Competition in (Data) Privacy: 'Zero' Price Markets, Market Power and the Role of Competition Law

Samson Esayas*

[Pre-print of article published in *International Data Privacy Law* 8(3)(2018) pp. 181-199]

Abstract

Firms compete by offering consumers lower prices but also high-quality products, and a wide range of choices. With the increasing commercialization of personal data, there is a growing consensus that the level of privacy protection and deployment of Privacy Enhancing Technologies (PETs) could be subject to competition, as an element of quality, choice or innovation. A case in point is the recognition by the European Commission that data privacy constitutes a key parameter of non-price (quality) competition in markets for consumer communications and professional social networks. This development signifies that market power may be exerted by reducing the level of data privacy and foreclosing competition on PETs deployment. Despite this, how market power affects competition on privacy and PETs remains unclear. This is partially because microeconomic theory offers little help in predicting how market power or lack thereof affects quality (including choice and innovation).

The aim of this article is to examine how market power in the underlying services that generate data impacts competition in data privacy and whether the proxies for assessing market power in these underlying services cater to data privacy interests. To this end, first, the article begins by highlighting some emerging but inconclusive literature shedding some light on the link between market structure and competition in data privacy. Secondly, the article identifies and discusses the structural and behavioural considerations that might hinder effective competition through data privacy and PETs. Finally, it examines the role that competition law can play in promoting and maintaining such competition.

Key words: Competition in privacy; Competition in PETs; Data protection and competition law; Market power in zero price markets; Privacy and market power; Privacy and market structure.

* Doctoral Research Fellow at the Norwegian Research Center for Computers and Law (NRCCL), Department of Private Law, University of Oslo. E-mail: s.y.esayas@jus.uio.no. 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 Bygrave and Inger Ørstavik for their comments on earlier drafts. Part of this article was written while on a research visit at Queensland University of Technology, Faculty of Law, Australia and I am thankful for the wonderful working environment and the hospitality I received there. Special thanks goes to Angela Daly for the warm welcome in Brisbane and her support throughout my stay. However, the usual disclaimer applies.

I. The Role of Market Power in Competition Law

Market power – defined as the ability of a firm 'to profitably increase prices, reduce output, choice or quality of goods and services, diminish innovation'[1] – is a central guiding concept in the application of EU competition law. This is because most competition law violations depend on whether a firm or a group of firms possess market power. Unilateral conduct that contravenes Article 102 TFEU[2] are dependent on the existence of dominance, which is equivalent to 'substantial market power'.[3] Although less prominent, market power is important for TFEU Article 101. This is because the *de minimis doctrine* exempts some anticompetitive agreements, decisions or concerted practices owing to lack of market power.[4] Moreover, the rules on mergers are primarily aimed at controlling the accumulation of market power into a single or handful of firms.[5] Thus, arguably proof of market power, albeit of different degrees, is a prerequisite for competition law intervention.

Despite its importance, determining the ability of a firm to profitably increase price or reduce quality is not an easy exercise. In price theory, one resorts to the competitive price, understood to be close to the marginal cost of the product/service (incremental cost of producing one additional unit).[6] Thus, charging prices above the marginal costs gives a sign of market power.[7] The Lerner Index, a tool used for measuring market power, relies on price and marginal cost. However, marginal cost is a hypothetical construct and difficult to gauge, which makes computing market power based on price-marginal cost margins a formidable task.[8] Similarly, this approach is unworkable where the price is 'zero'.[9] Thus, often competition authorities have to resort to proxies that capture this ability to increase prices, reduce output, choice or quality.

Key factors signalling this ability include the existence or lack thereof of 'competitive constraints', which is assessed having regard to the constraints imposed by actual and potential competitors in the market but also the bargaining power of customers, commonly known as

[1] Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings OJ C 31/5 [2004], para 8.
[2] Consolidated Version of the Treaty on the Functioning of the European Union OJ C 326/47 [2012].
[3] Richard Whish and David Bailey, *Competition Law* (OUP, 2015) 26. Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/7 (Article 102 Guidance), para 10.
[4] Commission Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice) [2014] OJ C 291/01.
[5] COUNCIL REGULATION (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings OJ L24/1, Article 3. See Whish and Bailey (n 3) 876-877.
[6] William Landes and Richard Posner, 'Market Power in Antitrust Cases', *Harvard Law Review*, 94 (1981) 937.
[7] David Evans, 'Antitrust Economics of Free', *Competition Policy International*, Spring (2011) 17 available at SSRN: https://ssrn.com/abstract=1813193.
[8] Landes and Posner (n 6) 941.
[9] Herbert Hovenkamp, 'Antitrust and Information Technologies', *Florida Law Review*, 68/2 (2016) 425.

'countervailing buyer power'.[10] Market share, the most commonly used proxy to compute market power, captures the competitive constraints imposed by existing competitors. Under EU competition law, market share is a useful indicator of market power as it shows the relative economic position of undertakings active in the market and their ability to respond to a potential increase in price or reduction in quality.[11] Various metrics are used to compute market share but the most common method is based on turnover or volume of sales. Potential competition accounts for the existence of barriers to entry or expansion including legal barriers, control of essential supplies, economies of scope and scale.[12]

'Zero' price markets present challenges to current approaches for assessing market power – both in light of how to calculate market power and how market power can be exerted. This is particularly the case where the data privacy of individuals is at stake, as is the case with the most popular digital services. At the heart of the business models for companies such as Google or Facebook is a detailed collection and analysis of data about consumers—where they are, what devices they use, what they purchase, and different categories of their online behaviours and interests. Among others, such data allows the companies to create detailed profiles of consumers and to deliver online advertising in a precise fashion. In return, consumers are getting targeted ads and a broad array of 'free' content, products, and services. However, in many digital services 'free' does not equate to 'costs nothing'.[13] This is because the data collected from the services is monetised through advertisement, which in turn finances these 'free' services. Moreover, such collection and use of data is associated with data privacy concerns. Thus, 'zero' price can be a profit maximizing strategy and firms may exercise market power in such markets, e.g., by reducing the level of privacy.[14]

Despite initial scepticism,[15] there is a growing consensus that the level of privacy protection and deployment of PETs could be subject to competition as a parameter of quality, choice or innovation, particularly when services are provided for 'free' and in exchange for personal

[10] Article 102 Guidance (n 3) para 12. Countervailing buyer power is less important for the discussions on 'zero' price markets.
[11] Ibid para 13.
[12] Ibid para 17.
[13] John Newman, 'Antitrust in Zero-Price Markets: Foundations', *University of Pennsylvania Law Review*, 164 (2015) 173.
[14] Evans (n 7) 14. Ania Thiemann and Pedro Gonzaga, 'Big Data: Bringing Competition Policy to the Digital Era', (OECD, 2016) 17.
[15] *Kinderstart. Com. Llc v. Google, Inc* [2007] (Dist. Court, ND California), para 5 (questioning the applicability of antitrust to 'free' services). Case M 4731 *Google/DoubleClick* decision of 11 March 2008.

data.[16] More particularly, in the Facebook/WhatsApp merger, the European Commission (EC) indicated that in markets for consumer communications, data privacy and data security constitute key parameters of non-price competition.[17] The EC further affirmed this stance in Microsoft/LinkedIn, claiming that data privacy is '*a significant factor of quality*' in the market for professional social networks (PSNs) and could be negatively affected by the merger.[18]

This development brings competition policy closer to the digital reality by acknowledging that market power may be exerted by reducing the level of data privacy and foreclosing competition on PETs.[19] However, how market power affects data collection practices of firms, particularly their incentives to compete on privacy and PETs, remains unclear. This is partially because microeconomic theory offers little help in predicting how market power or lack thereof (intensity of competition) affects quality (also choice and innovation) including the level of privacy. Moreover, in 'zero' price markets, the evidence available to gauge the existence of market power may be 'less plentiful and less clear.'[20] Given such lack of clear evidence, analysis of market structure could inform how market power ought to be computed in such markets and to better understand the role of competition law in maintaining competition in data privacy and PETs. Section II highlights this link between market structure and the level of competition in data privacy.

Another challenge is that despite the recognition that market power can be exercised through non-price parameters including the level of data privacy, the proxies used to assess market power remain largely price-centric or fail to cater to data privacy interests. For example, entry barriers, such as control over essential resources, are important proxies for market power because they prevent competitors from responding to price increases or quality reduction in timely manner. One may well then ask: where market power may be exerted by reducing the level of privacy, what factors may hinder competitors from responding to such a reduction and whether such factors are given due regard in market power assessments? Section III addresses this question by discussing the structural and behavioural considerations that might hinder effective competition through data privacy and PETs.

---

[16] However, this does not necessarily mean that privacy is irrelevant for paid services. This is consistent with the Commission's finding that loss of 'confidentiality' could be considered product degradation for paid services. See Case M 4854 *TomTom/Telia Atlas* decision of 14 May 2008, para 272-275.

[17] Case M 7217 *Facebook/WhatsApp* decsion of 3 Oct 2014, para 87.

[18] European Commission, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions', (6 December 2016).

[19] For a related discussion see Samson Esayas, 'Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism', *Paper Presented at 12th ASCOLA Conference https://ssrn.com/abstract=3075239*, (2017).

[20] John Newman, 'Antitrust in Zero-Price Markets: Applications', *Wash. UL Rev.*, 94 (2016) 73. Thiemann and Gonzaga (n 14) 17.

Similarly, the focus on turnover to compute market power is partly justified because if a firm charges prices above the competitive level, its turnover would reflect such ability. In other words, a strong link exists between the proxies used to compute market power and how this power is exerted. This raises the following question: where privacy is an important parameter of competition, whether the proxies used to assess market power (share) are able to capture the privacy considerations behind the collection and use of personal data. What alternative proxies can better capture these interests? Section IV demonstrates that some proxies can better capture data privacy concerns than others and highlights some of the constraints relevant for competition in data privacy and PETs.

II. Market Structure and Data Privacy

The Commission decisions in Facebook/WhatsApp and Microsoft/LinkedIn recognise that the level of data privacy can be an element of competition. Similarly, many academics have noted that firms engage in 'competition on privacy'[21] or 'competition on data protection'.[22] However, it is also true that, in most 'zero' price markets, e.g., search and social networks, privacy as a competition parameter often plays second fiddle to the competition in the quality of the underlying services.[23] Search engines compete based on the relevance and speed of the search results; and social networks by offering users richer functionality and a bigger network.[24] The question then is, if privacy is considered as a non-price (quality) parameter, how does the intensity of competition in the underlying services affect the level of privacy?

Unlike price, microeconomic theory does not offer a clear relationship between the intensity of competition and its impact on quality (including choice and innovation).[25] Reviewing many studies, the OECD roundtable indicates that the increased level of competition could have positive and negative effect on quality.[26] This is particularly the case if a firm's decision on price is unconstrained.[27] Accordingly, no general conclusions can be drawn on the effects of competition in the level of data privacy and understanding this would require empirical studies tailored to individual markets. However, exceptions apply. There is some measure of consensus

[21] Pamela Harbour and Tara Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets', 76(3) *Antitrust Law Journal* (2010). Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (OUP, 2016).
[22] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law', *Common Market Law Review*, 54 (2017).
[23] Ibid 27.
[24] *Facebook/WhatsApp* (n 17) para 102.
[25] OECD, 'Policy Roundtables: The Role and Measurement of Quality in Competition Analysis' (2013) 31.
[26] Ibid 20-40.
[27] Ibid 41.

that if firms' price making decisions are constrained, as in regulated markets, an increase in the intensity of competition can yield better quality.[28] If price constraints affect quality competition, one can ask whether 'zero' price markets exhibit such constraints. Specifically, are there forces that constrain firms' ability to adopt positive or negative prices?

The question is important because if 'zero' price markets are considered to exhibit such constraints, some of the research on regulated markets in relation to competition and quality could be relevant. In this regard, one argument is that the ubiquity of 'zero' price markets is not entirely coincidental as firms' pricing decisions in these markets might be constrained by several factors.[29] On the one hand, transaction costs may constrain the ability of companies to set positive prices. Particularly, costs from setting up and executing payment might be high enough that 'the unconstrained profit maximizing price would be close enough to zero'.[30] Concomitantly, companies might be deterred from setting negative prices, paying consumers for using their services, because this might 'create perverse incentives on the consumer side.'[31] Taking an ad-supported newspaper as an example, if the publisher offers payment for users to read the papers, many users might take the papers just to get the payment without necessarily increasing the exposure of the advertisement to additional users.[32] An additional problem with negative prices is that consumers might exploit such service under multiple identities.[33]

Thus, arguably, where these factors (transaction costs and perverse incentives) exist, the price making decisions of firms is constrained, resembling regulated markets, making the predictions also relevant to 'zero' price markets. If this is valid, one could then argue that where prizes are 'zero', a competitive market —understood as a market where a single or group of companies do not possess market power —can be generally considered to lead to better quality products/services including the level of data privacy.[34]

Although inconclusive, there is emerging empirical evidence that lends support to this claim. In a working paper assessing the relationship between market power and data privacy of around two million apps in the Google Play App store, a positive correlation was found between

[28] Lawrence White, 'Quality Variation when Prices are Regulated', 3(2) *The Bell Journal of Economics and Management Science*, (1972). See OECD (n 25) 31.
[29] Keith Waehrer, 'Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions' (2015) https://ssrn.com/abstract=2701927 11-12.
[30] Ibid 12.
[31] Ibid.
[32] Ibid.
[33] Benjamin Edelman, 'Priced and Unpriced Online Markets', *Journal of Economic Perspectives* 23 (2009) 21-22 (noting that overconsumption and horading can occur 'when resources are provided without charge.')
[34] See Waehrer (n 29) 12.

the market shares of an app in a specific market with more data collection.[35] Having computed the market share of each app, a combination of quantitative and qualitative parameters was used to assess the privacy practices of the apps. The quantitative parameter looks at the number of permissions, out of the 140 permissions available, that the app requests when downloaded.[36] The qualitative parameter looks at the number of permissions that are considered privacy sensitive. Based on another study, 12 permissions were identified as privacy-sensitive including permissions to read: 'phone state and ID', 'fine gps location', 'sms or mms', 'contact data', 'browser data' and 'sensitive log data'.[37]

The lack of a benchmark for the optimal level of data collection (permissions) in a specific market was one of the challenges, which the authors countered by using the mean number of privacy-sensitive permissions. Accordingly, apps that have higher market share were found to require more privacy-sensitive permissions than the average in that specific market.[38] In another study covering 300,000 Android apps over a period of four years (2012-2016), the same authors find positive correlation between the market share of the apps and the number of data access permissions by the apps.[39] According to them, 'market share is strongly correlated with using intrusive permissions… [and] … acquiring more data.'[40] Moreover, the authors find that apps with higher market shares are 'more likely to share their data with (many) outside parties.'[41]

Other studies have shown similar results. Reviewing the data collection practices of 140 websites, Preibusch and Bonneau found a positive correlation between the number of players in a market and the competition through data privacy.[42] According to them, where there are many competitors in a market, consumers 'have [a] fair chance of finding a provider whose privacy regime matches their preferences.'[43] More importantly, the survey found that websites facing little competition (having no major competitor) tend to collect significantly more data

[35] Reinhold Kesler, Michael Kummer, and Patrick Schulte, 'User Data, Market Power and Innovation in Online Markets: Evidence from the Mobile App Industry' (2017) Working Paper (link). Although most of the apps studied were free, the studies also cover apps that charge small fees. Data from other sources show that 92 percent of the apps in Google Play were free (2016).
[36] Ibid 13.
[37] Ibid.
[38] Ibid 18. The authors use data from Google's Play on 'similar apps' to define 'app secific' markets and sub-markets. Ibid 12-13.
[39] Reinhold Kesler, Michael Kummer, and Patrick Schulte, 'Mobile Applications and Access to Private Data: The Supply Side of the Android Ecosystem', *Centre for European Economic Research Discussion Paper No. 17-075*, (2018) 26.
[40] Ibid.
[41] Ibid 25.
[42] Sören Preibusch and Joseph Bonneau, 'The Privacy Landscape: Product Differentiation on Data Collection', in Bruce Schneier (ed.), *Economics of Information Security and Privacy III* (Springer, 2013) 280.
[43] Ibid.

than those facing more competition (that have more competitors).[44] All the websites with no major competitors are provided at 'zero' price.[45]

Although these studies need to be taken with caution,[46] they highlight an important and timely issue as competition authorities start to grapple with privacy. Additionally, this seems to be the stance echoed by many regulatory agencies and commentators, albeit for reasons not directly related to the abovementioned constraints.[47] For example, remarking on the effectiveness of consent, the EDPS indicated that '[w]here there is a limited number of operators or when one operator is dominant, the concept of consent becomes more and more illusory'.[48] This implies that consumers' privacy choices are limited in less competitive markets dominated by few players. This stance is shared by Commissioner Vestager who was quoted saying that 'when you have markets that are competitive, every little thing that makes your service more appealing to consumers can help you to compete. And that includes better protection for personal data.'[49]

Moreover, in its Microsoft/LinkedIn decision, the Commission followed similar reasoning.[50] According to the Commission, the pre-installation and integration of LinkedIn with Windows Operating System and Office products could lead to the foreclosure of competing PSNs. This in turn would harm consumers because it would lead to 'a substantial reduction of consumer choice, as LinkedIn's platform would remain the only PSN service provider available to users in the EEA.'[51] More importantly, the Commission indicated that the conduct would reduce consumer choice in relation to privacy. This is because such conduct would reduce the number of PSN providers including players offering 'a greater degree of privacy protection than

[44] Ibid.
[45] Ibid 279.
[46] Some scholars have disputed the link between concentration and privacy, even arguing that concentrated markets with bigger firms can be better for privacy as bigger firms are likely to provide users with more privacy control tools than smaller firms. See Darren Tucker, 'The Proper Role of Privacy in Merger Review', *CPI Antitrust Chronicle*, 2 (2015) 5. However, there are questions on whether such control mechanisms would actually enhances users' data privacy. For example, three consumer surveys find that creating some sense of control increases the amount of sensitive data that consumers reveal to companies. Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox', *Social Psychological and Personality Science*, 4/3 (2013). Fred Stutzman, Ralph Gross, and Alessandro Acquisti, 'Silent Listeners: The Evolution of Privacy and Disclosure on Facebook', *Journal of Privacy and Confidentiality*, 4/2 (2013) 22-24.
[47] See Daniel O'Brien and Doug Smith, 'Privacy in Online Markets: A Welfare Analysis of Demand Rotations', *FTC Working Paper No.323*, (2014) 37. Stucke and Grunes (n 21) 66. Harbour and Koslov (n 21) 794-797.
[48] EDPS Preliminary Opinion, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy', (2014) 35.
[49] European Commission, 'Making Data Work for Us: Speech by Commissioner Vestager' (9 September 2016).
[50] Case M 8124 *Microsoft /LinkedIn* decision of 6 Dec 2016.
[51] Ibid para 349.

LinkedIn'.[52] The logic behind the decision seems that consumers' privacy needs are better served in a market where there are several players than a market dominated by a single player.

The positive correlation between more competition and better privacy might seem at odds with the competition in other parameters, particularly functionality as such competition can be manifested by introducing features that solicit more data from users.[53] For example, Facebook's addition of features that allow users to express their feelings (happy, loved) enriches users' experience on the platform but also is a source of sensitive personal data with significant privacy implications.[54] Similarly, the integration of third party apps (e.g. games) into Facebook enhances functionality but has privacy implications because users' data are shared with app developers and usage of the app generates further information for Facebook and the apps.[55] Thus, an argument could be made that competition primarily driven by functionality might have negative implications for data privacy.[56]

However, not all competition on functionality entails reduced data privacy. For example, a study among 45 social networks shows that 'functionality is not related with more data collection.'[57] Moreover, in a well-functioning and competitive market, firms would offer different alternatives that cater to varying privacy preferences of individuals.[58] If some players are non-transparent about their data collection and usage, other firms would offer consumers with a clearer and better privacy policies. Similarly, if consumers feel that they are being asked for too much personal data, a competitive market would respond by offering users services that collect as little data as possible and if necessary, charge a subscription fee.[59] The emergence of

[52] Ibid para 350.

[53] Claus-Georg Nolte, Jonas Schwarz, and Christian Zimmermann, 'Social Network Services: Competition and Privacy', in Jan Marco Leimeister and Walter Brenner (eds.), *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (Institut für Wirtschaftsinformatik, Universität St.Gallen, 2017)* (2017) 829.

[54] Facebook has faced critics for targeting users' based on their emotional states and allowing advertisers 'to reach those who feel "insecure," "anxious," or "worthless."' See Matthew Crain and Anthony Nadler, 'Commercial Surveillance State: Blame the Marketers', (*NPlusOne*, 27 September 2017).

[55] See Brandimarte, Acquisti, and Loewenstein (n 46).

[56] Ramon Casadesus-Masanell and Andres Hervas-Drane, 'Competing with Privacy', *Management Science,* 61/1 (2015) 4 (noting that 'higher intensity of competition ... can result in an increase in the stock of information disclosed'). Paul Ohm, 'The Rise and Fall of Invasive ISP Surveillance', *U. Ill. L. Rev.,* 5(2009) 1425-1427 (showing how intense competition in the broadband market has led to 'trading user secrets for cash').

[57] Joseph Bonneau and Sören Preibusch, 'The Privacy Jungle: On the Market for Data Protection in Social Networks', in Tyler Moore, David Pym, and Christos Ioannidis (eds.), *Economics of Information Security and Privacy* (Springer, 2010) 132-135. Social networks (SN) are broadly defined to include services that are available for anyone to join where 'people commonly present their real-world identity' and interact 'with others via profile pages on the Web.' The definition includes general-purpose SNs that have over 500000 users (e.g. Facebook), specialised SNs (e.g. LinkedIn), media-recommendation sites (last.fm). Excluded are websites such as YouTube, instant messaging services, online-role playing games, and SN not available in English. Ibid 124-126.

[58] See O'Brien and Smith (n 47) 37. Stucke and Grunes (n 21) 51.

[59] See Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer law and Data Protection', *Journal of Intellectual Property Law & Practice,* 11/11 (2016) 859.

numerous services in the last few years trying to cater to the privacy concerns of individuals is a confirmation that companies can compete through differentiation. A prominent example is the search engine DuckDuckGo that differentiates itself through its privacy policy, promising users that it does not track or share their personal data. Its marketing motto is 'The search engine that doesn't track you.'

Despite such emerging competition, consumers still suffer from a lack of viable alternatives.[60] For example, the EDPS noted that the market for privacy and PETs is underdeveloped.[61] Similarly, The Economist observed that consumers are 'showing symptoms of what is called "learned helplessness"' where they have no choice than to accept 'impenetrable' terms and conditions on their data use.[62] Consumer surveys further strengthen the lack of viable alternatives. According to Eurobarometer survey, many Europeans feel they have lost control over their privacy, with 71 percent indicating the lack of alternative to obtain products/services without providing their personal information.[63] A similar survey of Americans found that the majority 'are resigned to giving up their data' and 'believe [that] it is futile to manage what companies can learn about them'.[64] Another survey documents the lack of adequate differentiation through data collection practices and privacy policies among search engines and social networking sites.[65] The study underlines that welfare could be enhanced if there were more variances in the data collection practices and suggest that regulatory policy might target mandating that 'search engines and online social networks were more spread out over the continuum of privacy preferences.'[66] But before delving into what regulation can do, one needs to ask why the market is not offering adequately differentiated services that cater to privacy preferences of consumers, a subject discussed in the next section.

III. Structural and Behavioural Considerations

This section examines the structural and behavioural features that might hinder effective competition through data privacy and PETs. Structurally, the dominance of key digital markets by a handful of firms and their control of key gateways together with alignment of incentives

[60] Stucke and Grunes (n 21). See The UK Competition and Markets Authority, 'The Commercial Use of Consumer Data', (2015) para 3.78 (noting the 'absence of competition over privacy' and 'markets failing to deliver what consumers want').
[61] EDPS (n 48) 11.
[62] 'Fuel of the Future: Data is Giving Rise to a New Economy', (6 May 2017).
[63] TNS Opinion & Social, 'Special Eurobarometer 431: Data Protection', (2015) 7.
[64] Joseph Turow, Michael Hennessy, and Nora Draper, 'The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation', https://ssrn.com/abstract=2820060, (2015) 3.
[65] Preibusch and Bonneau (n 42) 281.
[66] Ibid.

of those dominant companies with players that depend on monetization of data (vertical integration) are relevant considerations. The behavioural considerations address some of the factors that limit users' ability to discipline firms for their data privacy practices. These behavioural considerations in turn can affect the supply of privacy-friendly services, leading to a 'dysfunctional' market equilibrium.[67] It bears mentioning that competition policy is ill suited to address many of these structural and behavioural considerations. However, these considerations carry important implications for competition analysis focusing on data privacy and PETs.

The structural considerations highlight the incentives and capabilities of firms to engage in practices that reduce or suppress competition in data privacy and PETs including the fact that such reduction could be a profit maximising strategy. This becomes important in analysing the incentives of firms to degrade such competition, for example following a merger, especially where leading digital players are involved. The behavioural considerations become important in assessing barriers (demand- and supply-side) that could prevent competitors and consumers from disciplining firms conduct in reducing the level of data privacy. This implies that to the extent that competition authorities view data privacy as a competition parameter, their findings on the ability of users' and competitors to constrain or react to reductions should be supported by empirical evidence on consumer behavioural and market realities.[68] Moreover, the discussions pinpoint that competition law, particularly merger control, is the appropriate regulatory tool to foster competition in data privacy and PETs where a firm that breaks the 'dysfunctional equilibrium' by offering better privacy becomes a target of acquisition by dominant players that have their business models on the monetisation of personal data (see Section III(B)). Further legal implications of the structural and behavioural considerations are dealt with under Section IV, particularly Section IV(B).

A. Structural Considerations

The number of firms and their vertical integration are two commonly discussed structural characteristics that affect competition in a market. In this regard, two structural factors may contribute to the lack of effective competition on data privacy and PETs. The first is that key digital markets and gateways are dominated by a handful of players with business models that rely on monetization of personal data.[69] Google controls more than 90 percent of the Internet

[67] Joseph Farrell, 'Can Privacy be Just Another Good?', *J. on Telecomm. & High Tech. L.,* 10 (2012) 258-259.
[68] For more on how behavioural considerations can inform antitrust see Amanda Reeves and Maurice Stucke, 'Behavioural Antitrust', *Indiana Law Journal*, 86 (2011). Avishalom Tor, 'Understanding Behavioural Antitrust', *Tex. L. Rev*., 92 (2013).
[69] Stucke and Grunes (n 21) 66.

Search market in Europe (and globally).[70] Google's Android mobile operating system (MOS) commands around 80 percent market share in Europe and around the globe.[71] Google Play is the leading App store in terms of total number of app downloads with more than 60 percent global market share.[72] In YouTube, Google owns the largest video sharing site and the third most visited site in the globe with more than 1.5 billion registered users. Moreover, Google Chrome is the most used browser in Europe with more than 50 percent of market share.[73]

Although precise figures are difficult to find, Facebook is the leading social network with more than two billion active users globally and an estimated market share of above 45 percent. Additionally, Facebook owns the most popular messaging apps, WhatsApp and photo-sharing app, Instagram with more than 1.2 billion and 700 million users. For app developers, Facebook is not only a platform with more than 2 billion users but also a provider of social login functions. A study by the Commission shows a significant increase, from 11 percent in 2014 to 88 percent in 2015, in the use of social network accounts for logging into other apps (websites).[74] Such concentration has significant implications for competition in data privacy and PETs.

One implication is that like any other market where companies have dominance, these players have little incentive to compete on data privacy and PETs. The resulting weak competition may allow the dominant firms to engage in excessive data collection and offer fewer privacy options than would be the case in a competitive market.[75] This is compounded by the fact that more data might enhance the quality of the service, e.g. the search result. This means that users may lack 'qualitatively similar' search engines, which might in turn force them to accept much higher prices (in the form of collected data) and further-reaching privacy policies than what could be expected in situations of effective competition.[76] As noted above, there is some empirical research supporting this claim.

The second and more important structural feature is that given the nature of their business models, the interests of the dominant platforms are more aligned with actors that compete on collecting and monetizing personal data than actors trying to limit and enhance users control over their data (alignment of incentives with vertical players). In 2015, Google generated more than 90 percent of its revenue from advertising and in 2016, advertising accounted for 88

[70] CASE AT.39740 *Google Search (Shopping)* [2017] decision of 27 June 2017, para 283. Also Statista.com
[71] European Commission, 'Commission Sends Statement of Objections to Google on Android Operating System and Applications', (20 April 2016).
[72] Ibid.
[73] Statista.com
[74] European Commission, 'Commission Staff Working Document: Online Platforms SWD(2016) 172', (2016) 35.
[75] Kerber (n 59) 860.
[76] Ibid. See Monopolkomission, 'Competitition Policy: The Challenges of Digital Markets', *Special Report No 68* (2015) 75.

percent.[77] Advertising accounted for 97 percent of Facebook's revenue in 2016 up from 95 percent in 2015.[78] This reliance on advertisement of such dominant players leads to an environment where the companies create an ecosystem that rewards players engaging in collection and tracking of users and punishes those that try to prevent or mitigate such behaviour. For example, Google's AdSense is an advertising network that allows publishers (website owners) to serve ads and earn 'extra revenue'. According to Google, 'AdSense shows timely and relevant ads alongside your own online content – and pays whenever someone clicks'.[79] Similarly, Google's AdMob is described as the 'the best platform to monetize your apps and maximize your ad revenue through advertising'.[80]

These rewarding schemes create competition for more clicks on the ad, which websites and apps try to achieve by collecting as much personal data as possible in order to better target the advertisement.[81] Given that Google's revenue is also dependent on users clicking the ad, Google offers such apps and websites tools that facilitate better targeting of the ads. For example, AdMob offers app owners the 'best-in-class technology' that allows them to 'gain insights about your users'.[82] Similarly, ad networks such as Google's AdSense and DoubleClick offer publishers tools to better target ads including tools for tracking consumers and improve the ads.[83] Additionally, the data collected by third party websites and apps feed into the advertising networks and exchanges primarily controlled by Google (AdSense and DoubleClick) and Facebook.[84] Thus, it is in Google's (and Facebook's) monetary interest that publishers and apps are able to track and better target users so that users can click on the ad. Once users click on the ad, Google and Facebook get paid, and publishers and app developers 'get their cut'.[85] This alignment in commercial interest in turn can lead the platform to disregard the privacy concerns of its users.[86]

Thus, it is not surprising to see that such platforms perceive innovations and the competition in privacy as a threat to their business models. Google identifies technologies that block ads

[77] Alphabet Inc. FORM 10-K, 'Annual Report for the Fiscal Year 2016' (2017) 7.
[78] Facebook Inc. FORM 10-K 'Annual Report for the Fiscal Year 2016' (2017) 9.
[79] See https://www.google.com/adsense/
[80] See https://www.google.com/admob/
[81] Ariel Ezrachi and Maurice Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard UP, 2016) 182-183.
[82] See https://www.google.com/admob/
[83] European Commission (n 74) 38.
[84] See Wolfie Christl, 'Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions', (CRACKED LABS, 2017).
[85] Ezrachi and Stucke (n 81) 183.
[86] See ibid.

and the tracking of users through cookies as a threat to its business model and its revenue.[87] Similarly, Facebook indicates the threat of ad and cookie blockers.[88] In its latest report, Facebook identifies 'the success of technologies designed to block the display of ads' and 'the degree to which users cease or reduce the number of times they click on our ads' as key threats to its financial results and its business model.[89] Ad and cookie blockers do exactly that – block ads but also prevent tracking through cookies, which reduces the likelihood of users' clicking on the ad.

Two points bear reiterating from the foregoing discussion. First, given the dominance of key digital markets by few players, the dominant platforms have little incentive to compete on data privacy and PETs. Secondly, the reliance of their business models on advertising means they consider such competition as a threat, which in turn can give rise to incentives to suppress competition. Culminating these two considerations is that these companies control key gateways to consumers, e.g., App Stores, MOS and other platforms (ecommerce or search). It is trite that such platforms are important 'entry points to certain markets and data' and have significant power in how different players are remunerated.[90] This control gives the companies the power to set the rules of the game on who gets in, who gets promoted, who gets demoted in their platforms, and ultimately the power to 'control and cut off' the 'oxygen supply' of many digital players.[91] In light of the above three factors, the dominant platforms not only have the incentive but also the ability to suppress the competition in data privacy and PETs.[92]

Such harms to competition could take the form of excluding a company from gaining access to consumers e.g. blocking a privacy-enhancing app from App stores or using their financial muscle to acquire a start-up that threatens the financial results of the dominant firms by offering greater privacy. For example, in 2015 Google expelled an ad blocking software, Disconnect, from its Play Store, citing that the app violates the terms and conditions.[93] The Disconnect app allows users to safeguard their 'privacy and security … by blocking invisible, unsolicited network connections between a user's browser or mobile device and sites/services that engage

[87] See Alphabet Inc. FORM 10-K (n 77) 16.
[88] Facebook Inc. FORM 10-K (n 78) 19.
[89] Ibid 9 & 13.
[90] European Commission, 'Commission Communication on A Digital Single Market Strategy for Europe, COM(2015) 192 final', (2015) 11-12.
[91] Ezrachi and Stucke (n 81) 145. For discussion on the implications of 'gatekeeping power' for human rights, see Orla Lynskey, 'Regulating Platform Power' *LSE Legal Studies Working Paper No. 1/2017*, 13ff.
[92] Harbour and Koslov (n 21) 795. Giuseppe Colangelo and Mariateresa Maggiolino, 'Data Protection in Attention Markets: Protecting Privacy Through Competition?', *Journal of Competition Law and Practice*, 8(6) (2017) 2.
[93] Following the ban, Disconnect filed a complaint against Google for infringement of Article 102 TFEU 'through bundling into the Android platform and the related exclusion of competing privacy and security technology'. See Case COMP 40099 *Complaint of Disconnect, Inc.* [2015] Unreported.

in invisible tracking or are known or suspected distributors of malware.'[94] Recently, citing the same reason, Google banned AdNauseam, a research-based privacy tool, that limits the tracking of users.[95] In contrast, Google fails to take the same action for apps that deliberately deceived users about how their data is used and thereby violate its privacy policy for the App store.[96] Similarly, the acquisition of WhatsApp by Facebook was viewed as an elimination of a competitive threat that attracted users from Facebook through its greater privacy protection.[97]

Whether the above specific conducts constitute anticompetitive in light of current competition rules is beyond the scope of this article. For example, blocking an app from a dominant App Store may not constitute anticompetitive conduct unless the App Store is an essential facility. However, one could ask whether competition law is equipped to deal with multiple conducts where an ad blocker is banned from a dominant App store (e.g. Android), demoted from the dominant search engine (Google search) and blocked by the dominant Browser (e.g. Chrome) at the same time. What happens if such conducts are used strategically over time to kill the momentum for such services? The question is relevant because of the important role that momentum plays in the adoption of technology in general but also in privacy enhancing services.[98] These are issues that need consideration going forward and the recent Commission initiative to address platform fairness and transparency is a step in the right direction.[99] For now, it suffices to indicate that competition law may not be best suited to creating incentives to compete in privacy; however, these considerations would be relevant in assessing the extent entities might engage in privacy reducing conducts (see Section IV(B)).

B. Behavioural Considerations

One might reasonably argue that if existing players lack the incentive to compete and offer users the desired level of privacy, new players would enter or existing players would reposition to cater to users' privacy preferences. Additionally, although the control of key gateways may make it difficult for the new players to compete effectively, one could still argue that they, as Facebook and Google have done, can build their own platforms. The main reason for lack of effective competition on data privacy and PETs, some argue, is that consumers, particularly the

[94] Ibid.
[95] See https://adnauseam.io/free-adnauseam.html
[96] Ezrachi and Stucke (n 81) 181-182.
[97] Stucke and Grunes (n 21) 262. See Samson Esayas, 'Competition in Dissimilarity: Lessons in Privacy from the Facebook/WhatsApp Merger', *CPI Antitrust Chronicle*, 1/2 (2017).
[98] Ashlin Lee, 'A Question of Momentum–Critical Reflections on Individual Options for Surveillance Resistance', *Teknokultura*, 11/2 (2014).
[99] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on promoting fairness and transparency for business users of online intermediation services COM(2018)238.

young generation, do not care about privacy, i.e., no sufficient demand for privacy. Marc Zuckerberg's remark that 'privacy is no longer a social norm'[100] is emblematic of this stance. It may be true that some consumers care less about their privacy than others, but there is hardly any evidence to draw broader conclusions.[101] In fact, there are many empirical studies showing that consumers, including younger ones, care about their privacy.[102]

Another related claim is that even if consumers care about their privacy, they do little to protect it and the market responds to this signal. In other words, markets respond to what users signal through their actions and choices, known as the 'revealed preference theory', rather than to consumers' stated attitudes in surveys.[103] However, several behavioural considerations might prevent consumers from translating their 'inner' preferences into actions and limit their ability to discipline (reward) firms' behaviour on data privacy and PETs.

At the forefront of the behavioural considerations is the information asymmetry between users and firms in terms of what data is collected and how it is used. At least in the EU context, such information asymmetry and the potential market failure from such asymmetry is one of the justifications for data privacy regulation,[104] which, among others, try to ameliorate the asymmetry by forcing firms to provide users certain information on the kind of data collected and the purpose for its use.[105] Such disclosure rules are also important in facilitating 'competition on privacy' by informing users about privacy practices and allowing users to make choices that fit their preferences.[106] Often companies try to comply with such requirements through privacy policies. However, in practice, privacy policies are of little help for users.

---

[100] Bobbie Johnson, 'Privacy No Longer a Social Norm, Says Facebook Founder' (*The Guardian*, 11 Jan 2010)
[101] Stucke and Grunes (n 21) 57.
[102] Chris Hoofnagle et al., 'How Different are Young Adults From Older Adults When it Comes to Information Privacy Attitudes & Policies?' http://repository.upenn.edu/asc_papers/399 (2010) 3 (concluding that young adults are as concerned as their older counterparts). See Mary Madden and Lee Rainie, 'Americans' Attitude about Privacy, Security and Surveillance' (Pew Research Center, 2015). On the European side, the Eurobarometer survey shows that 67% of respondents 'are concerned about not having complete control over the information they provide online'. Furthermore, 57% of respondents disagree with the statement, 'providing personal information is not a big issue for you'. See TNS Opinion & Social (n 63) 6. Another Eurobarometer survey on 'online platforms' reaffirms the above claims with 72% of consumers 'concerned about the data collected about them or their activities.' See TNS opinion & Social, 'Special Eurobarometer 447: Online Platforms', (2016) 40.
[103] See Joshua Wright and Douglas Ginsburg, 'Behavioral Law and Economics: Its Origins, Fatal Flaws, and Implications for Liberty', *Northwestern University Law Review*, 106/3 (2012) 1034.
[104] Orla Lynskey, 'Deconstructing Data Protection: The 'Added-Value'of a Right to Data Protection in the EU Legal Order', *International and Comparative Law Quarterly*, 63/03 (2014).
[105] 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), Article 11-13.
[106] Florencia Marotta-Wurgler, 'Self-Regulation and Competition in Privacy Policies', *The Journal of Legal Studies*, 45/S2 (2016) 2 & 8.

Many studies have shown that, first, users hardly read those policies.[107] Even when they do, the policies are obscure and full of legalese. Leaving data subjects in the dark—i.e. confusology—in terms of how their data is used is a prevalent business practice.[108] Thus, unless consumers are able to understand properly how firms use their data, they are unable to discipline firms' behaviour in relation to privacy. Having analysed 261 privacy policies across seven markets, Marotta-Wurgler concluded that in the current state of affairs, privacy polices fail to serve users and if this continues, competition through privacy cannot work.[109]

In the rare case that consumers read and understand the policies, other behavioural considerations may impair them from behaving competitively. Examples include uncertainty on privacy risks, immediate gratification, and status quo bias. For example, users, even those who are privacy sensitive, tend to engage in risky information revelations in the face of immediate benefits from disclosure (e.g., unlocking a feature).[110] Another behavioural phenomenon that might affect users' privacy decisions is status quo bias, particularly default settings.[111] Defaults make switching difficult even if users are able to detect degradation and have information about an alternative product/service with superior data privacy protections.

Moreover, the above demand-side considerations transform into supply-side problems where firms' incentives become aligned with users' undesirable behaviour, leading to what economist Farrell refers to as the 'dysfunctional equilibrium'.[112] One outcome of the abovementioned consumer behaviour on privacy policies is that new entrants learn that they are unable to affect demand by opting for 'more protective policies and clearer disclosures' and 'making privacy-protective promises'.[113] This is partly because firms expect that users will not read privacy policies and reward them for this behaviour.[114] Some surveys support this assertion. Research among 45 social networks shows that the majority do not mention privacy as a promotional tool and no site attempted to use the content of its privacy policy as a draw to its services.[115] Even sites that mention privacy as a promotional tool do so in 'a vague and

[107] According to 2015 Eurobarometer survey, only one in five (18%) fully read privacy statements. TNS Opinion & Social (n 63) 7. This is partly because it would take about 30 full working days every year for an average person to read the privacy policies of websites they visit. World Economic Forum and Boston Consulting Group, 'Unlocking the Value of Personal Data: From Collection to Usage', (2013) 11.
[108] Ryan Calo, 'Privacy and Markets: A Love Story', *Notre Dame Law Review*, 91(2)(2016) 673.
[109] Florencia Marotta-Wurgler, 'Understanding Privacy Policies: Content, Self-Regulation, and Markets', (2016) https://ssrn.com/abstract=2736513 25.
[110] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, 'Privacy and Human Behavior in the Age of Information', *Science*, 347/6221 (2015) 510.
[111] Ibid.
[112] Farrell (n 67) 257.
[113] Ibid.
[114] Ibid 259.
[115] Bonneau and Preibusch (n 57) 134.

general fashion'.[116] This, together with the dominance of few players and lack of viable alternatives, leads to consumer cynicism i.e. consumers learn that firms will not protect their data privacy regardless of their privacy promises;[117] consumers become 'resigned'[118] or develop 'learned helplessness'[119]. This cynicism may explain why even those firms that promote privacy do not get adequate reward. In this regard, the above research on social networks found that sites promoting privacy registered a significantly weak increase in traffic during the study period than sites which do not promote privacy.[120]

The combination of consumers' cynicisms and firms' lack of incentive leads to 'dysfunctional equilibrium', which Farrell explains as follows:

> If firms perceive that few consumers shift their demand in response to actual privacy policies, then the firm's incentives are to make its policy noncommittal and/or non-protective, and to go for the biggest available [revenue from reusing the data] ... It would then be tempting to design disclosures so as not to really communicate the choice of policy, if it is possible to obfuscate for the minority of consumers while retaining the ability to claim that the policy was disclosed. Meanwhile, if consumers perceive that firms behave in this kind of way, they will not expect attentive reading of privacy policies to be a rewarding activity. These patterns of conduct and expectations would reinforce each other, which is what makes them a game-theoretic or economic equilibrium.[121]

The challenge is that such equilibrium can be very hard to break because a) a consumer cannot suddenly start reading privacy policies as they do not see it as a rewarding activity; and b) even if she does, she is likely to learn little or get a confirmation of her cynicism as firms still expect that few consumers read polices and opt for vague policies.[122] Similarly, a smaller firm's ability to break such equilibrium is limited because users do not reward such behaviour and the firm's demand would not shift significantly; thereby the firm can only sacrifice revenue from monetizing data.[123] Thus, more often, Farrell argues, escaping such equilibrium requires actions 'by large and powerful players'.[124] However, as noted in Section III(A), the dominant players lack the incentive to break this equilibrium because their interests are better served in such equilibrium and can even contribute to its perpetuation by making it difficult for smaller players to break the equilibrium through blocking and demoting such players in their platforms.

---

[116] Ibid.
[117] Farrell (n 67) 257.
[118] Turow, Hennessy, and Draper (n 64) 3.
[119] The Economist (n 62).
[120] Bonneau and Preibusch (n 57) 153.
[121] Farrell (n 67) 258-259. Farrell describes the dysfunctional equilibrium as 'cynical market failure' because it 'can make mutually beneficial trades impossible.' Ibid 257. Others have discussed the 'lemons market for privacy'. See Bonneau and Preibusch (n 57) 149.
[122] Farrell (n 67) 259.
[123] Ibid.
[124] Ibid.

Furthermore, in the rare instance where a small player manages to break the equilibrium and attracts users, they might use their financial muscle to acquire such players and suppress emerging competition. A case in point is the acquisition of WhatsApp by Facebook and the subsequent change to WhatsApp's' privacy policy, which contributes to the perpetuation of the 'dysfunctional equilibrium'.

This is because WhatsApp was trying to disrupt market conditions based on harvesting personal information and offering behavioural advertisement by adopting a business model that was built on respecting users' privacy in exchange for small subscription fee. Contrary to Facebook, WhatsApp only stores limited information about its users and does not offer targeted advertisement. In this sense, one could argue that WhatsApp was seeking to disrupt the most commonly used business model that benefited Facebook, which is partly a result of the 'dysfunctional equilibrium'[125] and the 'free' effect.[126] From its popularity,[127] WhatsApp was succeeding in disrupting the equilibrium[128] and overcoming the challenges of the 'free effect', which seem to be halted by the merger.

Following the merger, WhatsApp not only changed its privacy policy to share data with Facebook but also, abandoned its subscription model by adopting a monetization strategy that allows users to communicate with businesses via WhatsApp. These changes could be sources of new information for WhatsApp (e.g., insights into health of users if a user is communicating with a psychiatrist) and WhatsApp has indicated that it would not exclude the possibility of introducing ads into its services.[129] This implies that before the merger, users had the option to choose among the leading messaging apps, one based on a subscription fee, minimum collection of personal data and an ad free experience; and another that heavily relies on collection and monetization of users' data, which seems to have disappeared after the merger.[130] Following the merger, the two leading messaging apps rely on monetization of personal data, taking aback the initial steps WhatsApp has taken in disrupting the 'dysfunctional equilibrium' and overcoming the 'free effect'. Thus, in the rare case where a small player breaks this equilibrium

[125] See Stucke and Grunes (n 21) 133.
[126] 'Free effect' relates to the nudging power of 'zero' price products/service and consumers' tendencies to overvalue such products/services even if they do not advance their 'revealed preferences'. See Newman (n 13) 183ff. One implication of the 'free effect' is that consumers' willingness to pay for a similar but much better alternative would be significantly reduced, which in turn makes entry into markets with 'zero' price difficult.
[127] WhatsApp had managed to acquire 600 million users even in a shorter time than Facebook and had more users than Messenger (approximately 250-350 million users). See *Facebook/WhatsApp* (n 17) para 84.
[128] Stucke and Grunes (n 21) 133.
[129] Deepa Seetharaman, 'Facebook Tees Up WhatsApp to Make Money', (*The Wall Street Journal*, 5 Sep 2017).
[130] Accordingly, the merger 'has entailed a loss of options by the user … [and] (decreased quality in terms of privacy)'. See Autoritat Catalana de la Competència, 'The Data-Driven Economy Challenges for Competition', (2016) 26.

and manages to attract users, competition policy seems to be the appropriate regulatory tool to protect the consumers' interest and prevent the nascent competition from being cut short. Absent that, acquisitions of WhatsApp's kind will only perpetuate the 'dysfunctional equilibrium' and competition on privacy and PETs will hardly mature.

Overall, these structural and behaviours considerations will affect the effectiveness of competition through data privacy and PETs, which need to be accounted for in competition analysis. However, given the limited scope of competition law (players with market power), other regulatory tools might be better suited to address some of the problems. For example, some of the changes under the General Data protection Regulation (GDPR) are aimed at mitigating the problems related with information overload and cognitive limitations. The rules introduce the possibility of communicating information to consumers using standard icons.[131] Standardizing information provision is a move in the right direction. Similarly, the principle of 'data protection by design and by default' will be important in 'hardwiring' privacy into services/products and incentivizing the development of PETs. However, at least in the EU context, data privacy rules impose an upper ceiling (maximum harmonisation) that flows from their goal of facilitating free flow of data.[132] Thus, the market remains key in incentivizing firms to aspire to provide even higher levels of privacy than those guaranteed under the rules through competition – provided such competition (its harm) is given proper consideration under competition law. The next section explores the role that competition law can play.

IV. The Role of Competition Law

At its core, competition policy is aimed at maintaining and prompting competition in private markets. The overarching question for this section is: what role can competition law play in maintaining and promoting competition in data privacy and the deployment of PETs.

First, as digital markets evolve towards services offered at 'zero' price but in exchange for personal data, the definition of market power should reflect the ability of firms to reduce the level of data privacy. An essential first step towards this is to recognize that privacy and the development of PETs constitute parameters of competition for digital services particularly where such services are provided in exchange for personal data. As shown in Section I, competition policy has already shown its flexibility to accommodate such competition. This is

[131] GDPR, Article 12(7).
[132] Dan Svantesson, 'Enter the Quagmire - The Complicated Relationship between Data Protection Law and Consumer Protection Law', *Computer Law & Security Review*, 34/1 (2018).

an important step forward if competition policy is to play a role in maintaining and prompting competition through data privacy and PETs.

The next and most important step is giving due regard to data privacy practices of firms and competition in privacy in assessing market power. Here, I offer two suggestions that could help promote competition in data privacy and PETs.

A. Proxies for Market Power (Share) that Better Capture Data Privacy

How market power is computed is often associated with how it can be exerted. In services where money changes hands, the reliance on a turnover to assess market power is justified because if a firm charges prices above the competitive level, its turnover would reflect such ability. In other words, a significantly high turnover, compared to competitors, signals the ability of the firm to charge higher prices than its competitors but also the limited ability of the competitors to respond to the price increase and thereby impose competitive constraints. To the extent that market power in zero price markets could be exerted by reducing the level of privacy, at issue is whether the proxies used to compute market share are able to capture the privacy considerations behind the collection and use of personal data.

The main point advanced here is that to the extent that market share is the relevant indicator of market power in services offered at 'zero' prices but in exchange for personal data, competition authorities ought to resort to proxies that could also cater to the data collection practices and related data privacy concerns of individuals.[133] Depending on the specific market, market share could be assessed based on different considerations and some proxies are better at capturing data privacy concerns than others. For example, in social media, market share could be computed based on the total number of users, active number users, or time spent on the service. But as shown below, the metric based on 'time spent' might be better at capturing the privacy concerns resulting from the data collection and use.

In the Facebook/WhatsApp merger, the Commission evaluated different proposals for computing market share. The merging parties suggested a metric based on the 'reach data', i.e., the percentage of users that have used an app during the last 30 days on iOS and Android smartphones.[134] While acknowledging its shortcomings, the Commission relied on the suggested metric citing the lack of reliable data on other metrics.[135] In so doing, the Commission

[133] The German Act against Restraints on Competition is amended to take account of the importance of data in market power assessments. See Daniel Wiedmann, 'Germany: Reform of German Competition and Merger Control Law' (*Mondaq*, 8 July 2016) (link). This is a step in the right direction. As much as high turnover can reflect the ability of a firm to charge a price above the competitive level so can scale and scope in data be indicative of the ability of a firm to extract excessive data than would be the case in a competitive market.
[134] *Facebook/WhatsApp* (n 17) para 97.
[135] Ibid.

rejected other suggestions from respondents. Among the suggestions submitted was one based on 'monthly minutes of use (how long a user engages with the app).'[136] Such metric, the respondents suggested, better captures '(i) the importance of the application to the end consumer (i.e. consumer engagement) and (ii) its potential value either through direct monetisation from the consumer or indirectly through advertising.'[137]

The time-based metric is also relevant from a data privacy perspective because it can better capture the data privacy interests of individuals where the business model relies on monetizing users' data than the metric suggested by the merging parties. This is because, first, although inconclusive, there is some empirical evidence showing that the more time users spend on a service, the more data they provide. According to a study conducted on Facebook users, 'the amount and scope of personal information that Facebook users revealed' has increased over time.[138] Another research shows the existence of a positive correlation between the time users spend on social networks and the content they generate.[139] Generating and interacting with content is often an additional source of personal data (observed and inferred) for such sites.

Secondly, as argued elsewhere,[140] the use of many digital services such as Facebook is associated with a continuous generation of personal data, which leads to overexposure, and loss of practical obscurity. This implies that the more time users spend on such services, the higher the risks to their privacy. This claim is strengthened by one study, which finds a positive correlation between users' privacy concerns and duration of usage, i.e. users' privacy concerns grew overtime through usage.[141] According to this research, users of new social networks have often 'little data uploaded and thus their privacy is less of a concern.'[142] In light of these considerations, a time-based metric could indirectly capture such concerns. In contrast, the metric based on 'reach data', followed by the Commission in Facebook/WhatsApp, would treat two apps with the same number of monthly users but significantly different amount of time spent on the apps (impliedly different privacy implications) as having the same market share and consequently market power, which may underestimate the above evidence of more time and higher privacy concerns.

[136] Ibid.
[137] Ibid.
[138] Stutzman, Gross, and Acquisti (n 46) 27.
[139] Nolte, Schwarz, and Zimmermann (n 53) 829.
[140] Samson Esayas, 'The Idea of 'Emergent Properties' in Data Privacy: Towards a Holistic Approach', *International Journal of Law and Information Technology*, 25/2 (2017).
[141] Bonneau and Preibusch (n 57) 158.
[142] Ibid.

Thirdly, using time as proxy captures situations where multi-homing could actually be a sign of market power over privacy sensitive groups. Unlike traditional goods/services, users can simultaneously use different digital services/products. No doubt, this facilitates entry into market and the possibility of exerting competitive constraints on existing players. However, sometimes, the impact of multi-homing on competition through data privacy can be exaggerated. This is partly because consumers who have downloaded an app (e.g. X) with better privacy conditions may still be forced to spend most of their time on another app (e.g. Y) with lesser privacy because of network effects. In such cases, the choice to multi-home between the apps (X & Y) is not necessarily an indication that these services exert competitive constraints on each other.[143] Instead, it can be an indication of the market power that Y has over the consumer group with higher privacy preferences that would have preferred using just X. This is described as a situation where 'the tyranny of the majority dictates the privacy choices of the minority.'[144] In such circumstances, time spent could be used to test whether a service (e.g. Y) may be exercising market power over the users who might have wanted to stick with just X. For example, a significant disparity in the time spent among the two services (e.g. X & Y) may give a preliminary indication that the service where users spend most of their time (e.g. Y) may be exercising market power over certain group of users regardless of users' multi-homing.

Moreover, time spent is positively associated with lock-in effects. This is because time spent curating and updating their profile on a social network can discourage users from multi-homing across different services and make it difficult to exit the network.[145] Such customer lock-in can give firms an incentive to engage in opportunistic behaviour, such as changing privacy policies or making such policies difficult to enforce,[146] which could be a sign of market power in such markets. From an administrative perspective, data on time spent could be easily available as market players collect such data for commercial purposes.[147]

Assessing market power through time spent (attention) is not necessarily novel although most discussions do not focus on its significance to cater to data privacy concerns. Having noted that online platforms compete on attention, Evans suggested computing market power through time spent, being the best proxy to measure attention, across broadly defined markets including

[143] Stucke and Grunes (n 21) 168.
[144] Ibid.
[145] *Microsoft /LinkedIn*, (n 50) para 345.
[146] Jan Whittington and Chris Hoofnagle, 'Unpacking Privacy's Price', *North Carolina Law Review*, 90/5 (2012).
[147] Tim Wu, 'Blind Spot: The Attention Economy & the Law', *Antitrust Law Journal* (2018 forthcoming) 8 https://ssrn.com/abstract=2941094.

search, social media, and ecommerce websites.[148] All such websites compete for scarce resource i.e. users' attention and the popularity of one service necessarily diverts attention from the other regardless of their content and thus ought to be in the same relevant market.[149] This implies that in assessing the market power of Google, one would factor in the time users spend on all Google services (e.g. Search, Maps and Gmail) vis-a-vis the time users spend on other platforms such as Facebook and Amazon. This is an interesting suggestion from data privacy perspective because it can also capture the data privacy concerns resulting from collecting and combining data across many services.[150] However, for competition law purposes, what is important is the substitutability of the services, not whether one service takes attention away from other services. Otherwise, such approach would lead to excessively broad markets as most paid products/services also compete for one scare resource i.e. users' money.[151] Wu offers similar suggestions where the market power of 'attention brokers' such as Facebook and Google is measured based on the time spent on such platforms.[152] Wu departs form Evan's suggestion in that the attention could be based on narrowly defined markets such as search or social media, which is more in line with current Commission practice.[153]

Overall, where market power is assessed in 'zero' price markets through market share, competition authorities could use a metric, where feasible, that can also cater to data collection practices of firms and associated privacy concerns. As shown above, relying on the time spent allows competition authorities to factor in, albeit impliedly, the personal data that consumers provide, the associated privacy concerns from more usage, the possibility to exert market power in the face of multi-homing and the lock-in problem from spending more time on a service. This is particularly the case if privacy is considered a parameter of competition. No denying such metric will have its own deficiencies,[154] but the goal is not to promote a particularly proxy for computing market share. Instead, the main suggestion is that where competition authorities have the possibility to use different proxies for assessing market share in markets where services are provided at zero price but in exchange for personal data, a good rule of thumb could be to

[148] David Evans, 'Attention Rivalry among Online Platforms', *Journal of Competition Law & Economics,* 9/2 (2013).
[149] Ibid 317.
[150] See Esayas (n 140)
[151] As one Court has noted 'when the automobile was first invented, competing auto manufacturers obviously took customers primarily from companies selling horses and buggies …, but that hardly shows that cars and horse-drawn carriages should be treated as the same product market.' Cited in Newman (n 13) 176.
[152] Wu (n 147) 25.
[153] *Google Search (Shopping)* (n 70). *Facebook/WhatsApp* (n 17).
[154] See *Facebook/WhatsApp* (n 17) para 97.

test the extent to which the different proxies cater to the possible risks from data collection and reduction in privacy, which can be a reflection of market power in such markets.

B. Competitive Constraints and Incentives behind Firms' Data Privacy Practices

Analysis of competitive constraints takes central stage in market power assessment. Regarding the competition on privacy and PETs, attention is drawn to the following three issues. The first deals with sources of competitive constraints. In conventional markets, the view is that the more identical the products are, the stronger the competitive constraints they impose on each other. This is the approach followed by the Commission in Facebook/WhatsApp where differences in privacy policies was taken as a sign that makes the messaging services complementary rather than competitors. However, as shown elsewhere,[155] competition analysis needs to embrace the possibility that when it comes to privacy and privacy policies, competition is more sequential than simultaneous and dissimilarity either in the technology (e.g. deploying end-to-end encryption) or policy (offering better conditions of data collection and processing) can be just the beginning of a competition that exerts competitive pressure on others, rather than make the firms complementary. In addition, when a new service, e.g., WhatsApp, attempts to draw users from an established network by offering superior privacy, the existence of an established network, e.g., Facebook, albeit with a different privacy policy, can still discipline the former's (WhatsApp's) behaviour.[156] Thus, going forward, the focus should be on the competitive constrains that entities impose on each other through providing more attractive alternatives to privacy-prioritising consumers.

More importantly, market power assessment should give due regard to the competitive constraints on firms' data privacy practices. Generally, assessment of competitive constraints indirectly addresses factors, e.g. control of essential resources, which prevent other competitors from responding to a price increase or output reduction. The intuition is that if a firm controls an essential resource, the ability of competitors to respond to a price increase or output reduction is unlikely or untimely. The argument here is that when it comes to the competition in privacy and PETs, there are factors that may hinder competitors from responding to a reduction in privacy, which need to be accounted for in market power analysis.

One such factor is the consumer behaviour discussed under Section III(B). In his book, Patterson suggests computing market power in information markets having regard to the

[155] Esayas (n 97).
[156] Ibid.

potentially anticompetitive conduct and relevant factors that prevent competitors from responding to such conduct.[157] Among others, Patterson identifies the challenges in detecting degradation in quality of information products (e.g. search) by both consumers and competitors. One could identify similar factors regarding competition in privacy and PETs. As noted in Section III(B), consumers' decision-making in data privacy are impacted by information asymmetry, confusology and default settings (status quo bias). Similarly, if users do not read or understand privacy policies, firms are unable to attract demand by offering better privacy. These factors play a role in the ability of consumers and competitors to respond to a reduction in privacy and need to be taken in to account in market power analysis.[158] This implies, for example, that any assessment by competition authorities that pre-existing privacy policies would constrain a firm from behaving in a certain way without factoring in the limitations with consumer behaviour on privacy policies would be inadequate. The Commission's decision in Facebook/WhatsApp is illustrative of this problem.

Assessing how a reduction in privacy might serve as a constraint on the merged entity's incentive to introduce targeted advertisement in WhatsApp, the Commission noted that this would be unlikely because WhatsApp has to change its privacy policy and start collecting more data.[159] According to the Commission, if the merged entity were to change its privacy policy in order to collect more data (age, gender, country, message content) from WhatsApp users, some users may switch to 'less intrusive' and ad free texting apps.[160] Moreover, the introduction of ads might lead to abandoning the end-end encryption in WhatsApp, which might create dissatisfaction among users that value their privacy.[161] This analysis of competitive constraints is predicated on two assumptions that are untenable given consumer behaviour and the incentives of firms for collecting more data.

The first assumption is that users are able to impose effective competitive constraints on firm's data collection practices and privacy policies. However, the post-merger behaviour of WhatsApp to change its privacy policy without any adverse consequences demonstrates that the Commission's assumptions were built on shaky foundations. Two years after the merger, WhatsApp changed its privacy policy to the effect that data generated by WhatsApp will be shared with Facebook (and family companies), allowing Facebook to display more relevant ads

[157] Mark Patterson, *Antitrust Law in the New Economy* (Harvard UP, 2017) 84.
[158] Autorite de la Concurrence and Bundeskartellamt, 'Competition Law and Data', (2016) 23 (indicating that privacy policies are likely to impact competition when they are carried out by a dominant undertaking that relies on data as an input).
[159] *Facebook/WhatsApp* (n 17) para 174 & 186.
[160] Ibid.
[161] Ibid para 174.

on WhatsApp users' Facebook accounts.[162] However, unlike the Commission's prediction for users to punish such behaviour, the change seems to have no or little impact on WhatsApp.[163] Even after the change, WhatsApp remains the leading messaging service with active monthly users of 1.2 billion, up from 600 million users at the time of the merger. Then the question is how could WhatsApp, contrary to the Commission's prediction, be able to change its privacy policy to share data with Facebook and still remain a market leader in messaging services?

One explanation can be found in the above-mentioned behavioural considerations (Section III(B)). WhatsApp's privacy policy seems to have been designed with the objective that users are not alerted to the changes and to make it difficult for users to opt-out of sharing their data with Facebook. The following diagram shows the notification and the opt-out mechanism WhatsApp employed.

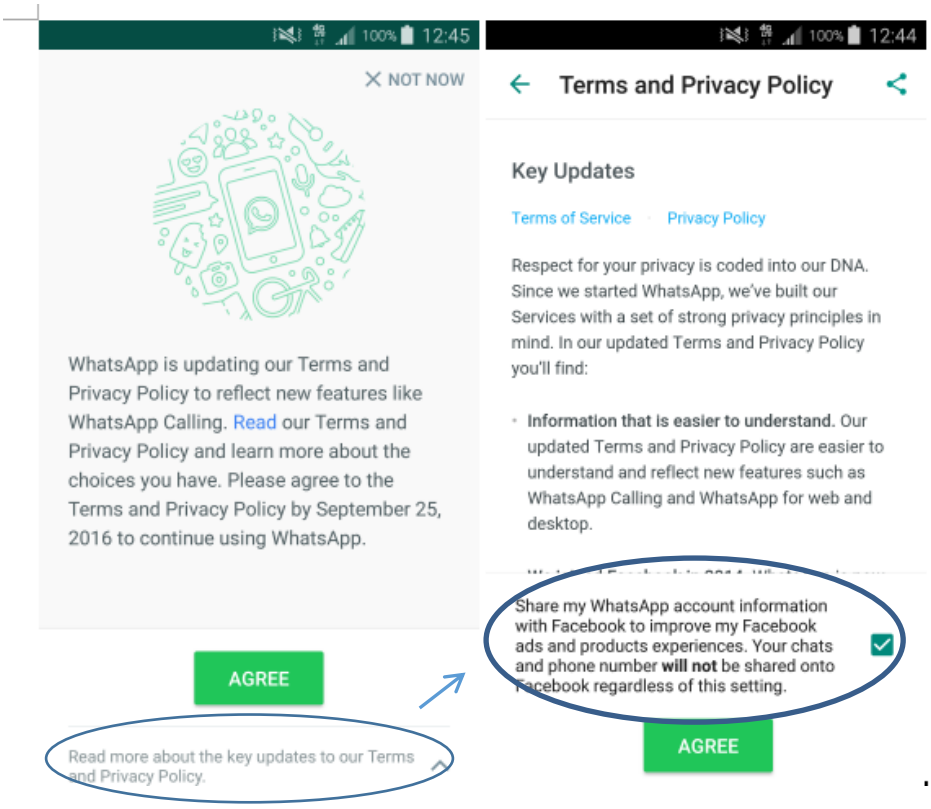

Figure 1 – WhatsApp's Privacy Policy Notice (Mobile)

As can be seen from the screenshot (left), first, users are prompted to 'agree' to updates on 'Terms and Privacy Policy' that 'reflect new features like WhatsApp calling' without any mention that data from WhatsApp will be shared with Facebook. By so doing, WhatsApp hides

[162] WhatsApp Blog, 'Looking ahead for WhatsApp' (25 August 2016).
[163] See Georg Clemens and Mutlu Özcany, 'Obfuscation and Shrouding with Network Effects - The Facebook/WhatsApp Case', https://ssrn.com/abstract=3023467, (2017). Stucke and Grunes (n 21) 169 (noting that the change 'did not prompt a significant exodus').

the central information from the first screen. In order to 'opt-out' and get more information, a user has to click 'read more about key updates' in smaller texts just below the 'agree' button. If a user clicks that, she is shown the screen on the right side of the diagram. Here WhatsApp reiterates its commitment to respect privacy of users and prompts users to agree to the sharing of 'WhatsApp account information with Facebook'. In the literature about behavioural economics, marrying critical information with other information can lead users to discount the significance of the former (in this case the sharing of their data with Facebook).[164] Agreeing to the terms will allow Facebook to use account information, such as mobile number, contact lists, and information about the last time of using the service. Here it is important to underline that the default, as shown by the checked-box, is set for users to agree to the sharing of their WhatsApp account information with Facebook. This means that a user who does not want to share her data with Facebook has to 'uncheck the box'. The complexity of the design clearly shows that how market players can exploit the behavioural considerations of users through sophisticated design and the power of defaults. The policy change has led to fines for Facebook and WhatsApp at the Commission and national levels.

The Commission fined Facebook Euro 100 million for providing misleading information about its ability to combine data from WhatsApp, albeit with the caveat that the fine does not concern privacy.[165] Moreover, the Italian Competition and Consumer Protection Authority (AGCD) fined WhatsApp three million Euro for forcing users to accept the sharing of their data with Facebook 'by inducing them to believe that without granting such consent they would not have been able to use the service anymore'.[166] The agency indicated that the design choices, particularly 'the pre-selection of the option to share the data (opt-in)' and 'the difficulty of effectively activating the opt-out option once the Terms' were accepted, prevented users from making effective choices.[167]

WhatsApp's post-merger policy changes and the findings from the AGCD contradict the Commission's assumption that consumers possess the knowledge and ability to react to privacy policy changes and thereby effectively constrain firms' behaviour on privacy. This is strengthened by a recent study that attributed the lack of consumer retaliation to WhatsApp's privacy policy changes to an 'obfuscation and shrouding' strategy that 'allows companies to

[164] See Clemens and Özcany (n 163) 2. Brandimarte, Acquisti, and Loewenstein (n 46) 343-344.
[165] European Commission, 'Mergers: Commission alleges Facebook provided misleading information about WhatsApp takeover (20 Dec. 2016).
[166] Autorità Garante della Concorrenza e del Mercato (AGCM), 'WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook' (12 May 2017)
[167] Ibid.

deliberately limit the visibility of cost', in this case, the cost of sharing users' data with Facebook.[168] One source of weakness in the decision is that the Commission's conclusion was based on replies given by firms, not consumers. However, given that the Commission's conclusion was predicated on the consumer's ability to exert effective constraints on the data collection practices and privacy policy of firms, it should have also taken into account whether actual consumer behaviour supports that assessment.[169]

One could argue that the post-merger measures taken by the AGCD is an indication that other regulatory measures can step in when the competition analysis fails to account for such changes. However, this does not change the shortcomings of analysis in the merger i.e. market evidence does not support the Commission's stance that users can effectively exert competitive constraints on the data privacy practices and privacy policies of firms. Such consideration is particularly crucial where privacy is a key parameter of competition for the merging entities or serves as a competitive constant on the advertising market. Thus, going forward, if competition authorities are to rely on the competitive significance of privacy policies, they should complement their analysis with consumer surveys and research on behavioural economics. This implies that if exercising effective competitive constraints through users' behaviour forms a central element of the competition analysis but the market evidence shows that users are unable to effectively exert such constraints, competition authorities must take necessary measures to mitigate those limitations.

In other words, if the Commission's conclusion that the merger would not lead to concentration in the advertising market or reduction in privacy were solely dependent on the ability of users to constrain WhatsApp from sharing data with Facebook but the market evidence shows the existence of factors that hinder users from exerting such constraint, measures should be taken to prevent such sharing. For example, some of the competition law measures suggested by the Japan Fair Trade Commission (JFTC) include limiting or requiring changes in corporate privacy policies and restrictions on data collection.[170] Such measures are fully in line with some of the market evidences on consumer behaviour in data privacy. Absent that, firms will be able to exploit consumers' cognitive limitations, information asymmetry,

[168] Clemens and Özcany (n 163) 2.
[169] One could argue that the Commission need not conduct such assessment, as it did not accept that the sharing of data would lead to concentration. However, for the sake of future guidance, the Commission could have indicated the need for conducting such an assessment and why it was unnecessary to do so in that particular situation.
[170] Japan Fair Trade Commission, 'Summary Report of Study Group on Data and Competition Policy', (7 June 2017) 2.

confusology and the power of defaults to make decisions that will undermine the competition analysis conducted by the authorities.

The second assumption by the Commission in the merger relates to the incentives of the merging firms to change the privacy policies. According to the Commission, WhatsApp lacked the incentive to change its privacy policies and to start collecting more data because this could 'prompt some users to switch to different consumer communications apps that they [would] perceive as less intrusive.'[171] 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, the change in privacy policy to introduce targeted ads leads to consumers deserting WhatsApp, it does not necessarily make the practice unprofitable. This is because the policy change allows Facebook to use data from WhatsApp for advertising, and the revenue generated from such increased targeting possibility might be superior to the loss of consumers resulting from the change in privacy policy.

Forbes magazine estimated that the change in WhatsApp's privacy policy and its business model – introducing tools that allow users to communicate with businesses could 'yield revenues of around 5 billion US dollars for Facebook in 2020'.[172] To the extent this is valid, the change in privacy policy in order to share data with Facebook can be a profit maximizing strategy. This may be the case even in the face of consumers deserting WhatsApp following the change. Despite such possibility, the Commission only looked at the change of privacy policy as something that is inherently 'unprofitable' without counter balancing the possible gains from the advertising on Facebook. This problem is associated with platform cross-subsidisation where the data collected by WhatsApp is monetized on Facebook. By considering a change of privacy to be an unprofitable strategy, the Commission seems to overlook the interdependence of the business models and the value generated from the data on the advertising market. Thus, any analysis of the competitive constraints in relation to data privacy practices and privacy policy should factor in not only the consumer behaviour but also the incentives of firms in the form of revenues in other markets from changing the privacy policies.

Last but not least, competition analysis should pay sufficient regard to how market power might be exerted by degrading or undermining competition in data privacy and PETs. An initial first step is to identify and discuss how some conduct of dominant players might undermine competition in privacy and PETs. In this regard, the Commission Communication on 'Digital

[171] *Facebook/WhatsApp* (n 17) para 174.
[172] Trefis Team, 'How Much Revenue Can Facebook's WhatsApp Generate in The Next Five Years?', (*Forbes*, 3 March 2016).

Single Market Strategy for Europe' expresses concern over the 'growing market power of some platforms' and underlines that market power in such platforms such as search, social media and e-commerce could be linked to, among others, 'a lack of transparency as to how they use the information they acquire'.[173] This approach would cater to competition in data privacy because it is the cause of the dysfunctional equilibrium discussed above. The lack of transparency means that users are unable to comprehend and make informed decisions, which leads to the problem of credibility and then the vicious circle that affects supply-side. Thus, to the extent that the conduct of a dominant player can be linked to undermine the competition in privacy and PETs, it can be considered as anticompetitive conduct punishable under TFEU Article 102.

There are encouraging developments in this direction. One such development pertains to the emerging discussion that lack of transparency about data collection and unilateral changes to the conditions of processing without providing a meaningful option for users can constitute an abuse of dominance under Article 102.[174] Similarly, in their joint report, the French and German Competition Authorities have indicated that excessive data collection by dominant undertakings could be challenged as exploitative conduct under Article 102 that is comparable to excessive pricing.[175] More importantly, the Bundeskartellamt has looked into the possible abuse of dominant position by Facebook in the market for social networks by imposing unfair privacy terms and conditions.[176] In its preliminary assessment, the Bundeskartellamt found Facebook's data collection practices from third party sources to be unfair in light of 'European data protection principles' and constitute an abuse of dominance under German competition law.[177] According to the authority, Facebook's terms and conditions 'are neither justified under data protection principles nor are they appropriate under competition law standards.'[178]

The investigation is based on a precedent from the German Federal Court of Justice where the incompatibility of contract terms with the laws regulating general conditions and terms are regarded as abuse of dominance under the German competition law.[179] Two points from the investigation require particular mention. First, this is perhaps the first case where harms to data privacy (competition on privacy) are at the centre of a competition law investigation. Some of

[173] European Commission, 'Commission Communication on A Digital Single Market Strategy for Europe, COM(2015) 192 final' 11.
[174] Kerber (n 59) 861. Aleksandra Gebicka and Andreas Heinemann, 'Social Media & Competition Law', *World Competition*, 37/2 (2014) 162.
[175] See Autorite de la Concurrence and Bundeskartellamt (n 158) 24-26. Costa-Cabral and Lynskey (n 22) 35. Also Gebicka and Heinemann (n 174) 163-165. Monopolkomission (n 76) para 326-329.
[176] Bundeskartellamt, 'Background Information on the Facebook Proceeding' (19 December 2017).
[177] Ibid 5.
[178] Ibid 2.
[179] See Autorite de la Concurrence and Bundeskartellamt (n 158) 25.

the consumer harms identified 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'.[180] Secondly, the investigation resorts to data privacy law as a metric for assessing abuse. This is particularly relevant because the lack of a concrete benchmark for measuring degradation in privacy is a key source of scepticism for using competition law to address harms to competition in privacy and PETs.[181] Although the resort to data privacy law seem unprecedented, it is consistent with the precedents from the Commission and EU courts where other legal norms (e.g. IP) provide normative guidance in the application of competition law.[182]

Developments such as the Bundeskartellamt's case against Facebook would help firms internalize the costs related to lack of transparency and excessive data collection. As noted above, considering 'lack of transparency' on data collection and use as an abusive practice could help firms to internalize the externalities that lead to 'dysfunctional equilibrium', particularly the tendencies from newcomers to learn that they are not able to attract sufficient demand by providing clear and privacy friendly policies. Similarly, prosecuting dominant players for excessive data collection can address some of the externalities of accumulation of data by firms to other consumers and society at large.[183].

The Commission's decision in Microsoft/LinkedIn is another step forward in the discussion of competition through privacy and the use of market power to harm such competition. Having already identified data privacy as 'a significant quality' parameter of competition between PSNs, the Commission held that if Microsoft were to pre-install and integrate LinkedIn with Windows OS and Office products, it would reduce consumer choice in relation to privacy.[184] This is because such conduct may lead to the foreclosure of PSN providers such as XING that 'offer a greater degree of privacy protection than LinkedIn'.[185] The decisions clearly recognizes that the choices users have when providing their data and their ability to control its use as key quality attributes of the competition in data privacy and that reduction in data privacy as a quality parameter is not limited to an increase in the amount of data collected. The decision also shows that reductions in the level of privacy could fit easily into existing theory of harms so far

[180] Bundeskartellamt (n 176) 4.
[181] See Esayas (n 19).
[182] Costa-Cabral and Lynskey (n 22) 32.
[183] See Esayas (n 140). Also Esayas (n 19).
[184] *Microsoft /LinkedIn* (n 50).
[185] Ibid para 350.

as competition authorities are cognizant that privacy can be a form of quality (non-price) competition.

This is not to portray that there are no challenges in incorporating data privacy into competition analysis. These challenges relate to users' subjective preferences over privacy, difficulty to measure reductions in privacy, and the potential trade-off between privacy degradation and quality improvements in the underlying services. However, competition authorities have tackled similar challenges on subjectivity and measurement in relation to many non-price parameters including economic efficiency (allocative and dynamic in particular) by resorting to proxies and presumptions. Thus, there is no evidence to suggest that the challenges with data privacy are insurmountable.[186] Additionally, the Microsoft/LinkedIn decision demonstrates that users' control over their data is another parameter of quality and such users' preferences need not be in tension with the preferences of other consumers or other quality improvements. Moreover, the decision shows that it is not always necessary to quantify the reduction in privacy. In this instance, the Commission reached the conclusion by looking at the foreclosing effect of the conduct, i.e. tying, without tackling the thorny issue of measuring quality of privacy.

V.Conclusion

This article has explored the complex relationship between competition, market power and data privacy in 'zero' price markets. The main point is that despite the recognition that market power may be exerted through non-price parameters, including a reduction in the level of data privacy, the proxies for computing market power largely remain price-centric or are unable to capture the data privacy interests of individuals. This is the case even in markets where privacy is considered an important parameter of competition. Accordingly, the article suggests that where privacy is an important parameter of competition and market power is assessed through market share, competition authorities should consider the extent that different proxies cater to the possible risks from data collection and reduction in privacy, which can be a reflection of market power. Similarly, factors that hinder consumers and competitors from responding to reductions in privacy are not adequately accounted for in market power assessments. Thus, competition authorities should consider the behavioural and structural considerations that might hinder consumers and competitors from behaving competitively. In particular, where competition authorities rely on the users' ability to exert competitive constraints on data privacy

[186] The author has addressed some of these scepticisms in another work. See Esayas (n 19).

practices of firms and competitive significance of privacy policies, they should complement their analysis with surveys on consumer behaviour and consider the potential competition through dissimilarity, the incentives of firms, and possible revenues in other markets, from changes in privacy policy.