, consumer information is instrumental in online advertising and serves as a key revenue source for these online content providers, which in turn is used to finance a broad array of free content, products, and services for consumers. A notable development that reflects the commercial importance of data is the growing number of data-mergers, which are partly aimed at adding data scale and variety that could be used for innovating new or improving existing products or services.[10] According to the Organisation for Economic Co-operation and Development (OECD), such data-mergers have tripled over the last couple of years.[11] This development in the digital economy ushers in a new challenge on whether, and if so to what extent,

[6] For example, the recent Commission decision in Microsoft/LinkedIn contains 26 instances of 'data protection', 19 instances of 'personal data' and 11 instances of 'privacy'. See Case M 8124 *Microsoft /LinkedIn*, decision of 6 Dec 2016.

[7] For the purpose of this document, 'big data' are 'large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future'. See National Science Foundation, 'Solicitation 12–499: Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA)' (2012) 5 <Link>. However, it should be noted that not all big data are considered personal data, although increasingly almost any data about consumers are becoming capable of being linked to an individual.

[8] In 2009, Meglena Kuneva, then European Consumer Commissioner, remarked that 'Personal data is the new oil of the internet and the new currency of the digital world.' See European Commission Press Release, 'Keynote Speech by Meglena Kuneva: Roundtable on Online Data Collection, Targeting and Profiling' (31 March 2009).

[9] Ian Brown and Christopher Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (The MIT Press 2013) XVII.

[10] See *Microsoft/Yahoo! Search Business* (n 1), para 163 on the data-driven efficiencies put forth by the merging parties.

[11] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* (OECD Publishing 2015) 94.

privacy is a concern in competition law assessments when companies in data-rich industries seek a merger or acquisition.

There are at least two emerging approaches for incorporating data privacy concerns into competition assessments. One approach is based on the argument that data privacy is a fundamental right, and competition law should consider how certain conduct (a merger or exclusionary act) directly affects this right.[12] This approach, initially proposed in a merger case, calls for competition authorities to block mergers that endanger the data protection rights of individuals, unless the merged entity implements adequate privacy safeguards.[13] Given that this approach does not consider purely competition concerns (for example, price increase, output reduction or quality reduction), it would have to overcome insurmountable challenges to succeed and thus is beyond the remits of this chapter. Furthermore, both the CJEU and the Commission have clearly indicated that privacy is beyond the scope of EU competition law.[14] Another approach is based on the argument that data privacy is a concern so far as it affects the parameters of competition, that is, reduces privacy protection as a form of quality or deprives consumer choice.[15] This approach acknowledges competition law's concern as being limited to competitive issues but posits that privacy should form a competition dimension.[16] Although this line of argument is gaining some traction among scholars and regulatory authorities, questions on how to operationalise such an approach through concrete theory of harm remain largely unchartered and sometimes controversial. It is the aim of this chapter to explore how privacy might fit

[12] Complaint and Request for Injunction, 'Request for Investigation and for Other Relief in the Matter of Google and DoubleClick' <link>.

[13] ibid. See also Costa-Cabral and Orla arguing that the incorporation of data protection right into the TFEU following the Lisbon Treaty implies that the Commission is required to respect and promote this right in its decisions, including mergers. Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 38ff.

[14] See Case C-238/05 *Asnef-Equifax v Asociacion de Usuarios* [2006] ECR I-11125, para 63. See also Case M 4731 *Google/DoubleClick* decision of 11 March 2008. See Case M 7217 *Facebook/WhatsApp* decision of 3 Oct 2014.

[15] See Peter Swire, 'Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall' (18 Oct 2007) <link>. See also Pamela Harbour and Tara Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (2010) Antitrust Law Journal 769-97.

[16] A third line of argument links the accumulation of too much information with the potential to foster first-degree price discrimination, which could be captured by competition law. See Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (Oxford UP 2016) 88-9. See also Wolfgang Kerber, 'Digital markets, data, and privacy: competition law, consumer law and data protection' (2016) 11(11) Journal of Intellectual Property Law & Practice 856-66.

into a competition analysis as a quality (non-price) parameter and to reflect on some of the scepticism surrounding this issue.

Price is often viewed as the chief competition parameter although competition policy is 'as concerned with quality as it is with prices'.[17] Part of the reason for focusing on price is that in most cases, quality can be factored into the price, meaning that price considerations will also cater to quality aspects. However, the reliance on price to factor in quality starts to break down when the product or service is offered for 'free', as is the case with the most popular digital services, such as Facebook and Google search. In such cases, one alternative is to consider the personal data collected by such entities as either the price paid by the user in return for receiving the 'free' product or as a dimension of product quality.[18] In the *Microsoft/Yahoo!* merger, the Commission indicated that when a product is free, quality becomes an essential and significant competition parameter.[19] As a result, privacy is attracting a considerable amount of attention as a quality parameter when services are provided for 'free' and in exchange for personal data.[20] In the EU, mergers involving Facebook/WhatsApp and Microsoft/LinkedIn were the most recent decisions articulating privacy-as-a-quality (non-price) parameter. In the former, the EC considered that in markets for consumer communications, data privacy and data security constitute key parameters of non-price competition that need to be factored into the merger assessment.[21]

In the most recent decision involving Microsoft/LinkedIn, the EC further affirmed this stance, claiming that privacy 'can be taken into account in the competition assessment to the extent that consumers see it as *a significant factor of quality*' and indicating that 'data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the

[17] OECD, 'Policy Roundtables: The Role and Measurement of Quality in Competition Analysis', (2013).
[18] Eleonora Ocello, Cristina Sjödin, and Anatoly Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case' (2015) 1 *European Commission-Competition Merger Brief* 6.
[19] *Microsoft/Yahoo! Search Business* (n 1), para 101.
[20] However, this does not necessarily mean that privacy is not relevant when services are exchanged for a price. This is consistent with the Commission finding that loss of 'confidentiality' could be considered product degradation, even for services where money changes hands. See Case M 4854 *TOMTOM/ TELE ATLAS* decision of 14 May 2008, paras 272-75.
[21] *Facebook/WhatsApp* (n 14), para 87.

transaction'.[22] There is a similar vigour at the national level. A report issued by the UK Parliament concurred with this line of thought, stating that the degradation of privacy standards by dominant online platforms could potentially constitute the abuse of market position under EU competition rules.[23] In a joint report entitled 'Competition Law and Data', the French and German Competition authorities also indicate that a merger of companies that compete on privacy-as-a-quality dimension could lead to a reduction of such quality, which needs to be factored into merger assessments.[24]

The privacy-as-a-quality approach has also received a fair share of attention in the United States. In the Google/DoubleClick merger, the FTC acknowledged that mergers can 'adversely affect non-price attributes of competition, such as consumer privacy'.[25] In a thought-provoking dissenting opinion to the FTC's decision and a subsequent co-authored law journal article, then Commissioner Pamela Harbour criticizes the majority for focusing only on the services market and suggests the need for considering 'privacy related markets'.[26] Noting that the conventional analysis overlooks the privacy interests in data-mergers, Harbour insists on defining 'privacy related markets' when companies that have massive personal data merge, and she brings up the need to consider different theories of harm that make privacy 'cognizable' under competition law.[27] The growing importance of privacy for consumers necessitates that competition law recognize 'privacy' as a competition dimension.[28] This implies that a competition analysis ought to consider whether a merger or achieving a dominant position changes the incentives to compete on privacy and privacy policies.[29] Another FTC commissioner, McSweeny, remarked that privacy and data protection could constitute a 'quality dimension of non-price competition', something which competition law ought

[22] European Commission - Press release, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions' (Brussels, 6 December 2016).
[23] The UK House of Lords, Select Committee on European Union, 'Online Platforms and the Digital Single Market' (10th Report of Session 2015-16, 20 April 2016), para 180.
[24] See Autorite de la Concurrence and Bundeskartellamt, 'Competition Law and Data' (2016) 24. See also a report by the Japan Fair Trade Commission, 'Report of Study Group on Data and Competition Policy' (2017) 38 (noting that in certain digital markets such as markets for Social Network Sites (SNS) 'the degree of privacy protection could be regarded as a component of product quality').
[25] See Statement of FEDERAL TRADE COMMISSION Concerning Google/DoubleClick FTC File No. 071-0170 (2007).
[26] See Dissenting Statment of Commissioner Harbour (n 5). See also Harbour and Koslov (n 15).
[27] Dissenting Statment of Commissioner Harbour (n 5) 10.
[28] Harbour and Koslov (n 15) 792-3.
[29] ibid 794.

to consider when diminished.[30] All in all, there is some measure of consensus among regulatory authorities and academics[31] that privacy could be factored in as a quality (non-price) parameter in competition analysis.

This notwithstanding, there is still significant uncertainty and scepticism about what constitutes degradation of privacy, whether monopolies have sufficient economic incentive to degrade privacy and how such a reduction affects effective competition. For example, James Cooper claims that 'On its face the privacy-as-quality analogy is appealing. Upon closer inspection, however, the analogy breaks down'.[32] Moreover, Geoffrey Manne and Ben Sperry state that 'privacy advocates have failed to prove a product quality case'.[33] This chapter is perhaps an initial step in filling in this apparent gap in the literature. I do not intend to provide an answer to the proper role of privacy in an antitrust analysis in general, but rather to investigate and cast some doubt on some of the privacy-specific uncertainties and scepticism surrounding the quality-based arguments, while highlighting how the privacy legal system and competition law may interact.

The remainder of this chapter is structured as follows: Section 2 highlights the quality-based theory of harm, particularly what constitutes a reduction in privacy-as-a-quality parameter. Section 3 identifies and addresses some of the scepticism in relation to the quality-based arguments. Three sources of scepticism are dealt with. Section 3.1 responds to the lack of a link between privacy harms and the accumulation of too much information. Section 3.2 deals with the claim that monopolies have little or no economic incentive to reduce privacy. Section 3.3 addresses the alleged trade-off between privacy harms and quality improvements. Finally, Section 4 discusses the role of data privacy law in understanding and determining the degradation of privacy in competition law assessments.

[30] European Data Protection Supervisor-BEUC Joint Conference, 'Big Data: Individual Rights and Smart Enforcement' Remarks of Commissioner Terrell McSweeny (Brussels, 29 September 2016) 9.
[31] For privacy and quality based scholarship, see, among others, Richard Pepper and Paul Gilbert, 'Privacy Considerations in European Merger Control: A Square Peg for a Round Hole' (2015) 5 *Antitrust Chronicle.* Ocello, Sjödin, and Subočs (n 18). Allen Grunes and Maurice Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (2015) *Antitrust Source*. Darren Tucker, 'The Proper Role of Privacy in Merger Review' (2015) 2 CPI Antitrust Chronicle.
[32] James Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity' (2012-2013) Geo. Mason L. Rev 1135.
[33] Geoffrey Manne and Ben Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (2015) 2 *Antitrust Chronicle* 3.

3. Theory of Harm behind Privacy-as-a-Quality

The quality-based argument was initially articulated in a testimony provided by Professor Peter Swire to the FTC Commission for the Google/DoubleClick merger. Swire argues that a merger that leads to 'a less privacy-protective structure' reduces consumer welfare because consumers, particularly those with high privacy preferences, 'pay more for a good if greater privacy intrusions are contrary to their preferences'.[34] Accordingly, as with any other harm to consumer preferences, harms to consumers' privacy preferences should be part of the traditional antitrust analysis. Swire further concretises this argument by elaborating how the Google/DoubleClick merger reduces the quality of the search product for consumers with 'high privacy preferences'.[35]

Reduction in the quality of a product or service is a standard category of antitrust harm, and privacy harms could constitute reductions in the '*quality of a good or service'*, which should be accounted for and minimised in the standard antirust analysis.[36] Noting that Google has 'deep' and DoubleClick has 'broad' information about individuals, the merger, Swire argues, could lead to a search product that is based on 'deep' and 'broad' information collection.[37] Google collects massive amounts of personal data through a number of its online services, including e-mail, search, map service, video sharing, browser and Google analytics—leading to 'deep' information about individuals. DoubleClick, on the other hand, is a company with a variety of tools and targeting services that enable websites to display graphic-based ads to visitors and monitor the ads' performance. In so doing, DoubleClick has amassed a 'broad' array of information about consumers by tracking their browsing behaviour across millions of websites. According to Swire, the combination of Google's 'deep' and DoubleClick's 'broad' information about consumers may lead to 'a significant reduction in the quality of the search product' for many individuals with 'high privacy preferences'.[38] Swire reasons as follows:

> "Before a merger, a consumer may be able to surf subject to one level of tracking, kept in a database of one magnitude. After the merger, doing a search

[34] Swire (n 15) 5.
[35] ibid.
[36] ibid. [Emphasis in original].
[37] ibid.
[38] ibid.

> or doing other surfing may carry with it a significantly higher level of tracking, in a larger database. To the extent that is true, then antitrust regulators should expect to assess this sort of quality reduction as part of their overall analysis of a merger or dominant firm behavior."[39]

The underlying idea behind Swire's argument is that privacy is a quality component of the search service, and providing such service based on the combined data from Google and DoubleClick reduces the quality of the search product.[40] In this regard, the amount of data collected and used to provide a certain service is a relevant consideration when assessing the level of privacy and the overall quality of the product. In clearing the merger, the FTC noted that it 'has investigated the possibility that this transaction could adversely affect consumers' privacy' but 'the evidence does not support a conclusion that it would do so'.[41] Although the FTC subscribes to the idea that privacy constitutes a non-price competition parameter in the merger, it offers little help regarding when and how a merger could be considered to reduce consumer privacy.

Similar decisions from the European Commission that recognize privacy as a non-price competition parameter leave the question largely unanswered. For example, in Facebook/WhatsApp, although the Commission identifies privacy as a key parameter of competition in the market for consumer communications,[42] it did not specifically assess how the merger might impact this competition parameter. However, the Commission did come up with an important caveat on the limits of competition law and pointed out that 'Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules'.[43] In this sense, the Commission seems to reject the argument

[39] ibid.
[40] Needless to say, privacy is not the only quality component of a search service. Thus, if the reduction in privacy improves other quality aspects, for example, relevance of the search results, it must be balanced against these improvements. This aspect is specifically dealt with under Section 3.3.
[41] Google/DoubleClick FTC File (n 25) 2-3.
[42] *Facebook/WhatsApp* (n 14), para 87.
[43] ibid para 164. However, Stucke and Grunes criticize the Commission for erroneously 'assuming that any privacy-related concerns flowing from the increased concentration of data were beyond the scope of competition law'. See Stucke and Grunes (n 16) 81.

that the combination of data from merging parties as such constitutes a reduction in privacy.

This notwithstanding, the Commission did assess how a reduction in privacy might serve as a constraint on the merged entity's incentive to introduce targeted advertisements in WhatsApp, which could reinforce Facebook's position in the online advertising market.[44] The Commission noted that this would be unlikely because WhatsApp would have to change its privacy policy and start collecting more data from users.[45] More particularly, the Commission noted that if the merged entity were to collect more data (age, gender, country and message content) from WhatsApp users, some users may switch to other texting apps that are 'less intrusive' and ad free.[46] Moreover, the Commission stated that the introduction of ads might also lead to abandoning the end-end encryption in WhatsApp, which might create dissatisfaction among users who value their privacy.[47] In this regard, the Commission referred to a submission showing that following the announcement of the acquisition by Facebook, a large number of German WhatsApp users downloaded alternative messaging services such as Threema.[48] Although the Commission did not explicitly articulate the relationship between more data and reduction in privacy-as-a-quality, it did, *albeit* indirectly, highlight that collecting more data to introduce targeted ads could reduce privacy or prompt privacy-sensitive users to switch to texting apps that afforded greater privacy protection. In other words, demanding more data from users could constitute a reduction in privacy in so far as it results from reduced competition in the market.
Strengthening the above claim is a comment made by some Commission officials on the merger, who argued as follows:

> A website that, post-merger, would start requiring *more personal data* from users or supplying such data to third parties as a condition for delivering its 'free' product could be seen as either increasing its price or as *degrading the quality of its product*. In certain circumstances, this behaviour could arguably amount

[44] *Facebook/WhatsApp* (n 14), para 174.
[45] ibid para 174 and 186.
[46] ibid.
[47] ibid para 174.
[48] ibid. Threema advertises itself as a service designed 'to protect the users' privacy – an app that stores as little as possible and prevents surveillance and data misuse'. See Threema Press Release, 'Threema: The Best Selling Secure Messenger' (*Threema Press-Info*, 22 Dec 2015) <link>.

to an infringement of competition law (irrespective of whether or not it also constitutes an infringement of data protection rules).[49]

Other commentators have also expressed similar views.[50] Hence, more generally, a reduction in data privacy could be understood to involve an increase in the amount of personal data demanded or an increase in the use of the data (that is, usage for purposes other than initially promised).[51] Although variations to the quality-based argument might be found,[52] one underlying assumption behind such arguments is that more data or accumulation of 'too much' information of the consumers can lead to a degradation of privacy.[53] However, there is a strong scepticism toward such a quality-based theory of harm. In the following paragraphs, I shall address this scepticism.

4. Some Reflections on the Scepticism

There is no doubt that, like any other quality dimension, privacy suffers from subjectivity and measurability, and thus, it would be equally difficult to incorporate into a competition analysis. Given that these challenges of incorporating quality aspects into a competition analysis are widely extoled,[54] my focus is only on the privacy-specific sources of scepticism. The major ones relate to the lack of a link between privacy

[49] Ocello, Sjödin, and Subočs (n 18) 6. [Emphasis added].
[50] See, for example, Howard Shelanski, 'Information, Innovation, and Competition Policy for the Internet' (2013) University of Pennsylvania Law Review 1691-92 (higlighting that extracting 'more information' from customers without offering some benefit that offsets the reduced privacy could lead to consumer harm that needs to be considered under competition law). See Maurice Stucke and Ariel Ezrachi, 'When Competition Fails to Optimise Quality: A Look at Search Engines' (2016) 18 (70) *Yale J.L. & Tech.* 104 (noting the degardation of privacy as a quality if a firm can 'collect more personal data and provide less privacy protection for the data'). See Stucke and Grunes (n 16) 216 (arguing that a domaint player might reduce the quality of privacy by extracting 'more personal data than the firm otherwise could in a competitive market').
[51] Ania Thiemann and Pedro Gonzaga, 'Big Data: Bringing Competition Policy to the Digital Era', (OECD 2016) 19.
[52] Discussing the acquisition of WhatsApp by Facebook as an elimination of a maverick that improved the quality of texting apps by offering enhanced privacy protection. See Stucke and Grunes (n 16) 262. See also Harbour and Koslov (n 15), who dicuss the need for a competition analysis to account for whether a merger or achieving a dominant position changes the incentives to compete on privacy-enhancing technologies and privacy policies. See also the Commission decision in Microsoft/LinkedIn where the possibility of integrating and promoting LinkedIn through Microsoft Windows and Office products was considered to reduce consumer choice in relation to privacy. See *Microsoft /LinkedIn* (n 6), para 350. For an overview of the different theories of harm on privacy as a non-price competition parameter, see Samson Esayas. 'Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers' *University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2018-26* (2018) https://ssrn.com/abstract=3232701
[53] Swire (n 15) 5.
[54] See OECD (n 17). Stucke and Ezrachi (n 50). Keith Waehrer, 'Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions' (2015) <https://ssrn.com/abstract=2701927>.

harms and more data collection, the lack of economic incentive to reduce privacy and the alleged trade-off between privacy degradation and quality improvement.

The Lack of a Link between Privacy Harms and More Data Collection

One main source of scepticism when it comes to the quality-based argument is the lack of a link among more data collection, privacy degradation and consumer welfare. This scepticism could be looked at from three angles. The first angle disputes the lack of a link between the accumulation of more data in the hands of a single firm and the resulting privacy interests harmed by this accumulation. Manne and Sperry argue that 'for each consumer the 'problem' of a large concentration of information being accumulated in a single company is seemingly insignificant'.[55] In this regard, the very first task for privacy scholars and regulatory authorities is, according to Cooper and Wright, 'to articulate the privacy value being harmed' by the accumulation and use of personal data.[56] The second scepticism relates to the claim that even if the accumulation of data raises privacy concerns, consumers internalise, with the assistance of privacy agencies, the risks of disclosure and misuse of this information.[57] Thus, according to Manne and Sperry, there is little evidence that 'accumulation of too much information' about other people and a consumer 'increases the uncertainty of this risk assessment, or makes harm to the individual consumer more likely'.[58] The third scepticism disputes the possible link between privacy harms and consumer welfare, which is often associated with economic efficiency, under competition law. Disputing this link, Manne and Sperry argue that that 'there is … no necessary (or even likely) connection between more data collection and use and harm to consumer welfare'.[59] This section reflects on these concerns by identifying the relevant privacy interests in the accumulation of data and then critiquing some of the associated scepticisms.[60]

---

[55] Manne and Sperry (n 33) 4.
[56] James Cooper and Joshua Wright, 'The Missing Role of Economics in FTC Privacy Policy' in Jules Polonetsky, Evan Selinger and Omer Tene, eds., *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2017 forthcoming) 18 manuscript available <https://ssrn.com/abstract=2894438>.
[57] Manne and Sperry (n 33) 3.
[58] ibid 3-4.
[59] ibid 6. Manne and Sperry are not alone in taking such a position. See also Cooper (n 32).
[60] Much of the text used to address the scepticism in Section 3.1 is adopted from Samson Esayas, 'The Idea of 'Emergent Properties' in Data Privacy: Towards a Holistic Approach' (2017) 25(2) International Journal of Law and Information Technology 139-78.

Thus, the aim in this section is threefold. The first is simply to establish a link between the 'accumulation of too much data' and privacy concerns. To this end, three specific privacy interests that are threatened by accumulation and aggregation practices are identified. First, the accumulation of too much information about an individual, collected by expanding to a broad array of new product areas or through the acquisition of companies, overexposes the individual and thereby undermines his or her free choice. Second, and related to the first, too much information about consumers, including information about other consumers, makes protecting one's privacy costly and leads to the loss of practical obscurity. Third, the accumulation of too much information, at least in the EU context, distorts the very foundation upon which transparency and accountability mechanisms are built, which then makes it almost impossible to hold entities accountable for non-compliance of data privacy rules.

Before proceeding further, some point of caution is in order. It can be argued that these issues are not competition concerns, and I tend to share some of this scepticism. In fact, I have argued elsewhere for an enhanced responsibility regime under data privacy for certain actors based on the totality of the channels (products or services) through which an entity collects data from individuals and data aggregation practices.[61] This is akin to the regulation under competition law, where companies with a dominant position have a special responsibility and are subject to closer scrutiny and oversight than others.[62] This notwithstanding, the dangers of overexposure go beyond just privacy interests, affecting interests that are relevant for competition. As shown further below, overexposure undermines 'innovative practice', that is, one's ability to freely tinker and experiment,[63] which is of interest for competition law. Similarly, overexposure facilitates 'digital market manipulation' which 'causes or exacerbates economic harms'.[64] In some cases, the accumulation of data about consumers and

[61] See ibid, particularly172 et seq.
[62] ibid.
[63] See Julie Cohen, 'What Privacy Is for' (2012) 126 Harv. L. Rev. 1919.
[64] Ryan Calo, 'Digital Market Manipulation' (2013) 82 Geo. Wash. L. Rev. 1026-1027. See also Nathan Newman, 'Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2013) 40 Wm. Mitchell L. Rev., 849.

related network effects can also give rise or exacerbate market power, which in turn leads to consumer harm.[65]

The second aim is to demonstrate that not all these issues are fully addressed under current data privacy rules and not necessarily internalised by consumers, even with the help of regulators (focus on EU context). As argued elsewhere, these risks represent 'emergent properties' in the sense that the sum, that is, the aggregated and accumulated data, contains risks that are not present in the individual datasets (in EU terms, processing activities).[66] Against this background, the current EU data privacy rules focus on individual processing activity based on a specific and legitimate purpose, with little or no attention to the totality of the processing activities—that is, the sum—based on separate purposes.[67]

The third aim is to demonstrate that these kinds of privacy degradations (interests) are to some extent linked to economies of scale and scope. These are important considerations in gaining market power and a dominant position, and when achieved, bring entities into much closer scrutiny under competition law. In a similar fashion, scale and scope in services that generate data have a direct impact on the privacy interests of individuals in terms of their overexposure and the losses of accountability, transparency and practical obscurity. As discussed further below, the larger the number of channels (products or services) through which an entity collects and aggregates data on individuals, the more the individuals are exposed, and the more difficult it becomes to hold entities accountable for non-compliance with the data privacy rules.[68] I believe that these discussions can contribute to the debate on the

[65] See Nathan Newman, 'Search, Antitrust, and the Economics of the Control of User Data' (2014) 31 *Yale J. on Reg* 440-41 (noting that, 'Ultimately, Google's monopoly in online search advertising is unassailable because no other company combines such a diverse set of data on users or is capable of deploying an ad at the "time of intent" when people search for a product or service.' This reduced competition in the online advertising market harms consumers because 'the higher prices charged to advertisers inevitably gets passed onto consumers in the form of higher prices for the advertised goods and services they buy'). See also Stucke and Ezrachi (n 50) 77-9 dicussing how data-driven network effects (scale and scope in data) together with behavioural consideraions (such as difficulty detecting reduction in quality) can protect a search engine from competition and allow it to reduce quality by favouring its own products.

[66] At its core, the concept of an emergent property, tracing its roots from the old Aristotelian dictum, underlines that 'the whole is more than the sum of its parts,' where the 'whole' represents the 'emergent property'. This kind of thinking allows system engineers to look beyond the properties of individual components in a system and understand the system as a single complex. See Esayas (n 60) 145.

[67] ibid.

[68] I do not claim that entities with smaller economies of scale and scope are not able to engage in these kinds of privacy violations, but such entities can easily be held responsible for these breaches under data privacy rules.

interplay among privacy, quality and market power.[69] To the extent that privacy degradations can be linked to market power, the quality-based arguments may have more appeal to competition authorities.

Accumulation of Too Much Information Makes Protecting One's Privacy Costly and Leads to a Loss of Practical Obscurity

While admitting the appeal of the quality-based arguments, Manne and Sperry question 'how having a larger amount of data could reduce nonprice privacy competition'.[70] According to them, 'it is difficult to see why a company's mere possession of private information about other people is of much concern to any particular consumer'.[71] There are two reasons why such accumulation could be problematic. First, the accumulation of too much information on people increases the costs of protecting one's privacy. In a seminal literature review of the economics of privacy, Acquisti et al. recount that 'protecting one's data becomes increasingly costly the more others reveal about themselves'.[72] Clarifying this claim, the authors show how having a social network account, such as Facebook, is becoming a must have to access some websites or services (free Wi-Fi). One such example is the dating app, Tinder, which can only be used if someone has a Facebook user ID. This imposes an additional cost on users who do not want to create a social media account.[73] Other scholars have also shown that the more data others willingly reveal about themselves, the more those who hold back the data become 'stigmatized and penalized'.[74]

The problem does not end there. Even the information that users choose not to reveal 'may still be inferred through the analysis of similar individuals who did not choose to protect theirs'.[75] Here, the popular anecdote involving the US retail outlet Target serves

[69] For further discussion on this issue, see Samson Esayas 'Competition in (Data) Privacy: 'Zero' Price Markets, Market Power and the Role of Competition Law' *International Data Privacy Law* (forthcoming 2018).
[70] Geoffrey Manne and Ben Sperry, 'The Law and Economics of Data and Privacy in Antitrust Analysis' (2015) *A Federal Trade Commission Workshop: The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators* 8.
[71] Manne and Sperry (n 33) 3-4.
[72] Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 (2) Journal of Economic Literature 446.
[73] ibid.
[74] Scott Peppet, 'Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future' (2011) 105 Nw. UL Rev. 1156.
[75] Acquisti, Taylor, and Wagman (n 72) 446.

as a good example. In this widely reported story, Target identified shopping patterns from its baby shower registry that contained purchasing data of women who willingly revealed their pregnancy.[76] Based on this analysis, Target identified the most common products that pregnant women would be likely to buy. These data were used to analyse the purchasing data of other female shoppers and to predict if they were pregnant. Based on this pregnancy score, Target sent discounts on baby-related products to customers not included on the baby shower registry, including a teenage girl.[77] Angry with such an offer being sent to his teenage daughter, the father of the girl reportedly visited the manager of the store to ask if Target was 'trying to encourage her to get pregnant', only to find out a few days later that his daughter was in fact pregnant.[78] This involves a serious breach of the data privacy of the teenage shopper,[79] which was made possible, to a larger extent, by the existence of the baby shower registry that contained the purchasing data of women who willingly revealed their pregnancies. This signifies the existence of negative externalities to third parties from the accumulation of data about a consumer or other consumers. In this regard, considering reduction in privacy, understood as an increase in the amount of personal data collected, as quality degradation can help firms internalise those externality costs.

Second and more generally, the accumulation of too much information leads to a loss of practical obscurity. In its broadest sense, practical obscurity represents the cost and practical difficulties one encounters in obtaining and compiling information on the private lives of individuals or, more generally, intruding on a person's privacy. Practical obscurity has served privacy a great deal, owing to the costs and difficulties associated with following and recording every footstep that individuals take. However, with the ubiquity of smartphones connected to the Internet 24/7 and the sinking cost of storage,

[76] Ariel Ezrachi and Maurice Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard UP 2016) 92.
[77] ibid 93.
[78] ibid.
[79] Solove compares the use of personal data for unrelated purposes to a 'breach of confidentiality, in that there is a betrayal of the person's expectation of privacy when giving out information'. See Daniel Solove, *Understanding privacy* (Harvard UP 2008) 131. Similarly, citing Nissenbaum, Cohen describes such a problem as 'disruption of contextual integrity'. See Julie Cohen, 'Privacy, Visibility, Transparency, and Exposure' (2008) 75 (1) The University of Chicago Law Review 194. In the EU, the fairness principle under Art 5(1(a)) of the General Data Protection Regulation (hereinafter GDPR) ensures that the processing of personal data does not exceed the expectation of individuals and that its further processing is not objectionable in light of these expectations. See 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 OJ L119/1 (GDPR). .

companies are able to track and record every digital footprint of an individual through his or her mobile and browsing habits. The more data that are collected, recorded and combined, the more practical obscurity becomes almost a lost cause.

In a recent article titled 'The Transparent Citizen',[80] Reidenberg cites one example from the United States where the federal government sought information about pornography and issued subpoenas to the five largest search engines, ordering them to log files for all user search requests during a specific period.[81] In the absence of such platforms, Reidenberg argues, the alternative would have been to wiretap a large portion of net traffic. For one, this would be a very costly exercise for the government to conduct.[82] Even more so, this 'is something the government chose to avoid' because '[i]t would have faced strict legal constraints, namely the need for search warrants for each of the individual account holders'.[83] In this sense, the circumvention of the constitutional safeguards—that is, the need to obtain a search warrant—is facilitated by the loss of practical obscurity. The loss of practical obscurity, in turn, is facilitated by the accumulation of massive data about individuals within private entities and, more importantly, by their practices of aggregation of data about individuals. In addition, governments can look to data-aggregating companies, such as ChoicePoint, to connect the missing links.[84] Thus, the accumulation of massive data about individuals and aggregation practices by private entities not only makes it cheaper or even cost-free for governments to engage in what could have been a costly conduct, but also provides a way of circumventing constitutional safeguards.[85]

There is also an emerging case law showing how the accumulation of data from different sources creates privacy risks that do not exist in individual datasets. In the EU, this line of reasoning is observed in the Court of Justice of the European Union's (CJEU) judgement that invalidated the Data Retention Directive.[86] In that judgement, the Court emphasised the wide array of data on a private person that providers of

[80] Joel Reidenberg, 'The Transparent Citizen' (2015) 47 Loyola University Chicago Law Journal.
[81] ibid 117.
[82] íbid.
[83] ibid.
[84] *Democracy Now*, 'Data and Goliath: Bruce Schneier on the Hidden Battles to Collect Your Data and Control Your World' (13 March 2015) <http://www.democracynow.org/2015/3/13/data_and_goliath_bruce_schneier_on>
[85] ibid.
[86] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Others* ECLI:EU:C:2014:238, para 26.

electronic communication services or networks are required to retain, including data concerning the following:

> The source of a communication and its destination, … the date, time, duration and type of a communication, … users' communication equipment, and … the location of mobile communication equipment, the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services.[87]

According to the Court, '[t]hose data, *taken as a whole*, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained...'.[88] The reference of 'taken as a whole' reflects some emergent property reasoning in the sense that although the retention of different sets of data individually might not constitute a breach of the rights of individuals, collectively, they constitute a breach of the right to respect a person's private life and the fundamental right to the protection of personal data.

There is similar emerging case law from the US Supreme Court showing that the *volume* and *variety* of data create a 'reasonable expectation' of privacy in situations that are traditionally outside the protection of the Fourth Amendment.[89] For example, in the *US v Jones,* Justices Alito and Sotomayor concurred with the DC Circuit Court's stance that although it might be legal for the government to carry out GPS tracking of single trips in public spaces, the aggregation of numerous trips over the course of a month becomes illegal because it reveals more private information than the individual constituent parts (individual trips or locations).[90] In other words, individuals may not have a reasonable expectation of privacy for their single public movements, but an aggregation of these single public movements could create a reasonable expectation of privacy. Thus, the accumulation of 'too much data' about an individual or about others increases the cost of protecting one's privacy and can give rise to privacy risks that do not exist in individual datasets.

[87] ibid.
[88] ibid para 27 (emphasis added).
[89] See Case *US v Jones* 132 Supreme Court (2012) 945. See also *Riley v California* 134 Supreme Court (2014) 2473.
[90] See Case *US v Jones* (n 89) 964.

Overexposure of the Individual Undermines Free Choice

The growing importance of personal data for commercial purposes, coupled with the ever-sinking cost of storage, is creating a drive for a 'digital land grab', shifting the priorities of organisations to collect and harness as much personal data as possible to maximise their market position.[91] This desire is being pursued using legitimate grounds, such as expanding to new product sectors and acquiring entities with valuable personal information. Now under the umbrella of parent company Alphabet,[92] Google's aggressive expansion to a broad array of new product areas is a case in point. An investigation from 2013 by the Spanish Data Protection Authority shows that Google collects personal data through nearly 100 'consumer-facing products or services',[93] of which more than 70 are offered for free. This number is not only a result of legitimate acquisitions, but also controversial practices of nudging users to consume the new product or subscribe to the service launched. When launching its social networks, individuals with a Gmail account were automatically given a Buzz account (now defunct) and later a Google+ account.[94] Furthermore, companies combine data across these different processing activities based on separate purposes.[95] The end result is a large pool of processing activities involving data that are collected legally and controversially. Accumulating personal data from multiple sources together with data aggregation overexposes individuals, thereby undermining their ability to freely choose or consent.

Apart from the personal information collected during product or service registration, as part of its YouTube service, Google collects data on the types of videos a user watches and the user's likes and dislikes. As part of its search function, Google obtains insights on what products a user is interested in, the books he or she might want to purchase or an illness he or she might have. Google knows one's contact list from Gmail,

[91] White House, 'Big Data: Seizing Opportunities, Preserving Values' (Executive Office of the President 2014) 54.
[92] For the purposes of this article, I use Google instead of Alphabet because of the familiarity of the name 'Google'.
[93] See Agencia Española de Protección de Datos Press Release, 'The AEPD Sanctions Google for Serious Violation of the Rights of the Citizens' (19 December 2013) 1 <https://googleblog.blogspot.ca/2012/01/updating-our-privacy-policies-and-terms.html>.
[94] See Alexei Oreskovic, 'Google Linking of Social Network Contacts to Email Raises Concerns' *Reuters* (9 January 2014) <http://www.reuters.com/article/us-google-gmail-idUSBREA081NH20140110>
[95] Google's 2012 change of privacy policy is a good example. See Google Official Blog, 'Updating Our Privacy Policies and Terms of Service' (24 January 2012) <https://googleblog.blogspot.ca/2012/01/updating-our-privacy-policies-and-terms.html>.

Google+ and Groups. Google knows one's gathering places from Calendar and Maps. One's locations are further revealed through Maps, Search and Earth, and Android GPS tracks one's location, even when no apps are running. Credit card and bank information are accessible if one uses CheckOut, Finance or Google Wallet. Search, Gmail, Books and Health (before its discontinuation) might contain health information. Talk, Voice, Maps and Calendar signal destination plans. One's browsing habits are monitored and recorded through Google Chrome.

Even more, through GoogleX, Google is becoming an Internet service provider, offering Wi-Fi, wireless broadband (Fi) and fibre, providing a window into virtually everything a user does on the Internet. What people write (and think) is scanned from Gmail attachments, Google Drive and Dropbox. Millions of mobiles run on Google Android. Moreover, through its Nest Cam, Google is promising to 'help you look after your home and family – even when you're away. With 24/7 live streaming, advanced Night Vision, activity alerts, one app for all your Nest products, and a versatile magnetic stand, Nest Cam helps you keep an eye on what matters'.[96] Through its Analytics service and DoubleClick, Google collects the browsing habits of individuals from millions of third-party websites. The list goes on; there is hardly anything that Google does not do or plan to do.[97] Organisations also resort to controversial means of collecting user data. The Google Street View Project is a good example; here, Google accessed the communication of individuals transmitted over Wi-Fi networks in many countries, which also led to fines and confiscation of properties, for example, in North Korea.[98] It is claimed that the access was deliberately designed because the resulting data are considered instrumental for the success of Google Maps and self-driving cars.[99]

Essentially, Google can be one's browser, search engine, messenger, guide for driving and taking public transport and a platform for writing and storing files. Mobile

[96] Nest Cam website <https://nest.com/ie/camera/meet-nest-cam/>

[97] This includes smart fabric or clothing, contact lenses and watches. See Zach Miners, 'Google's Project Jacquard to Make Smart Fabric for Smart Clothing, Levi's First Official Partner' *PC World* (29 May 2015) <http://www.pcworld.com/article/2928372/this-smart-fabric-from-google-can-change-the-music-and-turn-off-the-lights.html> accessed 30 Dec 2016

[98] See Mark Burdon and Alissa McKillop, 'The Google Street View Wi-Fi Scandal and Its Repercussions for Privacy Regulation' (2014) 39 Monash University Law Review 702.

[99] See Yasha Levine, 'Google's For-Profit Surveillance Problem' *PANDO* (16 December 2013) <https://pando.com/2013/12/16/googles-for-profit-surveillance-problem/> accessed 30 Dec 2016, arguing that '[i]t was all part of the original program design: Google had equipped its Street View cars with surveillance gear designed to intercept and vacuum up all the wireless network communication data that crossed their path'.

phones run on Google. It will not be long before Google cars flood the streets. Even people's houses are coming under Google's surveillance cameras. This means that even the use of a fraction of these services creates a transparent data subject, an individual who exposes significant aspects of his or her life willingly to use the services. This may lead both to non-economic (purely privacy) and economic harms.

Such practice of accumulation, as David Lyon comments, 'renders ordinary everyday lives increasingly transparent to large organizations'.[100] A central objective of the data privacy rules is to allow the individual to selectively self-disclose his or her information based on free choice, referred to as information self-determination, thereby preventing undue interference in the individual's autonomy, integrity and dignity. This ensures the protection of the individual from 'manipulation or control by others'.[101] However, the more exposed an individual becomes, the easier it is to 'force his obedience' and suppress his or her capacity to make free choices.[102] Such limitless knowledge of the individual transforms into a significant power imbalance, where entities (private and government) become 'omnipotent parents and the rest of society … helpless children'.[103] Harcourt echoes similar views, claiming that overexposure renders individuals open and accessible to serve idiosyncratic corporate and governmental interests.[104]

Overall, overexposure makes individuals powerless, turning them into predictable citizen-consumers who can easily be stimulated and nudged to serve profit-maximising goals.[105] Thus, it is not a mere happenstance that big companies such as Facebook and Google are increasingly coming under closer scrutiny for their undue power to influence the voting behaviour of users.[106] For example, Facebook triggered outcries

[100] David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' (2014) 1 (2) *Big Data & Society* 4.
[101] Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law Intl 2002) 133-4.
[102] Paul Schwartz and Joel Reidenberg, '*Data Privacy Law'* (Michie 1996) 39; see also Daniel Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stan L. Rev 1396.
[103] Schwartz and Reidenberg (n 102) 39; see also Solove (n 102) 1396.
[104] Bernard Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Harvard UP 2015) 454-5 (Kindle locations) 289-92 and 482-6 (noting that the more exposed we are to others, the more we lose 'our sense of control over our destiny and self-confidence, our sense of self').
[105] Cohen (n 63) 1919.
[106] Robert Bond and others, 'A 61-Million-Person Experiment in Social Influence and Political Mobilization' (2012) 489 (7415) *Nature* 295.

for manipulating users' behaviours through two separate experiments conducted on its users, including its power to influence users' turnout in elections by hundreds of thousands.[107] Many have written about the power of Google to swing election results.[108] These experiments have shown how easily a social network or search engine with a deep knowledge of individuals' personal details can influence users' moods and even their voting behaviours.[109]

In this regard, it is important to note the link between the economies of scope and scale and the resulting exposure of individuals. The more data the entity knows about the individual, either by widening the arenas for collection or through the acquisition of companies with information, the more exposed individuals become, particularly if there is a possibility of combining data across these processing activities, and the more difficult it becomes for individuals to control self-disclosure and exercise free choice. For example, one study claims that firms that offer diverse services (that is, more economy of scope) find it easier to convince consumers to consent than new entrants and small and medium enterprises (SMEs).[110] It could be argued that the more services consumers use from an entity, the more they come to trust the company, and thus, the company can easily obtain consent. However, this claim bears little relation to reality. According to a Eurobarometer survey, 63 per cent of Europeans do not trust online businesses, such as search engines.[111] Thus, an alternative explanation could be that when consumers use diverse services from a single entity, they become so dependent that they develop a sense of helplessness and are unable to refuse the provision of consent.[112] Even more important is the claim by Schwartz and Reidenberg that the

[107] Adam Kramer, Jamie Guillory and Jeffrey Hancock, 'Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks' (2014) 111 (24) *Proceedings of the National Academy of Sciences.*
[108] See Jonathan Zittrain, 'Engineering an election' (2013) 127 Harv. L. Rev. F. 335. Robert Epstein and Ronald E Robertson, 'The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections' (2015) 112 (33) Proceedings of the National Academy of Sciences E4512-E4521.
[109] Bond and others (n 106).
[110] James Campbell, Avi Goldfarb and Catherine Tucker, 'Privacy Regulation and Market Structure' (2015) 24 (1) Journal of Economics & Management Strategy 47.
[111] Special Eurobarometer 431, Data Protection (European Commission 2015) 63.
[112] ibid 7 (noting that most Europeans [71 per cent] 'say that providing personal information is an increasing part of modern life and accept that there is no alternative other than to provide it if they want to obtain products of services'). See also Joseph Turow, Michael Hennessey, and Nora Draper, 'The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them up for Exploitation' (2016) <http://ssrn.com/abstract=2820060> 3 (recounting that 'a majority of Americans are resigned to giving up their data—and that is why many appear to be engaging in trade-offs. Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them').

more the company knows the individual, the more ability it has to force the individual's obedience and suppress free choice.[113] This in turn undermines one's ability to selectively disclose information (data privacy interest).

However, the potential harms from the accumulation of data and resulting overexposure are not limited to privacy; these harms can affect interests that are directly relevant for competition law. For example, it is argued that privacy is an essential prerequisite for creativity. This argument is primarily advanced by Julie Cohen. Cohen underlines the paramount importance of innovative practice—that is, one's ability to freely tinker and experiment—for innovation.[114] Innovation does not emerge from a vacuum; instead it requires a capacity for critical reflection and 'a room to tinker'.[115] Understood this way, innovation thrives best when privacy is adequately protected because privacy guards the space for tinkering and experimentation, which in turn drives innovation.[116] In contrast, Cohen argues, an environment with diminished privacy, for example, with constant surveillance, promotes conformity and impairs innovation.[117] If individuals' space for critical reflection and their capacity for tinkering are not adequately protected, creativity is stifled, and innovation is hampered.[118]

Overexposure can also facilitate what Ryan Calo refers to as 'digital market manipulation', which 'causes or exacerbates economic harms'.[119] For example, companies, especially platforms, can use their knowledge of the user together with behavioural biases to extract consumer surplus through dynamic price discrimination and persuasion profiling.[120] Although the welfare effects of price discrimination are often unclear, sometimes, Calo argues, such digital market manipulation could 'hinder or distort competition and impose an outsized burden on the least sophisticated consumers'.[121] At a minimum, digital market manipulation could give rise to a 'behaviour by one or more market participants that generates externalities and

[113] Schwartz and Reidenberg (n 102) 39.
[114] Cohen (n 63) 1919.
[115] ibid.
[116] ibid 1906.
[117] ibid.
[118] ibid 1927.
[119] Calo (n 64) 1026-27. For a more detailed analysis of how behavioural price discrimination may fit into antitrust, see Newman (n 64) 849.
[120] Calo (n 64) 1026-27.
[121] ibid 1026.

decreases overall market efficiency'.[122] More importantly, as shown in Section 3.3, the accumulation of data about consumers and related network effects can give rise or exacerbate market power.[123] This could lead to consumer harm both in the form of higher prices to advertisers that inevitably gets passed to consumers in the form of higher prices on the final goods and in the form of lower quality products (suppressing competition in privacy-enhancing technology or less relevant search results).[124]

Accumulation and Aggregation Weakens Consumers' and Regulators' Ability to Hold Entities Accountable for Non-Compliance with the Data Privacy Rules

In this section, I demonstrate how the accumulation of data, be it through expanding the channels of collection or acquisition of companies, distorts the very foundation, at least in the EU context, upon which the transparency and accountability mechanisms are built. This implies that even with the assistance of data privacy authorities, consumers might not be able to internalise the risks associated with the accumulation of too much data about them. Before proceeding to this, a few words about the EU data privacy framework and its challenges with the scale and scope of data.

The Atomised Approach and its Challenges with the Scale and Scope of Data

The protection of the data privacy rights of individuals in the EU, and to a certain extent the United States, is based on compliance with certain core data privacy principles.[125] Of particular importance to the discussions in this chapter is the purpose limitation principle, which stipulates that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.[126] The principle is considered the 'cornerstone of data protection' legal

[122] ibid 1027.
[123] Newman (n 65) 440-1. See also Stucke and Grunes (n 16) 204, noting that data-driven network effects (scale of data/trial-by-error, scope of data and spill-over) can entrench dominance and facilitate anticompetitive behaviour. See also Stucke and Ezrachi (n 50) 84.
[124] Newman (n 65) 441. See also Stucke and Ezrachi (n 50) 84. See also Harbour and Koslov (n 15).
[125] The core principles of EU data privacy are anchored in Article 5 of the GDPR (n 79). These include the lawfulness and fairness principle (Art 5(1(a)), purpose limitation principle (Art 5(1(b)), data minimization principle (Art 5(1(c)), accuracy or data quality principle (Art 5(1(d)), the principle on storage limitation (Art 5(1(e)) data security principle (Art 5(1(f) and accountability principle (Art 5(2)).
[126] GDPR (n 79) Art 5(1(b)).

framework.[127] This is mainly because it is an essential prerequisite in the application of data privacy rules in general and for the other principles under Article 5 of the GDPR. For example, a regulator or an internal auditor who is interested in assessing the compliance of a particular processing activity should be able to identify the *specific purpose* for which the personal data were collected; if there is a legitimate basis and if this legal basis suits the particular *purpose*; if the data collected were the minimum necessary for the *purpose*; if the data collected were accurate and up-to-date for that particular *purpose*; if the personal data are not stored for longer than necessary to achieve the *purpose*; and if the processing of such data is fair (that is, it does not exceed the expectations of individuals, which is assessed regarding the initial *purpose*).

The use of the term 'purposes' (plural) under Art. 5(1(b)) of the GDPR[128] implies that personal data can be collected for more than one purpose. In such cases, the Article 29 Working Party, a group composed of national Data Protection Authorities, requires that 'each separate purpose should be specified in enough detail to be able to assess whether collection of personal data for this purpose complies with the law' and '*the data quality requirements must be complied with separately for each purpose*'.[129] This implies that when an entity processes personal data for multiple purposes, each processing must comply with the data privacy principles separately in light of the specific purpose and the relevant legal basis. This represents an individualistic view of processing; in other words, the assessment of compliance focuses on the individual processing based on a specific purpose and distinct legal basis, regardless of the total number of processing activities and data aggregation practices across the different processing operations.

This (atomised) approach relies on two underlying assumptions: (i) distinguishing among different processing activities and relating every piece of personal data to a particular processing is possible and (ii) if each processing is compliant, the data privacy rights of individuals are not endangered. However, these assumptions are untenable in an era where companies process personal data for a panoply of purposes, where almost all processing generates personal data and where data are combined

[127] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' [2013] (hereinafter, WP203) 4.
[128] GDPR (n 79).
[129] WP203 (n 127) 12 and 16 [emphasis added].

across several processing activities. These practices blur the lines between different processing activities and complicate attributing every piece of data to a particular individual processing. Moreover, when entities engage in these practices, there are privacy interests independent of and/or in combination with the individual processing activities.

A salient example is Google's aggressive expansion to a broad array of new product areas, ranging from e-mail, search, map service, video-sharing, social network, mobile operating system, payment service and so forth. As noted above, Google offers more than 100 services and combines data collected across these different services based on separate purposes.[130] The focus on individual processing activity means that compliance with the data privacy rules, for example, in relation to Gmail, will be assessed on its own, as will the processing of data in relation to Google+, YouTube, Search and the remaining (close to 100) Google services. At least, this would have been the approach before Google decided to consolidate the services under one account.[131] This, however, overlooks the fact that the totality of personal data collected based on separate purposes and/or the combination of data across these processing activities could be, as discussed above, a source of concern for the individual (for example overexposure) or society at large (for example, loss of practical obscurity).

Moreover, the existing accountability and transparency mechanisms based on the purpose limitation principle start to break down when the entities engage in accumulating and aggregating combining data across different services based on separate purposes. Both transparency and accountability are central elements of the purpose limitation principle because having a specific and explicit purpose for processing enables data controllers to be transparent both to regulators and data subjects about how they use personal data, thereby ensuring the accountability of entities processing personal data.[132] Transparency is related to the openness of the data-processing entities toward both data subjects and regulators on what data are collected, for what purpose and how the data are used.[133] Furthermore, accountability is related to the responsibility of the parties, particularly the controller, to implement

[130] Google's 2012 change of privacy policy is a good example. See the Google Official Blog (n 95).
[131] Or the alternative is to try and find a legitimate and specific purpose under the umbrella of generic 'Google services', which essentially makes the purpose specification and limitation principle, and other principles that are built on it, ineffective.
[132] WP203 (n 127) 18
[133] See GDPR (n 79) Art. 5(1(a) and Arts 12-14.

and demonstrate compliance with the data privacy principles enshrined under Article 5(1) of the GDPR.[134] However, the aggregation of data across different services or products obscures the transparency in terms of what data have been collected, for which purpose(s) and whether the data are necessary for that (those) particular purpose(s). Similarly, assessing whether a certain reuse of data is or is not compatible with the original purposes becomes very challenging, which then makes it almost impossible to hold entities accountable for non-compliance with the data privacy rules. The losses of transparency and accountability, in turn, make it difficult for individuals to understand and enforce their rights. Although this may not constitute an economic harm in itself, such loss of transparency and accountability in turn could contribute to harms that are relevant for antitrust. For example, Newman discusses how the lack of transparency contributes to consumer harm through consumer exploitation, where consumers surrender their data to a monopolist 'at an artificially low price'.[135]

Overall, the above discussions demonstrate that the current data privacy rules are not well-suited to address problems associated with the scale and scope of data. In other words, when entities accumulate the personal information of individuals by entering into a wide array of areas and then aggregate data across those channels, there are 'emerging privacy risks', namely the overexposure of the individual and the loss of transparency, accountability and practical obscurity, all of which are not adequately addressed under the current data privacy rules.[136] Granted, it is not the antitrust's role to fill in the gaps in privacy laws, but it does demonstrate that (i) there are privacy risks resulting from the accumulation of personal data; (ii) that the data privacy risks in such accumulation and aggregation of data are not, even with the assistance of regulators, necessarily internalised by consumers; and (iii) that these privacy risks can result from and/or lead to market power. These considerations together with the recognition of privacy as a non-price competition parameter might reinforce the appeal of the quality-based arguments for competition authorities.

Lack of Economic Incentive to Reduce Privacy

[134] ibid, Art 5(2). More specifically, the accountability principle consists of an obligation (i) to adopt concrete and practical measures for the implementation of the core data privacy principles and to do so in a verifiable manner; (ii) to ensure that these measures are effective; and (iii) to assume liability when the relevant measures are not taken or are ineffective.
[135] Newman (n 65) 442. See also Newman (n 64).
[136] Esayas (n 60).

Another reason for scepticism toward the privacy-as-a-quality argument stems from the lack of an economic incentive for firms to reduce privacy. According to Manne and Sperry, proponents of the theory have failed to provide 'an economically sound case for why the feared privacy degradation would occur at all' and 'unfortunately' there is 'no obvious reason why monopolists would have an incentive to degrade privacy'.[137]

This scepticism could be looked at from two angles. The first line of argument is that more data collection entails no benefit for the entities and can even be costly for them. Manne and Sperry write as follows:

> A monopolistic firm would have an incentive to degrade quality if doing so would lower its costs …But in the case of privacy protections—where, for example, one "harm" might be the maintenance of personal information on a firm's servers for extended periods without deletion—it would seem that a firm might actually incur more cost in degrading (storing information for longer) than in maintaining (deleting cumbersome information from limited storage space) privacy.[138]

To begin with, the argument that more data collection is rather costly for the service providers overlooks the fact that the collection, storage and processing of data involves substantial fixed costs but low marginal costs, that is, it requires substantial upfront investment, but the cost of the collection of additional data is minimal.[139] This is without mentioning the dramatic decline in the cost of storage, which motivates the accumulation of data.[140] Greater storage capacity at a cheaper cost erodes the desire to discard data. In fact, the perception has grown in the opposite direction to the point that deleting data is now viewed as costly and increasingly equated with 'killing babies'.[141]

A more important question is whether degradation in privacy is in fact a worthwhile exercise for monopolies. Sometimes, this problem arises from mixing data privacy and information security. Given that data privacy also includes data security aspects, it

[137] Manne and Sperry (n 33) 6.
[138] ibid 4.
[139] The UK Competition and Markets Authority, 'The Commercial Use of Consumer Data: Report on CMA's Call for Information', (2015) 75.
[140] OECD (n 11) 145 (For example, the average cost per gigabyte of consumer hard disk drives (HDDs) dropped from USD 56 in 1998 to USD 0.05 in 2012, representing an average decline of 40 per cent a year).
[141] Dave Eggers explores a fictional Google-like company where this perception is held. See Dave Eggers, *The Circle* (Penguin Books, 2013) 204 (Kindle edition). This is confirmed by Google's Cloud Platform Director Tom Kershaw. Kershaw remarked that 'Never delete anything, always use data – it's what Google does'. See Quentin Hardy, 'Google Offers Cheap Storage for Certain Kinds of Data' *The New York Times* (11 March 2015).

might be difficult to generalise that all reductions in data privacy are profitable. This is partly because the potential cost of data breaches could make a decrease in quality unprofitable, thus constraining the firm from reducing the level of data security.[142] However, a reduction in privacy could be considered profitable if the reduction is understood in the form of collecting more data or increasing the usage of the data.

As noted by Mayer-Schönberger and Cukier, in the data-driven economy, the highest value lies in the repurposing, recombining and multi-purposing of personal databases.[143] More importantly, the underlying logic with big data practices, as Mayer-Schönberger and Cukier put it, is that 'the sum is more valuable than its parts, and *when we recombine the sums of multiple datasets together*, *that sum too is worth more than its individual ingredients*'.[144] More particularly, it has been indicated that 'more data about users enables' more targeted ads.[145] In the proposed Microsoft/Yahoo merger, both the EC and the US Department of Justice (DoJ) recognized the value of the data for advertisement. The EC noted that more targeted ads can lead to increased return of investment (ROI) for adversities, which translates to increased willingness to pay more for ads and ultimately more revenue for Microsoft.[146] Similarly, the DoJ noted the strong relationship between scale in search data and 'competitive performance' in search advertising, explaining how Microsoft's algorithms benefit from access to large sets of search queries from Yahoo and Bing.[147] According to the DoJ, the merged entity would have access to 'larger data pool' that 'may enable more effective testing and thus more rapid innovation of potential new search-related products, changes in the presentation of search results and paid search listings, other changes in the user interface, and changes in the search or paid search algorithms'.[148] Economist Joseph

[142] Even such an argument assumes that one is able to attribute the data breach to a specific entity, which is not always straightforward. See Joseph Farrell, 'Can Privacy Be Just Another Good?' (2012) 10 *J. on Telecomm. & High Tech. L.* 256.
[143] See Viktor Mayer-Schönberger and Kenneth Cukier, *Big data: A revolution that will transform how we live, work, and think* (Houghton Mifflin Harcourt 2013) 108.
[144] ibid 108
[145] See Waehrer (n 54) 3 (indicating that 'If a decrease in privacy results in better targeted advertisements or more data to sell, then a decrease in privacy would increase the revenue of an online service').
[146] *Microsoft/Yahoo! Search Business* (n 1).
[147] The US Department of Justice, 'Statement of the Department of Justice Antitrust Division on Its Decision to Close Its Investigation of the Internet Search and Paid Search Advertising Agreement between Microsoft Corporation and Yahoo! Inc.' (18 Feb 2010) .
[148] ibid.

Farrell likens more information collection or repurposing of data to a reduced marginal cost.[149]

Moreover, given that data privacy regulation suffers from scaling problems,[150] accumulation and aggregation become attractive because they diminish transparency and accountability for companies going forward. In other words, the practices of accumulating personal information from a wide array of sources and aggregation practices reduces the likelihood of a company being held accountable for data privacy breaches. This is because, as noted above, such practices distort the very foundation, at least in the EU context, upon which the transparency and accountability mechanisms are built. Even more, considering the business value that such aggregation practices add and the diminished transparency and accountability for companies going forward, paying fines for data aggregation practices could become a worthwhile investment.

The second argument relates to the question on how a 'less-privacy-protective structure' rewards the monopolist'.[151] As Manne and Sperry put it:

> Claims that concentration will lead to a "less-privacy-protective structure" for online activity are analytically empty. One must make out a case, at minimum, that a move to this sort of structure would reward the monopolist in some way, either by reducing its costs or by increasing revenue from some other source.[152]

This is based on the argument that less privacy is not a problem unless it benefits the monopolist. However, this argument has several limitations. To begin with, privacy degradation in the form of accumulation of consumer information could constitute an exploitative practice if 'producers take valuable consumer information without payment or without payment at a competitive price'.[153] To the extent that consumers demand privacy, the question for competition law is whether the market 'satisfies those tastes' and whether the failure to satisfy these needs can be linked to market power (failure).[154] This implies that it is not necessary for consumers to 'justify' why the

[149] Farrell (n 142) 255 (This means that if a firm earns 'Y' amount from repurposing the data collected in providing a good, it would be equivalent to a reduction by 'Y' amount in the marginal cost of producing that good).
[150] See Campbell, Goldfarb and Tucker (n 110) 83.
[151] Manne and Sperry (n 33).
[152] ibid 5.
[153] Mark Patterson, *Antitrust Law in the New Economy* (Harvard UP 2017) 167.
[154] ibid (citations omitted).

desired taste enhances their welfare, nor is it necessary that the monopolist profits from its conduct that harms consumer welfare.[155]

Even leaving that aside, the Facebook/WhatsApp merger could be illustrative in terms of how a 'less-privacy-protective structure' might be rewarding. Before the merger, WhatsApp was known for its restrictive data collection practices. As indicated by the Commission, contrary to Facebook, WhatsApp only stored limited information about its users (namely, user name, picture, status message, phone number and the phone numbers in the user's phone book) and did not offer targeted advertisement. By contrast, Facebook collects information about users, including, but not limited to, their real names, gender, birthdate, birth place, religion, political affiliations, 'likes' and social media contacts. Facebook also tracks users' browsing behaviour through millions of websites that have Facebook plugins. Furthermore, using the data, Facebook offers targeted advertisement and shares the information with third parties.

If one assumes that any change in WhatsApp's policy by the merged entity so that WhatsApp could collect more data and introduce advertisement would create a 'less-privacy-protective structure',[156] the question is how would that benefit the merged entity?

One argument is that the privacy protective feature together with the growing popularity of WhatsApp could be seen as imposing a competitive pressure on Facebook to compete on privacy. Commenting on a similar subject, former FTC Commissioner Harbour and her legal advisor, Koslov, argue as follows:

> Absent pressure from competitors [*such as WhatsApp*] who might provide more attractive alternatives to privacy-prioritizing consumers, a dominant firm [*such as Facebook*] might rationally choose to innovate less vigorously around privacy or, perhaps, to dole out privacy-protective technologies to the marketplace more slowly.[157]

In this sense, one could argue that WhatsApp imposes certain competitive constraints on Facebook to try to compete on privacy-enhancing technologies, which entail costs.

[155] ibid (referring to the often cited quote that 'the best of all monoploy profits is a quiet life').
[156] This is the position taken by the Commission in the *Facebook/WhatsApp* (n 14), para 147.
[157] Harbour and Koslov (n 15) 795 [addition mine].

However, if WhatsApp becomes like Facebook and begins to collect information and offer advertisements, it would reduce the competitive pressure and related costs to compete on privacy-enhancing technologies.[158]

Moreover, given that WhatsApp was trying to induce Facebook users to use its messaging App by offering more privacy and was succeeding, a 'less-privacy-protective structure' would benefit Facebook. As the Commission itself pointed out, most of WhatsApp users are also users of Facebook's social network. The Commission's assessment shows that in April 2014, 80–90 per cent of WhatsApp users were users of Facebook's social network and 'were therefore already within the reach of Facebook Messenger'.[159] The Commission further noted that although both messaging services offer similar functionalities, the user experience in Facebook Messenger is far richer than WhatsApp because of its integration with the core aspects of Facebook's social network.[160] Moreover, at the time of the merger, WhatsApp users in many countries were paying a subscription fee of USD 1, but they could use Facebook's Messenger for free.[161] This means that all other things being equal, one would expect Facebook Messenger to be more attractive for users than WhatsApp. However, as was indicated by the Commission, WhatsApp had more users (approximately 600 million users worldwide) than Facebook Messenger (approximately [250–350] million users).[162]

It is not contentious that one of the key competitive advantages of WhatsApp over Facebook Messenger is highly related to its restrictive data collection practice.[163] Arguably, it is the key feature that led to WhatsApp acquiring 600 million users in a shorter time than Facebook managed. In this sense, it is safe to say that to remain competitive with Facebook (to keep Facebook social network users using WhatsApp's messaging service), WhatsApp had to offer something that Facebook did not.

[158] See discussions in Samson Esayas, 'Competition in Dissimilarity: Lessons in Privacy from the Facebook/WhatsApp Merger', *CPI Antitrust Chronicle*, 1/2 (2017).
[159] *Facebook/WhatsApp* (n 14), para 105 and 70-80.
[160] ibid para 104.
[161] At the time, WhatsApp charged an annual subscription fee of around EUR 0.89 in Italy, the United Kingdom, Canada and the United States. See ibid para 90. The Commission also noted that 'WhatsApp was previously charging subscription fees also in Germany and Spain. However, WhatsApp cancelled subscription fees in these two Member States in the first half for 2014 for several reasons, among which…' See ibid para 91.
[162] ibid para 84.
[163] See Tal Zarsky, 'The privacy-innovation conundrum' (2015) 19 (1) Lewis & Clark Law Review 167 (noting that the privacy sentiment might have been the main reason for WhatsApp's popularity).

However, if WhatsApp had to start collecting personal data, its unique feature that attracted users away from Facebook's social network would disappear, and its customers might spend less time using its services and more time on other services, including Facebook Messenger.[164] As noted by Stucke and Grunes, 'Facebook sought users who spend more time on its texting app Messenger than WhatsApp. WhatsApp, to induce Facebook social network users to switch from messenger, offered greater privacy protections'.[165] Thus, WhatsApp's competitive concern would not only be that it would lose its users to messaging service with similar privacy policies, which might not happen because of the size of the networks, but also that it might lose its competitive edge over Facebook. And the more the market becomes less privacy protective, the more it would benefit Facebook. This is because in the absence of a privacy superior service, Facebook becomes a more attractive network due to its size and richer functionality. If this is valid, one logical explanation for WhatsApp's post-merger behaviour to degrade privacy[166]—by changing its privacy policy to the effect that data generated by WhatsApp will be shared with Facebook and other members of the Facebook family to improve service by, for example, allowing Facebook to display more relevant ads on WhatsApp users' Facebook accounts[167]—could well be because the merged entity can recapture some of the consumer loss to WhatsApp due to the privacy degradation through an increase in usage of Facebook Messenger.[168]

Interestingly, the Commission's decision in Facebook/WhatsApp partially reflects the claims put forth by Manne and Sperry that reducing privacy is not a rewarding behaviour. The Commission held that the merged entity lacks the incentive to change WhatsApp's privacy policy because, the change could 'prompt some users to switch to

[164] See Waehrer (n 54) 13 (arguing that if services compete in qulaity, such as privacy, 'the implication is that for any service an increase in its own quality level (all else equal) increases user demand for the service'). This partly explains why many Facebook social network users chose to use WhatsApp for messaging rather than Facebook Messenger.
[165] Stucke and Grunes (n 16) 132.
[166] See Autoritat Catalana de la Competència, 'The Data-Driven Economy: Challenges for Competition', (2016) 26 (claiming that the merger has 'decreased quality in terms of privacy' because 'where prior to the said merger two different models coexisted (WhatsApp – with greater data protection but with the requirement of an annual cash payment) and Facebook Messenger (less privacy protection but free) there is now just one (free service but with little privacy).'
[167] See WhatsApp Blog, 'Looking ahead for WhatsApp' (WhatsApp, 25 August 2016). See also WhatsApp privacy Policy <https://www.whatsapp.com/legal>.
[168] Waehrer (n 54) 14 (noting that services competing in quality can, post-merger, reduce the quality if 'a decrease in quality by service 1 results in the merged firm recapturing some of the customers lost to service 1 through an increase in usage of service 2').

different consumer communications apps that they [would] perceive as less intrusive.'[169] This implies that the Commission considered the potential change in privacy policy to collect data as an unprofitable strategy. However, this is a half-truth at best. Even if, against all odds of behavioural challenges (for example status quo bias and information asymmetry), the change in privacy policy to share the data for advertisement on Facebook leads to consumers deserting WhatsApp, it does not necessarily entail loss of revenue or is unprofitable.[170] This is because the revenue generated from the advertisement on Facebook might be superior to the loss of consumer resulting from the change of privacy policy. Forbes magazine estimated that the change in WhatsApp's privacy policy and its business model – introducing tools which would allow users to communicate with businesses via WhatsApp could 'yield revenues of around 5 billion US dollars for Facebook in 2020, contributing about 9-10% of the company's total revenues'.[171] To the extent this is valid, the change in privacy policy in order to share data with Facebook can be a profit maximizing strategy.[172] This may be the case even in the face of consumers deserting WhatsApp following the change.

The Alleged Trade-off between Privacy Degradation and Quality Improvement

Another source of scepticism stems from the idea that even if there is an economic incentive to degrade privacy, there are other benefits that offsets the degradation in quality. These arguments could be looked at from consumers' and advertisers' perspectives. On the consumer side, the argument is that more data about a consumer allows for a more personalised service according to one's preferences. For example, Cooper argues that any privacy degradation that results from collecting more data improves quality because the additional data collected can be used to enhance the quality of the service and to better tailor the service to its users' preferences.[173] This means, for example, that access to more data about consumers' preferences, previous searches and clicks allows search engines to provide more relevant, personalised

[169] *Facebook/WhatsApp* (n 14), para 174.
[170] Esayas (n 158) 7.
[171] Trefis Team, 'How Much Revenue Can Facebook's WhatsApp Generate in The Next Five Years?', (*Forbes,* 3 March 2016).
[172] Esayas (n 158) 7.
[173] See Cooper (n 32) 1135-6.

results and better respond to the consumers' queries. Similarly, the search engine could also tailor the advertisements according to the consumers' preferences and avoid showing irrelevant advertisements. However, it is not clear if personalised services and targeted ads constitute improvements in quality for consumers. Is it an improvement in quality if Google, having known all of a user's religious, political and sexual leanings, shows the user only ideas, links and ads that fit Google's understanding of the user? This might be true for some consumers but it should not be readily accepted that personalisation entails quality improvements for all consumers. This is because personalisation also eliminates the potential exposure to conflicting viewpoints that could challenge or broaden one's worldview,[174] which may prove to be bad for users and bad for democracy.[175] There is a burgeoning literature on the dangers of the 'filter bubble', which need not be reiterated here.[176]

Similarly, there is little evidence that consumers prefer targeted ads to non-targeted ads; in fact, this is far from the case. Many studies have shown that consumers dislike 'targeted ads' and would prefer a randomised advertisement.[177] For example, one study found that 66 per cent of adult Americans (18–24) do not want marketers to tailor advertisements to their interests.[178] This number grew to between 73–86 per cent when users were informed on how marketers gather data about them to tailor the ads.[179] Moreover, 86 per cent of those adults reject tailored advertisement if the data used to tailor the advertisement is obtained from other sources than the website they are visiting, and this rose to 90 per cent if the tailored advertisement is based on data from their offline behaviour.[180] There are also other studies showing that, increasingly, targeted advertisements are associated with 'creepiness', that is, the feeling that others are watching, tracking, assessing and capitalising at the cost of one's data privacy.[181]

[174] Allen Grunes, 'Another Look at Privacy' (2013) 20 (4) George Mason Law Review 1126.
[175] See Mostafa El-Bermawy, 'Your Filter Bubble is Destroying Democracy' WIRED (18 Nov 2016). See also Emma Barnett, 'Google and Facebook mean that we don't know what we're missing' *The Telegraph* (23 Feb 2012).
[176] See, for example, Eli Pariser, *The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think* (Penguin, 2011).
[177] See discussions in Catherine Tucker, 'Privacy and the Internet' in Simon Anderson, Joel Waldfogel and David Strömberg (eds), *Handbook of Media Economics Volume 1* (Elsevier 2015), 541-62.
[178] Joseph Turow et al., 'Americans reject tailored advertising and three activities that enable it' (2009) <https://ssrn.com/abstract=2820060> 1.
[179] ibid.
[180] ibid 3.
[181] See Lisa Barnard, *The Cost of Creepiness: How Online Behavioral Advertising Affects Consumer Purchase Intention* (ProQuest Dissertations & Theses A&I, 2014).

One could only expect this number to rise as consumers start to know more about how their data are collected and exploited.

From the advertisers' perspective, the argument is that 'more data about users' means better targeted ads, which in turn leads to more effectiveness.[182] There is some empirical evidence showing that targeted behavioural advertisements are 2.43 times as effective as non-targeted advertising.[183] This is followed by the argument that because the reductions in the privacy of consumers are compensated by benefits to advertisers, it is merely a transfer of resources from consumers to advertisers and thus is not a concern for competition law. For example, Manne and Sperry argue to this effect, as follows:

> A decrease in privacy protection is not simply a transfer from consumers to producers creating the famous deadweight loss of antitrust textbooks. Rather, the collection and use of larger amounts of information by a company like Google has the ability to improve … the successful targeting of its ads.[184]

Although scale in data is, indisputably, important in improving the quality of online services, the welfare effects on advertisers may be grossly overstated. According to one study, when adjusted for its price, targeted advertisement is not more effective. Several studies have shown that targeted advertisements could be three to five times more expensive than non-targeted advertisements.[185] And, if the effectiveness of advertising is measured in terms of the price paid to induce consumers to take some action, for example, purchase something, there are no 'benefits to the advertiser from the better-targeted advertisements as the advertiser continues to get the same level of effectiveness per dollar spent'.[186] In other words, when normalised for effectiveness, targeted and non-targeted ads are priced similarly.[187] In some instances, behaviourally targeted advertisements could even be less effective than non-targeted ads. For example, according to Lambrecht and Tucker, when a website targets a user based

[182] See Waehrer (n 54) 3 (indicating that 'If a decrease in privacy results in better targeted advertisements or more data to sell, then a decrease in privacy would increase the revenue of an online service').
[183] See references in ibid 11.
[184] Manne and Sperry (n 33) 5.
[185] See, for example, Waehrer (n 54) and references therein. See also Newman (n 65) 441.
[186] ibid 16. See also Anja Lambrecht and Catherine Tucker, 'When does retargeting work? Information specificity in online advertising' (2013) 50(5) Journal of Marketing Research 561-76.
[187] Waehrer (n 54)16.

on his or her browsing history in other websites, such ads were found to be on average less effective than non-targeted ads.[188] Other studies also associate behaviourally tailored ads to increased creepiness, and a subsequent reduction, by 5 per cent, in the effectiveness of the ads.[189] This implies that a decrease in privacy does not necessarily, at least not always, increase the welfare of advertisers.

Moreover, in some cases, accumulation of too much data about consumers could even harm the welfare of advertisers (and consumers).[190] For example, Newman demonstrates how Google's 'unmatched control of user data' gives rise to reduced competition in the advertising market, where advertisers are charged premium price.[191] Explaining why Google's control of user data gives rise to a premium price, Newman refers to a study showing that Google's cost per click (CPC) price for the same keywords is four to five times more expensive than the price charged by Bing and nearly twice Yahoo!'s rate.[192] Given that search advertising requires high fixed costs, Newman observes that the lower CPC for competitors was 'a key reason Yahoo! was forced out of the online search market'.[193] This reduced competition in the online advertising market harms consumers because 'the higher prices charged to advertisers inevitably gets passed onto consumers in the form of higher prices for the advertised goods and services they buy'.[194] Newman further identifies three consumer harms from Google's accumulation of data:

> (1) loss of private data at an artificially low price due to Google's monopoly position; (2) higher prices potentially charged by advertisers due to price discrimination facilitated by use of that data in targeted advertising; and (3) Google enabling use of that data for illegal and more generally exploitive uses by unethical businesses.[195]

[188] Lambrecht and Tucker (n 186) 561.
[189] See Barnard (n 181).
[190] Newman (n 65) 401. See also Stucke and Ezrachi (n 50).
[191] Newman (n 65) 411.
[192] ibid 418 ('all things being equal, the CPC price should be roughly the same since a user ultimately clicking through to an advertiser's pageshould in theory be just as valuable if the customer reaches the page via Google ... or via Bing').
[193] ibid 418 ('The lower CPC rate means that Google's potential competitors receive much less revenue but have to invest similar amounts in fixed costs to maintain a competitive search engine and platform').
[194] ibid 411.
[195] ibid 442. See also Newman (n 64). Although not all these harms may fit into traditional antitrust harm, Newman makes an interesting point.

Although Newman admits that Google's success has also come from its innovative algorithms, he considers consumer information to be 'the most important one in terms of entrenching the company's monopoly in search advertising'.[196] More particularly, Newman observes that Google's ability 'to charge a far higher price to advertisers for each "click" on an ad is due to Google's unmatched control of user data'.[197] According to Newman, 'Google built its dominant position in the search advertising market in part through a series of exclusive contracts that gave it access to an increasing amount of user data'.[198] At the same time, these exclusive contracts make it harder for customers to adopt rivals' technology and prevent rivals from accessing similar data from third-party websites—ultimately forcing competitors out of the market.[199] The EC statement of objection to Google in part confirms this position. The EC found that exclusive contracts 'have enabled Google to **protect its dominant position in online search advertising**. It has prevented existing and potential competitors, including other search providers and online advertising platforms, from entering and growing in this commercially important area'.[200]

In its Google Shopping decision, the European Commission imposed a fine of Euro 2.42 billion on Google for abusing its dominant position in searches 'by giving illegal advantage to own comparison shopping service'.[201] Noting that search users 'do not necessarily see the most relevant results in response to queries',[202] the Commission found Google to have abused its dominance in search by systemically 'promoting its own comparison shopping service in its search results and demoting those of competitors'.[203] According to the Commission, this practice has 'stifled competition on the merits in comparison shopping markets, depriving European consumers of genuine choice and innovation'.[204]

[196] Newman quotes Google's Chief Scientist Peter, claiming that 'We don't have better algorithms than everyone else; we just have more data'. See Newman (n 65) 421.
[197] ibid 404.
[198] ibid 423. See also Autorite de la Concurrence and Bundeskartellamt (n 24) 19.
[199] Autorite de la Concurrence and Bundeskartellamt (n 24) 19.
[200] European Commission - Press release, 'Antitrust: Commission takes further steps in investigations alleging Google's comparison shopping and advertising-related practices breach EU rules' (IP/16/2532, 14 July 2016) (emphasis in original).
[201] European Commission - Press release, 'Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service' (27 June 2017).
[202] European Commission - Press release, 'Antitrust: Commission sends Statement of Objections to Google on comparison shopping service' (MEMO/15/4781, Brussels, 15 April 2015).
[203] European Commission (n 201).
[204] ibid.

A very important question is if a search, as Google's former CEO observed, is characterised with low 'entry barriers because of the competition is a click away',[205] what are the factors that led Google to exercise market power by favouring its own comparison shopping product and thereby reduce search quality? There can be a cumulative of factors,[206] but the data-driven network effects play a significant role in such market power. For example, Stucke and Ezrachi identify scope in data (both search data and data about consumers) as one 'important variable' incentivising a search engine to intentionally degrade quality despite competition from rivals.[207] According to them, such scale and scope in data gives a 'larger search engine' such as Google the potential to 'degrade the quality of its search results by a small but significant amount, and still produce better search results than its smaller rivals'.[208] The widening gap in data scale, and consequently in the quality of the search, reduces the competitive constraints from smaller rivals, which in turn may lead to a degradation in the quality of the search by the dominant firm in a way that maximises its advertising revenue. This reduction in search quality harms both consumers and advertisers.[209] The Commission concurred this line of argument in its Google Shopping decision, pointing out that the search market exhibits 'high barriers to entry' partly because 'the data a search engine gathers about consumers can in turn be used to improve results'.[210]

Thus, although access to data can be used to improve qualities, there are also several ways such data could result in a loss of quality, including consumer privacy and reduced competition in the advertising market. This implies that the claim that privacy degradation through accumulation of data leads to quality improvements for users and/or advertisers does not always hold true. Moreover, the claim that privacy harms

[205] Eric Schmidt, 'Why Google Works' *Huffington Post* (20 Jan 2015) <http://www.huffingtonpost.com/eric-schmidt/why-google-works_b_6502132.html> accessed 10 July 2017.
[206] See for example Mark Patterson, 'Google and Search-Engine Market Power', *Harv. JL & Tech.*, 2013 (2013), 1. See also Patterson (n 153) dicussing, among others, the challenges with detecting degardation in search results.
[207] Stucke and Ezrachi (n 50) 92. Other relevant variables include the difficultly for consumers 'to accurately assess quality degradation' and 'the cost of conveying to consumers search engines'. See ibid 76-7.
[208] ibid 96.
[209] ibid 92. (noting that 'Under a "hold-up" scenario, the search engine could lower the ranking of potential advertisers appearing in the organic search to pressure the businesses to advertise with the search engine').
[210] European Commission - Press release, 'Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service', (IP/17/1784, 27 June 2017).

might lead to other quality improvements only implies that competition law needs to balance the harms and benefits but does little to dispel that privacy degradation can be a concern for competition law. Such an argument signifies the need to do the balancing on a case-by-case basis.

5. The Role of Data Privacy Law

If privacy could be considered a quality (non-price) parameter under competition law, what role, and even should, data privacy law play in understanding and determining degradation in privacy? This question is particularly important because the lack of a concrete benchmark for measuring degradation in privacy is a key source of scepticism against the quality-based arguments. As the argument goes, the absence of concrete benchmarks with which to determine degradation in privacy could lead to a nebulous application of competition law with unpredictable outcomes.[211] The counter argument, however, is that first, not all privacy degradations are difficult to measure. As the Commission's decision in Microsoft/LinkedIn demonstrates,[212] the classical anticompetitive conducts such as tying could lead to reduced competition in privacy as a competition parameter. In that decision, the Commission held that the possibility of integrating and promoting LinkedIn through Microsoft Windows and Office products was considered to reduce consumer choice in relation to privacy.[213] This is because such conduct may lead to marginalization and eventual foreclosure of professional social network providers such as XING that 'offer a greater degree of privacy protection than LinkedIn'.[214] This indicates that reductions in the level of privacy could result from classic anticompetitive conducts, eg. tying, so far as competition authorities are cognizant that privacy can be a form of quality (nonprice) competition.

Moreover, competition law is 'open to normative influence from other fields of law' and that data privacy can serve as a metric or benchmark for determining degradation in privacy.[215] It is not uncommon that competition authorities have sometimes resorted to different benchmarks to determine whether a certain conduct, for example, an excessive price, constitutes an abusive conduct. At least in one instance, the

[211] See citations in Costa-Cabral and Lynskey (n 13) 28-9.
[212] Microsoft/LinkedIn (n 6), para 350.
[213] ibid.
[214] ibid.
[215] Costa-Cabral and Lynskey (n 13) 31.

Commission used a standard set by an international standard-setting body as a benchmark to assess whether fees charged by financial institutions for using international securities identification numbers were excessive.[216] Given that competition law is bereft of its own standard for determining the fair ratio between the price and 'economic value' of the services,[217] the Commission sought guidance from an international standard. Similarly, there are few instances where competition authorities used another field of law as a benchmark to condemn a certain conduct under competition law.[218] In *Allianz Hungária Biztosító Zrt, v Gazdasági Versenyhivatal*, the CJEU resorted to domestic law in analysing the competitive impacts of a vertical restriction imposed by insurance companies on insurance brokers or intermediaries.[219] The domestic law prohibits intermediaries or brokers of insurance companies to be affiliated with the insurance companies and the Court found that such prohibition is relevant in assessing whether the vertical restrictions imposed by the insurance companies on the intermediaries would constitute a restriction by object under Article 101 of the TFEU. In this instance, competition law sought normative help from the national legislation, which regulates how a car insurance market should operate, in determining whether the agreement conformed with 'the proper functioning' of such a market.[220]

In a similar fashion, the German Federal Court indicated that contract terms by dominant undertakings, which are incompatible with the laws regulating general conditions and terms of trade, might constitute an abuse of dominant position under German competition law to the extent the terms can be linked to the company's dominance in the market.[221] Moreover, IP law has long been used as a normative yardstick in competition law, particularly in assessing whether the rewards of the legal monopoly, for example, licensing conditions, are concerns for competition law. To the extent the IP rights are acquired legally, competition law has often distanced itself from interfering with right holders' rewards and has played only a very limited role in cases

[216] Citing Commission decision Case COMP/39.592 - Standard & Poor's. See Richard Whish and David Bailey, *Competition Law* (Oxford UP 2015) 764.
[217] The excessiveness of a price is assessed having regard to the difference between the price and the 'economic value' of a good or service. See Case C27/76 *United Brands v Commission* [1978] ECR 207, para 250.
[218] See Costa-Cabral and Lynskey (n 13) 5.
[219] Case C-32/11 [2013] 4 CMLR 122-7, para 47.
[220] Case C-32/11, *Allianz Hungária*, para 47. See also Costa-Cabral and Lynskey (n 13) 32.
[221] See Autorite de la Concurrence and Bundeskartellamt (n 24) 25.

such as standard essential patents. However, there are cases where competition law has been used to limit rewards from IP rights, particularly when such rights are acquired illegally. For example, in *AstraZeneca,* the CJEU held that where IP rights are acquired unlawfully, the rewards are not based on 'merits' and thus considered abusive.[222] In this instance, whether the monopoly is acquired in compliance with the relevant IP rules provides normative guidance in assessing whether the rewards are legal under competition law.[223] All these examples illustrate that when competition law lacks the necessary metrics to assess a certain conduct, the regulating bodies seek guidance from norms outside competition law, including other fields of law.

Because data privacy law is the norm that specifies 'the desired level of data protection for consumers',[224] one can draw similar conclusions to claim that data privacy rules can serve as a benchmark for determining degradation in privacy (quality). This is particularly the case in the EU, where the EU rules are regarded 'the gold standard in data protection law' across the world.[225] Related to this, in the EU, both data privacy and competition law share common objectives, which necessitates for their coherent application where their objectives intersect.[226] In addition, as personal data becomes more and more of a key source of competitive advantage in providing many digital services,[227] data protection law takes a central stage in regulating the competitive process, meaning compliance or lack thereof with data protection rules could be a key competitive differentiator. Confirming this claim is a remark made by former European Commission Vice-President Vivian Reding stressing that the proposed General Data Protection Regulation (GDPR) 'is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world'.[228] To the extent that data protection law is about creating a competitive playing field, non-compliance with the rules is not just a matter of a breach of fundamental

[222] Case C-457/10 P *AstraZeneca v Commission* EU:C:2012 :770, para 47.
[223] Costa-Cabral and Lynskey (n 13) 36.
[224] ibid 32.
[225] European Data Protection Supervisor, 'Data Protection' <https://edps.europa.eu/data-protection_en>.
[226] For example, 'both promote market integration, seek to protect individuals, and tackle power asymmetries.' See Costa-Cabral and Lynskey (n 13) 21.
[227] See Monopolkomission, 'Competitition Policy: The Challenges of Digital Markets', (2015) *Special Report No 68*, para 108.
[228] European Commission Press Release, 'Speech by Viviane Reding: Making the EU Data Protection Reform irreversible' (11 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-208_en.htm>.

rights, but also could disrupt the competitive process.[229] This implies that at least in some instances, data protection rules could serve as a metric to determine what constitutes 'fair competition',[230] 'normal competition'[231] and 'competition on merits'.[232]

As an example, if the accumulation of data is considered to cause privacy degradation, one line of argument is that excessive data collection by dominant undertakings could be challenged directly as exploitative conduct that is comparable to excessive pricing or excessive trading conditions.[233] However, given the difficulty of determining excessive data collection, as is often the case with excessive prices, competition law can seek guidance from data privacy rules. Highlighting this point, a joint report by the German and French Competition authorities indicates the following:

> [L]ooking at excessive trading conditions, especially terms and conditions which are imposed on consumers in order to use a service or product, data privacy regulations might be a useful benchmark to assess an exploitative conduct.[234]

In this regard, the data minimisation principle together with purpose specification principle under data privacy law could provide normative guidance in assessing excessive data collection. The former requires that personal data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'.[235] The latter underlines the need for a specific and explicit purpose for the collection of personal data, one that must be determined prior to, or at the latest during, the collection of data.[236] Together, these principles can provide guidance in assessing if the data collected were beyond the minimum necessary for

[229] See Autorite de la Concurrence and Bundeskartellamt (n 24) 23 (noting that, 'Decisions taken by an undertaking regarding the collection and use of personal data can have, in parallel, implications on economic and competition dimensions').
[230] At least in one instance, a Belgian court found that the use of data acquired in providing banking operations to offer customers insurance and mortgage services was considered 'unfair competitive practice' because such a practice breaches the 'finality principle' under the Belgian data protection law, which restricts the use of personal data for purposes other than what they were originally collected for. See Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford UP 2014) 15-16.
[231] See Costa-Cabral and Lynskey (n 13) 33 (arguing that where personal data are used for competitive purposes, breaches of data protection law can fall outside 'normal competition').
[232] See discussions in Autorite de la Concurrence and Bundeskartellamt (n 24) 24-6. See also Costa-Cabral and Lynskey (n 13) 35 (noting that, 'Dominant undertakings are also under a special responsibility to only resort to "competition on the merits" and a data protection infringement represents a departure from such competition on the merits').
[233] See Autorite de la Concurrence and Bundeskartellamt (n 24) 24-6. Costa-Cabral and Lynskey (n 13) 35. See also Aleksandra Gebicka and Andreas Heinemann, 'Social media & competition law' (2014) 37(2) *World Competition* 163-5. Kerber (n 16) 861. See Monopolkomission (n 227) paras 326-9.
[234] Autorite de la Concurrence and Bundeskartellamt (n 24) 25.
[235] GDPR (n 79) Art 5(1(c)).
[236] GDPR (n 79) Art 5(1(b)).

achieving the purpose (that is, excessive). Prosecuting dominant players for excessive data collection can address some of the abovementioned externalities of accumulation of data by firms to other consumers (that is, increased cost of protecting privacy) and the society at larger (loss of practical obscurity). Similarly, if the lack of transparency about data collection and unilateral changes to the conditions of processing without providing a meaningful option for users could be considered abusive behaviour as some have argued,[237] the transparency principle under data privacy rules could provide some guidance in terms of what relevant information is missing.[238] Overall, because dominant undertakings have a special responsibility to resort only to 'competition on merits', certain data protection practices by such undertakings that breach data law could be considered an abuse of dominant positions.

In this context, the German Competition Law Authority (Bundeskartellamt) has looked into the possible abuse of dominant position by Facebook in the market for social networks by imposing unfair terms and conditions on users.[239] Questioning the admissibility of the terms and conditions in light of 'applicable national data protection law', the authority underlined that '[i]f there is a connection between such an infringement and market dominance, this could also constitute an abusive practice under competition law'.[240] In its preliminary assessment, the Bundeskartellamt found Facebook's data collection practices from third party sources as unfair in light of 'European data protection principles' and constitute an abuse of dominance under the German competition law.[241] According to the authority, Facebook's terms and conditions 'are neither justified under data protection principles nor are they appropriate under competition law standards.'[242] The investigation appears to resemble the abovementioned decision from the German Federal Court, where the incompatibility of the contract terms with the laws regulating general conditions and

[237] See Kerber (n 16) 861. See also Gebicka and Heinemann (n 233)162.
[238] Furthermore, Articles 13 and 14 of the GDPR require firms processing personal data to provide information regarding the purpose of the processing, the categories of information and other relevant information about the controller and potential recipients of the data.
[239] See the Bundeskartellamt Press Release, 'Bundeskartellamt Initiates Proceeding against Facebook on Suspicion of Having Abused Its Market Power by Infringing Data Protection' <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html>.
[240] ibid. See also Andreas Mundt, 'Digitalization Revolutionizes the Economy - And the Work of Competition Authorities' (2017) CPI Antitrust Chronicle 3.
[241] Bundeskartellamt, 'Background Information on the Facebook Proceeding' (19 December 2017) 5.
[242] ibid 2.

terms of trade are regarded as an abuse of dominance under the German competition law.

Two points from the investigation require particular mention. First, this is perhaps the first case where harms to data privacy (to competition on privacy) are at the centre of a competition law investigation. Some of the consumer harms identified by the Bundeskartellamt include users' loss of control on how 'their personal data are used', lack of choice to avoid merging of their data and 'a violation of users constitutionally protected right to informational self-determination'.[243] Secondly, the investigation resorts to data privacy law as a metric for assessing abuse.

Developments such as the Facebook investigation would help firms internalize the costs related to lack of transparency in data use for competition through privacy. More concretely, considering 'lack of transparency' on data collection and use as an abusive practice could help firms to internalize the externalities that lead to what economist Farrell describes as the 'dysfunctional equilibrium', particularly the tendencies from new comers to learn that they are not able to attract sufficient demand by providing clear and privacy friendly policies.[244] The lack of transparency by dominant players means that users are unable to comprehend and make informed decisions, which leads to the problem of resignation and consumer cynicism (that is, consumers learn that reading privacy policies is not a rewarding activity).[245] In turn, this affects the supply of services with clearer and protective policies because users do not reward such behaviour and firms' demand would not shift significantly, and thus the firm can only sacrifice revenue from monetizing data.[246]

Some data-processing practices could also constitute exclusionary abuses. For example, the Belgian National Lottery was found to have abused its dominant position by repurposing personal data collected in the context of its legal monopoly in the lottery

[243] ibid 4.
[244] Dysfunctional equilibrium occurs when users develop credibility issues and fail to read privacy policies and even when they read they expect firms will act differently than what they promise to do. This discourages a new firm from using privacy to attract users because there is no reward in doing so, and instead the firm opts for noncommittal and/or non-protective policy. See Farrell (n 142) 251-9.
[245] ibid 257.
[246] ibid 259.

market to advertise a newly launched betting product.[247] The Competition Authority found that personal details were not acquired 'following competition on the merits'.[248] Similarly, the French Competition Law Authority found that the cross-usage of data collected in one market as an input in another market resulted in a restriction of competition.[249] The agency held that cross-usage is not 'competition on merits' because the database was not a 'product of a specific innovation' but rather inherited from its past monopoly.[250] In both cases, the exclusionary effect of the data-related conducts was not evaluated regarding a breach of data protection but rather in light of the fact that the data were acquired in the context of the legal monopoly of the firms. However, one could also argue that digital monopolies' cross-usage of personal data collected in one market in another market that is in clear breach of the purpose limitation principle under data protection law might constitute abusive conduct.[251] Concomitantly, acquiring a dominant position through breaches of data protection law could be condemned under Article 102 of TFEU as an abusive exclusionary practice, provided there is a strong link between the data collection and the undertaking's market position.[252] This is because data protection law infringements represent deviations from 'competition by merits'.[253]

The possible intersection between data protection and competition law raises equally important institutional questions, such as what role should Data Protection Authorities (DPAs) play in such assessments. To the extent privacy can be considered a quality parameter of competition, it would necessitate a closer institutional collaboration between data protection and competition authorities. A report issued by the Catalan Competition Authority calls for a greater cooperation between competition and data protection authorities 'insofar as it will become increasingly necessary for competition authorities to assess aspects of the quality and the level of privacy offered by

[247] See EDPS, 'Opinion 8/2016: EDPS Opinion on coherent enforcement of fundamental rights in the age of big data ' (European Data Protection Supervisor (EDPS) 2016) 9.
[248] ibid.
[249] Autorite de la Concurrence and Bundeskartellamt (n 24) 31.
[250] Costa-Cabral and Lynskey (n 13) 35.
[251] See discussions in (n 230) where a Belgian court held that the reuse of data collected in providing banking services to offer mortgage and insurance services breaches the finality (purpose limitation) principle under the Belgian data protection law and thus violates principles of 'fair' competition.
[252] See Costa-Cabral and Lynskey (n 13) 36 (reaching at this conlusion by drawing parallels from the AstraZeneca decision). See also Autorite de la Concurrence and Bundeskartellamt (n 24) 25.
[253] See Costa-Cabral and Lynskey (n 13) 36. See also Autorite de la Concurrence and Bundeskartellamt (n 24) 25.

operators'.[254] The recent proposal from the European Data Protection Supervisor (EPDS) to establish a digital clearing house that facilitates such cooperation among data protection, consumer protection and competition law authorities is a welcome opportunity.[255] The Bundeskartellamt's Facebook investigation presents a good opportunity to experiment on such collaborations, and the Bundeskartellamt should be commended for involving different regulatory authorities in the proceeding. The proceeding reportedly brings together data protection authorities, consumer protection authorities, the European Commission and competition authorities from other EU member states.[256] Regardless of the outcome of the investigation, this is a step in the right direction in the effective enforcement of competition and data protection rules.

6. Conclusion

The growing value of personal data for commercial purposes and as a key source of competitive advantage is ushering in a new challenge in the intersection of data privacy and competition. One emerging approach that is gaining some traction is to factor in privacy as a quality (non-price) competition parameter. The idea behind this approach is that privacy constitutes a quality component of many of the digital services offered to consumers for 'free', and extracting 'too much' information could represent a reduction in the quality of the product or service offered. Despite some emerging consensus on the subject, there remains a significant amount of scepticism on the lack of a link between the accumulation of data and privacy harms, the lack of an incentive to reduce privacy and the trade-off between privacy degradation and quality improvement.

This chapter offered some reflections challenging these scepticisms and established a link among accumulation of data, privacy degradation and to certain extent market power. It is true that not all these privacy issues identified here are competition matters and may be better dealt with under data privacy law. At the same time, in some cases, the effective enforcement of the privacy rights of individuals while maintaining a healthy

[254] Autoritat Catalana de la Competència (n 166) 42.
[255] EDPS (n 247).
[256] Robert McLeod, 'Novel But a Long Time Coming: The Bundeskartellamt Takes on Facebook' (2016) 7(6) Journal of European Competition Law & Practice 367-8.

competitive environment requires moving beyond the ‘either-or’ mentality toward a holistic approach from different regulatory perspectives. Thus, to the extent that the privacy degradations can be linked to market power and not outweighed by other welfare gains, competition law can complement data privacy law by factoring in the privacy-as-a-quality (non-price) competition parameter.

Taking privacy as a quality (non-price) competition parameter dispels the potential criticism that competition law is used to remedy normative harms. However, given that competition law lacks a concrete benchmark for measuring degradation in privacy, at least in the EU context, data privacy law could provide normative guidance in such an assessment. This is consistent with the precedents from the Commission, the CJEU and national courts, where other legal norms (for example IP) play a similar role in the application of competition law. Going forward, this would entail the need for a closer cooperation between data protection and competition law authorities.