Data Privacy in European Merger Control: Critical Analysis of Commission Decisions Regarding Privacy as a Non-Price Competition

Samson Y. Esayas*

[Post-print of article published in *European Competition Law Review*, 40(4) (2019) pp. 166-181.]

ABSTRACT

In recent years, privacy has started to attract considerable attention in competition discussions, particularly in mergers involving data-rich industries. Prime examples of such mergers include Google/DoubleClick, Facebook/WhatsApp and the recent acquisition of LinkedIn by Microsoft. Given the central role that personal data plays in these mergers and associated privacy concerns for users, competition authorities have started to experiment with ways to incorporate privacy into merger assessment. One emerging approach is to factor in privacy as a non-price competition parameter. In its merger decisions involving *Facebook/WhatsApp* and subsequently *Microsoft/LinkedIn*, the European Commission held that data privacy constitutes a key parameter of non-price competition in the market for consumer communications and for professional social networks. This article provides a critical analysis of these decisions regarding the competition in privacy and Privacy Enhancing Technologies (PETs). The analysis is conducted from two angles: one looking at the Commission's approach in defining the market, particularly on how competition in privacy and PETs is manifested and when two firms are considered competitors based on these parameters and thereby of interest to competition law. The second angle takes aim at the competitive assessment and the theories of harm, particularly when a merger is considered to lead to reduction in privacy as a non-price competition parameter. The article maintains that the Commission's decision in *Microsoft/LinkedIn* represents a step forward in the discussion of privacy as a non-price (quality) competition parameter and the use of market power to harm such competition.

* 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. However, the usual disclaimer applies.

I. Privacy as a Non-Price Competition Parameter

At its core, competition policy is concerned with a market power that may harm 'consumer welfare'. According to the Commission Guidelines on the abuse of a dominant position, consumer welfare is determined regarding price and other factors, such as product quality, choice and innovation.[1] When a market is effectively competitive, it benefits consumer welfare in the form of lower prices, high quality and a wide range of choices.[2] In contrast, competition is harmed when a transaction or a conduct results in a significant increase in market power, defined as the ability of a firm or group of firms 'to profitably increase prices, reduce output, choice or quality of goods and services, diminish innovation, or otherwise influence parameters of competition'.[3] In this sense, the primary concerns of competition law are related with economic harms arising from price increase, reductions in output, quality, choice or innovation, and privacy considerations are often viewed as outside the realm of competition policy.[4] However, with the growing importance of data for commercial purposes and as a key source of competitive advantage and associated privacy concerns for users, privacy has attracted considerable attention in competition law discussions, particularly when companies in data-rich industries seek a merger or acquisition.[5]

A notable development that reflects the commercial importance of data is the growing number of data-mergers, which according to the OECD have increased significantly over the last few years.[6] Prime examples of such mergers include Google/DoubleClick, Facebook/WhatsApp and the recent acquisition of LinkedIn by Microsoft. Such mergers are partly driven by the desire to acquire and combine new data assets viewed as a key source of competitive advantage in developing and providing digital services.[7] Given the central role that personal data plays in these mergers, the question is whether, and to what extent privacy is a concern in merger assessments involving such data-rich companies.

There are at least two emerging approaches for incorporating data privacy concerns into competition assessments. One approach is based on the argument that data privacy is a fundamental right, and competition law should consider how certain conduct (a merger or

1 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, para 19.

2 See Case C-209/10 *Post Danmark AS v Konkurranceradet* [2012] EU:C:2013:172, para 22.

3 See 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.

4 See Dissenting Statement of Commissioner Pamela Jones Harbour in the Matter of Google/DoubleClick F.T.C. File No. 071-070, noting that '[t]raditional competition analysis fails to capture the interests of all the relevant parties,' particularly 'consumers whose privacy is at stake').

5 For privacy and merger scholarship, see, among others, Richard Pepper and Paul Gilbert, 'Privacy Considerations in European Merger Control: A Square Peg for a Round Hole', *Antitrust Chronicle*, 5 (2015). Eleonora Ocello, Cristina Sjödin, and Anatoly Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case', *European Commission-Competition Merger Brief*, 1 (2015). Allen Grunes and Maurice Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data', *Antitrust Source*, (2015). Darren Tucker, 'The Proper Role of Privacy in Merger Review', *CPI Antitrust Chronicle*, 2 (2015). Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (International Competition Law Series: Kluwer Law International, 2016).

6 OECD, Data-Driven Innovation: Big Data for Growth and Well-Being (Paris: OECD Publishing, 2015) at 94.

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

unilateral conduct) directly affects this right.[8] This approach, initially proposed in a merger case, calls for competition authorities to block mergers that endanger the data protection rights of individuals, unless the merged entity implements adequate privacy safeguards.[9] Given that this approach does not consider purely competition concerns (e.g., price increase, output or quality reduction), it would have to overcome insurmountable challenges to succeed and thus is beyond the remits of this article. Furthermore, both the CJEU and the Commission have clearly indicated that privacy *as such* is beyond the scope of EU competition law.[10]

Another approach, shared both by the European Commission (EC) and the US Federal Trade Commission (FTC), is based on the argument that data privacy is a concern so far as it affects the parameters of competition, that is, reduces privacy protection as a form of quality or deprives consumer choice or diminishes innovation.[11] This approach acknowledges competition law's concern at being limited to competitive issues but posits that privacy should form a competition dimension.[12] The need to factor in privacy as a competition dimension is particularly important in light of the ubiquity of services offered at 'zero' price and in exchange for personal data, which necessitates a change in approach. This is because price is often viewed as the chief competition parameter partly because quality can be factored into the price, meaning that price considerations will also cater to quality aspects (quality-adjusted price). However, the reliance on price to factor in quality or other parameters starts to break down when the product/service is offered for 'free', as is the case with the most popular digital service, such as Facebook and Google search. For example, in the *Microsoft/Yahoo!* merger, the Commission indicated that when a product is free, quality becomes an essential and significant competition parameter.[13] Moreover, increasingly consumers are exchanging their personal data to access such services, which means that consumers are effectively paying for these services through their personal data.

In such cases, given that the collection and use of personal data is associated with data privacy concerns, one alternative is to consider the personal data collected by such entities as either the price paid by the user in return for receiving the 'free' product or as a dimension of

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

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

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

11 See Peter Swire, 'Submitted Testimony to the Federal Trade Commission Behavioural Advertising Town Hall on Google/DoubleClick', (2007). Pamela Harbour and Tara Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets', *Antitrust Law Journal*, 76 (2010). See also 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).

12 A third line of argument links the accumulation of too much information with the potential to foster first-degree price discrimination, which could be captured by competition law. See Maurice Stucke and Allen Grunes, *Big Data and Competition Poli*cy (OUP, 2016). Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer law and Data Protection', *Journal of Intellectual Property Law & Practice*, 11/11 (2016).

13 *Microsoft/Yahoo! Search Business*, para 101.

product quality.[14] As a result, privacy is attracting a considerable attention as a non-price (quality) parameter among regulatory authorities in the EU and the US.

In the Google/DoubleClick merger, the FTC acknowledged that mergers can 'adversely affect non-price attributes of competition, such as consumer privacy'.[15] In a thought provoking dissenting opinion to the FTC's decision in *Google/DoubleClick* and a subsequent co-authored law journal article, then Commissioner Pamela Harbour insisted on defining 'privacy related markets' when companies that control massive personal data seek to merge.[16] Noting that the conventional analysis overlooks the privacy interests in data-mergers, Harbour argued, defining 'a privacy-based relevant product market' provides the hook to make privacy 'cognizable' under competition law.[17] This allows competition authorities to consider whether a merger changes the incentives to compete on privacy and deployment of Privacy Enhancing Technologies (PETs).[18]

In the EU, relevant decisions articulating privacy as a non-price competition parameter are the *Facebook/WhatsApp* and *Microsoft/LinkedIn* mergers. In the *Facebook/WhatsApp* merger, the Commission stated that in markets for consumer communications,[19] privacy and data security constitute key parameters of competition.[20] The Commission justified the need for recognizing data privacy as a competition parameter because privacy and security are 'becoming increasingly valued' by consumers.[21] In the most recent decision involving *Microsoft/LinkedIn*, the Commission further affirmed this stance, claiming that privacy 'can be taken into account in the competition assessment to the extent that consumers see it as *a significant factor of quality*' and indicating that 'data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction'.[22]

Despite the emerging consensus on accounting privacy as a non-price competition parameter, there are questions on how the competition in privacy and PETs is manifested. More particularly, when are two firms considered competitors based on these parameters and thereby of interest to competition law? Moreover, there is much uncertainty on how to operationalize such an approach through concrete theory of harm, particularly what constitutes reduction in privacy and when a merger is considered to reduce this competition.[23] This article seeks to

14 Ocello, Sjödin, and Subočs (n 5) 6. However, this does not necessarily mean that privacy is not relevant for paid services. This is consistent with the Commission finding that loss of 'confidentiality' could be considered product degradation even for services where money changes hands. See Case M 4854 *TomTom/Telia Atlas* decision of 14 May 2008, para 272-275.

15 Statement of Federal Trade Commission Concerning Google/DoubleClick FTC File No. 071-0170, 2.

16 Dissenting Statement of Commissioner Pamela Jones Harbour (n 4) 10. See also Harbour and Koslov (n 11).

17 Dissenting Statement of Commissioner Pamela Jones Harbour (n 4) 10.

18 Harbour and Koslov (n 11) 794.

19 In that decision, the Commission analysed three markets, namely, consumer communications services, social networking services and online advertising services. See *Facebook/WhatsApp*, para 34, 62 and 79.

20 Ibid. para 87.

21 Ibid.

22 European Commission - Press release, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions', (IP/16/4284, 6 Dec 2016). Also Case M 8124 *Microsoft /LinkedIn* decision of 6 Dec 2016.

23 Geoffrey Manne and Ben Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework', *Antitrust Chronicle*, 2 (2015) at 3 (noting that 'privacy advocates have failed to prove a product quality case'). See also James Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity', *Geo. Mason L. Rev*, 20/4 (2013) 1135.

examine these questions in light of the Commission's decisions in *Facebook/WhatsApp* and *Microsoft/LinkedIn*. The decisions are examined in light of the Commission's view on how the competition in privacy is manifested and how a merger might reduce privacy as a competition parameter. The analysis shows that the Commission has improved on several fronts in its *Microsoft/LinkedIn* decision that were sources of critics in relation to the *Facebook/WhatsApp* decision regarding the competition in privacy.

II. Market Definition and Competition in (Data) Privacy

Defining the relevant market is an essential first step for competition law enforcement in many jurisdictions, including the EU and the US.[24] The definition of the relevant market aims at identifying the competitive constraints imposed on a firm's behaviour to increase price or reduce output or quality. This is conducted by identifying actual and potential competitors that offer goods or services that are perceived by consumers as substitutes having regard to their intended uses, prices and characteristics.[25] Thus, under the conventional competition law, similar products or services are considered to exert more competitive constraints on each other than dissimilar products or services. This approach seems to apply to the competition in privacy. For example, Tucker argues that privacy considerations are 'cognizable' in mergers only where 'the merging firms are significant rivals due to their competition on privacy; and a large share of customers regard the merging parties as offering the best products as a result of their approaches to privacy.'[26] This implies that when entities exhibit significant differences in their value to privacy and how they handle personal data, they are not considered to be competitors. This seems to be the approach adopted by the EC in the *Facebook/WhatsApp* merger.

Despite recognizing data 'privacy and security' as key competition parameters, the Commission used the differences in privacy policies as a factor that makes WhatsApp and Facebook Messenger complementary services rather than competitors. In reaching this conclusion, the Commission mentioned the differences relating, among others, to 'the privacy policy (contrary to WhatsApp, Facebook Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities).'[27] The Commission further added that the 'only factors on the basis of which WhatsApp and Facebook Messenger were considered close competitors by certain respondents are the *communications functionalities* offered and *the size of their respective networks.*'[28] The Commission's stance seems based on the understanding that firms with identical privacy policies compete more fiercely than firms with dissimilar privacy policies. However, this is only partially true.[29]

24 See Richard Whish and David Bailey, *Competition Law* (Oxford University Press, 2015) 27.
25 COMMISSION NOTICE on the definition of relevant market for the purposes of Community competition law OJ C 372/5 [1997], para 7.
26 Tucker (n 5) 5.
27 *Facebook/WhatsApp*, para 102.
28 Ibid. para 103, and 172. See also footnotes. Even with regard to the communications functionalities, the Commission indicated that 'WhatsApp is not the closest competitor to Facebook Messenger (let alone to Facebook's social networking site).'
29 I do not dispute the claim that a merger of firms that draw customers due to their superior privacy can lead to reduced competition, particularly if the market for such services is already concentrated. But in today's market reality dominated by business models that heavily relay on collecting and analysis massive amount of personal data, a merger between two privacy friendly services could be positive for privacy because the merged firm could

Having the benefit of the post-merger behaviour of WhatsApp to change its privacy policies,[30] the Commission's approach could be critiqued from two angles.[31] Firstly, when it comes to privacy, dissimilarity either in the technology or policy can be just the beginning of a competition that exerts competitive pressure on others, rather than make the firms complementary. In the context of the merger, this implies that the Commission might have underestimated the competitive constraints that WhatsApp, by opting for a different privacy policy and luring users from Facebook, imposes on Facebook to compete on privacy technology and privacy policies. Related with this, given that WhatsApp was trying to induce users of Facebook social network to use its messaging service by offering superior privacy, despite the dissimilarity in privacy policy, Facebook, as an established network, imposes competitive constraints on WhatsApp's behaviour on privacy policy, which might be overlooked by the Commission. Secondly, although firms with similar privacy policies can impose competitive constraints on each other's behaviour regarding privacy, the strength of such constraint largely depends on the size of the networks. In this regard, the Commission might have overestimated the competitive constraints on WhatsApp's privacy policies that arise from messaging services with similar privacy policies but smaller size networks.

A. Competition in Dissimilarity

The dissimilarity in their privacy policies is one reason behind the Commission's treatment of WhatsApp and Facebook Messenger as complementary services rather than competitors. The question is: if privacy is a competition parameter, isn't dissimilarity in privacy policy one way where such competition could be manifested? From an economic standpoint, privacy remains a competitive dimension regardless of whether the specific entity provides little or more of it.[32] Whether the entities concerned collect massive amounts of consumer data or little data, they all try to assure consumers that they, consumers, are in control of their data and that the data is secure, which shows that competition, *albeit* to different degrees, exists among entities that deal with consumer information. In other words, if privacy and data security are competition parameters, one way this competition can be manifested is through deploying privacy enhancing technology (e.g. instant deletion of data, end-to-end encryption) and privacy policies (offering better conditions of data collection and processing). If so, competition in privacy and privacy policy is more sequential than simultaneous, meaning that it can occur through dissimilarity where the adoption of a certain technology, policy or a change thereof by an entity, if found attractive by consumers for offering better privacy, drives others to follow suit. There is some evidence showing that companies react to each other's behaviour on privacy policy.[33]

For example, between 2007 and 2010, Google, Yahoo and Microsoft responded to each other's changes on privacy policy in shortening the retention period for the data they collect.[34]

benefit from network effects and be able to impose better competitive constraints on the established firms' privacy conditions.

30 Despite making public promises not change its privacy policy post-merge, in August 2016, WhatsApp announced that it will start to share user information with Facebook and some entities. See WhatsApp Blog, 'Looking ahead for WhatsApp' (WhatsApp, 25 August 2016).

31 Part of this text is adopted from Samson Esayas, 'Competition in Dissimilarity: Lessons in Privacy from the Facebook/WhatsApp Merger' *CPI Antitrust Chronicle*, 1/2 (2017).

32 Stucke & Grunes, (n 12) 131.

33 Harbour and Koslov (n 11) 793-794.

34 Ibid, 793.

Back in 2007, Google announced its policy to anonymize users search queries after 18-24 months, which includes personally identifiable information such as log files and IP addresses,[35] as a 'step to further improve …[its] privacy practices.'[36] In September 2008, Google took 'Another step to protect user privacy' by cutting its retention period from 18 to nine months.[37] This competition further culminated when Yahoo! adopted three-month policy in Dec 2008.[38] Microsoft followed suit in adopting a six-month policy in January 2010.[39] In this sense, privacy policies are subject to constant change and the dissimilarity in privacy policy can be just the beginning of a competition that exerts competitive pressure on others to follow suit, rather than make the firms complementary.

In addition, competition in privacy could occur in the form of developing or deploying underlying technologies used to protect privacy such as encryption i.e. competition in innovation.[40] As noted by the Commission, unlike Facebook, WhatsApp provides an end-to-end encryption of messages and does not store consumers' information on its servers. This privacy protective feature together with the growing popularity of WhatsApp could be seen to impose a competitive pressure on Facebook to follow suit. Commenting on a similar subject, former FTC Commissioner Harbour and her legal advisor Koslov argued as follows:

> Absent pressure from competitors [*such as WhatsApp*] who might provide more attractive alternatives to privacy-prioritizing consumers, a dominant firm [*such as Facebook*] might rationally choose to innovate less vigorously around privacy or, perhaps, to dole out privacy-protective technologies to the marketplace more slowly.[41]

In this sense, WhatsApp could be seen to impose competitive constraints on Facebook to try to compete on privacy enhancing technologies, and thus is not merely complementary to Facebook. In fact, in a move that imitated WhatsApp, Facebook introduced an end-to-end encryption, *albeit* with a limited functionality, to its Messenger service. The main objective for such a change, according to Facebook's vice president of messaging products, is 'to make Messenger your primary messaging platform…'[42] Although this fact could be taken to argue that the merger did not reduce Facebook's incentive to compete on privacy enhancing technologies, it demonstrates that, even after the merger, Facebook still competes with WhatsApp to become the primary messaging platform by offering similar data security levels offered by other platforms such as WhatsApp. Moreover, it is questionable that Facebook would

35 According to Article 29 Working Party, log files are 'the most important personal data that are processed by the search engine providers.' The data consists of data describing the usage of the search service including: 'the query logs (content of the search queries, the date and time, source (IP address and cookie), the preferences of the user, and data relating to the user's computer); data on the content offered (links and advertisements as a result of each query); and data on the subsequent user navigation (clicks)'. See Article 29 Data Protection Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP148) (2008) 6.

36 Google Blog, 'Taking Steps to Further Improve Our Privacy Practices' (14 March 2007). https://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html

37 Google Blog, 'Another Step to Protect User Privacy' (8 Sep 2008).

38 Kim Dixon, 'Yahoo Cuts Data Retention to Three Months', (*REUTERS*, 17 Dec 2008).

39 See Bing Blogs, 'Updates to Bing Privacy' (19 Jan 2010) https://blogs.bing.com/search/2010/01/19/updates-to-bing-privacy-2

40 Harbour and Koslov (n 11) 793.

41 Ibid, 795 [addition mine].

42 Kate Conger, 'Facebook Messenger adds end-to-end encryption in a bid to become your primary messaging app' (*TechCrunch*, July 8, 2016).

compete as vigorously if WhatsApp had remained a separate entity. Facebook being in charge of matters now; it can effectively neutralize WhatsApp's vigour and innovation in privacy enhancing technology and offering better data privacy conditions.[43] The change in WhatsApp's privacy policy to share data with Facebook family companies is perhaps a testimony to such reduced vigour to compete on privacy and privacy policies. More importantly, Facebook's introduction of end-to-end encryption shows that competition in privacy enhancing technology can be manifested sequentially where the adoption of the technology by an entity, if found attractive by consumers for offering better privacy, drives others to follow suit. Thus, when it comes to privacy and privacy policies, dissimilarity either in the technology or policy can be just the beginning of a competition that exerts competitive pressure on others, rather than make the firms complementary. In the context of the merger, this implies that the Commission might have underestimated the competitive constraints that WhatsApp, by opting for a different privacy policy and luring users from Facebook, imposes on Facebook to compete on privacy technology and privacy policies.

Part of the problem with the Commission's analysis can be attributed to a lack of framework for identifying the relevant dimensions of competition in data privacy and PETs. For example, a look at one of the core data protection principles, i.e. data minimisation, as one relevant dimension of competition in privacy could have helped to better understand how such competition is manifested. In other words, by not collecting data or collecting the minimum necessary, one could view WhatsApp as trying to appeal to users of Facebook Messenger that value their privacy, which means that the differences in their privacy policies on data collection is in fact a manifestation of the competition through this dimension. Thus, having a framework for identifying the relevant dimensions of privacy competition can help competition authorities to easily detect how such competition is manifested. In this regard, data protection norms could be informative in highlighting the attributes of data privacy relevant for competition.[44]

For example, while firms compete by lowering prices, the competition in privacy and PETs occurs by increasing the level of privacy, which may include (1) not collecting or reducing the amount of personal collected to provide the service (data minimisation);[45] (2) not storing personal data or attaching shorter timestamps (storage limitation)[46]; (3) providing clear, precise and understandable privacy policies (transparency);[47] (4) deploying PETs e.g. end-to-end encryption, and pseudonymisation (data security and privacy by design);[48] (5) implementing privacy protective features by default (privacy by default).[49] This implies that analysis of

43 Costa-Cabral and Lynskey (n 9) 38.

44 This is consistent with the calls from the EDPS to establish a 'digital clearinghouse' that brings competition, consumer and data protection authorities together and develop guidelines for considering privacy issues in competition cases that reflect principles of data protection. See 'Opinion 8/2016: EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data ' (2016).

45 Derived from the data minimization and sensitivity principles. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data OJ L119/1 (GDPR), Art 5(1(c)) and Art 9.

46 Derived from the purpose limitation and storage limitation principles. See GDPR, Art 5(1(b)) and Art 5(1(e)).

47 Derived from the transparency principle and the rule on information provision. GDPR, Art 5(1(a)) and Art 12-14.

48 Derived from the data security principle. GDPR, Art 5(1(f)). Derived from the data security and the privacy by design principles. GDPR, Art 5(1(e)) and Art 25(1).

49 Derived from the provision on privacy by default. GDPR, Art 25(2).

privacy as a non-price component needs to focus on the incentives and the impact of a conduct to reduce these attributes.[50]

Although not exhaustive, the above list of attributes could provide a baseline framework that could help detect the competition in data privacy and PETs. A look at the privacy policy of the Internet search engine DuckDuckGo illustrates how these dimensions can help identify this competition. For example, its privacy policy states that DuckDuckGo 'does not collect or share personal data' and by so doing DuckDuckGo is trying to compete based on the data minimization and purpose limitation principles as the relevant dimensions. DuckDuckGo's privacy policy also states that it 'does not store personal data' where the relevant dimension of competition is the storage limitation principle. The search engine also undertakes to highlight policy changes in 'red text', which manifests a competition through the transparency principle and informed consent. Moreover, when conducting search, users' location is turned-off by default, which in turn manifests the privacy by default dimension as a competitive parameter. In this sense, the differences in privacy policy with Google would be a sign that DuckDuckGo is trying to compete based on privacy and PETs than making these two services complementary.

Indeed, the Commission seems to have shown a change of heart in its *Microsoft/LinkedIn* decision where the differences in privacy policy between XING and LinkedIn was taken as a sign of competition in privacy.[51] In analysing how the merger might affect the competition in privacy, the Commission referred to the differences in the privacy policies of XING and LinkedIn during registration process, when introducing new features that have implications on how users data is collected and used and users ability to continue to use the services without losing any of the functions to which they previously had access.[52] Of particular importance in light of the Commission decision in *Facebook/WhatsApp* is that the Commission did not consider the differences in data privacy practices as a factor that makes XING and LinkedIn non-competing services. Instead, the Commission held that XING's greater level of privacy, as manifested in its different privacy policy and data handling practices vis-à-vis LinkedIn, is what makes it an important competitor in the market for PSNs.

Another source of critique to the Commission's stance in *Facebook/WhatsApp* relates to the competitive constraints that Facebook, as an established network, imposes on WhatsApp privacy policy. If privacy is an important parameter of competition for a firm, which was the case with WhatsApp, the existence of an established network such as Facebook with a different privacy policy can still discipline the former's behaviour on privacy. This is particularly the case if the firm that offers increased privacy is using that feature to displace or lure users of the incumbent network. In such cases, the existence of the incumbent network (however different its privacy policy might be) can serve as a competitive constraint because any change that reduces the privacy features could lead to losing the competitive edge over the incumbent.

As the Commission itself pointed out, 80-90 percent of WhatsApp users were users of Facebook's social network and 'were therefore already within the reach of Facebook

50 See Samson Esayas 'Competition in (Data) Privacy: 'Zero' Price Markets, Market Power and the Role of Competition Law' *International Data Privacy Law* 8(3) 2018) 181-99.
51 *Microsoft /LinkedIn*, para 437-438.
52 Ibid.

Messenger.'[53] The Commission further noted that because of its integration with the core aspects of Facebook's social network, the user experience in Facebook Messenger is far richer than WhatsApp.[54] Moreover, at the time of the merger, WhatsApp users in many countries were paying a subscription fee of USD 1 while they can use Facebook Messenger free of monetary price.[55] This means that all other things being equal, one would expect Facebook Messenger to be more attractive for users than WhatsApp. However, as was indicated by the Commission, WhatsApp had more users (approximately 600 million worldwide) than Facebook Messenger (approximately 250-350 million).[56] Then the question is why WhatsApp was more attractive to Facebook's social network users than Facebook Messenger?

Needless to say, that the restrictive data collection practice is one of WhatsApp's key competitive advantages over Facebook Messenger. As indicated by the Commission, contrary to Facebook, WhatsApp only stores limited information about its users (namely, user name, picture, status message, phone number and the phone numbers in the user's phone book) and does not offer targeted advertisement. By contrast, Facebook collects information about users including but not limited to their real names, gender, birthdate, birthplace, religion, political affiliations, "likes" and social media contacts. Facebook also tracks users browsing behaviour through millions of websites that have Facebook plugins such as "like" and "share." Furthermore, using the data, Facebook offers targeted advertisement and shares the information with third parties. All in all, WhatsApp presented itself as a clear alternative to Facebook on how it handles user privacy and data by offering users an ad-free experience and superior privacy protection at nominal yearly subscription fee.[57] Arguably, this is the key feature that led to WhatsApp acquiring 600 million users even in a shorter time than Facebook itself managed.[58]

In this sense, it is fair to say that the existence of Facebook as the more established and leading communication service provider has, to some extent, imposed competitive constraints on WhatsApp's privacy policy, which is its key disruptive element to gain popularity. This is because in order to remain competitive with Facebook (to keep Facebook's social network users using WhatsApp's messaging service), WhatsApp had to offer something that Facebook did not. Because if WhatsApp had to start collecting personal data, its unique feature that attracted users of Facebook's social network would disappear and its customers might spend less time

53 *Facebook/WhatsApp*, para 105 and 70-80.
54 Ibid. para 104.
55 At the time, WhatsApp charged an annual subscription fee in Italy, the UK, Canada and the U.S. and up until first half of 2014 in Germany and Spain. See ibid. para 90-91.
56 Ibid. para 84.
57 The ideology behind the services also sits in clear contrast. Following the announcement of the acquisition, WhatsApp cofounder Jan Koum stated that '*Respect for your privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about you as possible*'. See WhatsApp Blog, 'Setting the Record Straight' (March 17, 2014) available at (link). Conversely, Facebook founder, Mark Zuckerberg remarked that '*privacy is no longer a social norm*.' According to him, 'people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people.' See Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' (*The Guardian*, 11 January 2010).
58 See Zarsky, 'The privacy-innovation conundrum', *Lewis & Clark Law Review*, 19/1 (2015), 167 (noting that the privacy sentiment is WhatsApp's main draw to its popularity).

using its services and more time on other services, including Facebook Messenger.[59] This is more so given Facebook Messenger's richer functionality. In other words, as a late follower, WhatsApp had to offer something to lure Facebook users and it used privacy as a draw to Facebook users.[60]

By so doing, WhatsApp has managed to attract the majority of its users (80-90 percent) from Facebook. Thus, WhatsApp's competitive concern, if it were to change its privacy policy and data handling practices, would not only be that it would lose its users to messaging service with similar privacy policies, which might not happen because of the size of the networks, but also (and more likely) that it might lose its competitive edge over Facebook. This implies that when a service attempts to draw users from an established network by offering superior privacy, the existence of an established network such as Facebook, *albeit* with a different privacy policy, can still discipline the former's behaviour. Thus, despite the dissimilarity, Facebook, as an established network, imposes competitive constraints on WhatsApp's behaviour on privacy policy, which might have been overlooked by the Commission.

None of these arguments should imply that the Commission would have reached at a different conclusion had it factored in the above arguments, rather the aim is to highlight some lessons that can be taken on board for future similar decisions. Although, in the absence of empirical evidence, it is difficult to attribute WhatsApp's change in privacy policy directly to the merger, one possible explanation for WhatsApp's post-merger behaviour to degrade privacy – by changing it privacy policy to share data with Facebook and also collect data from other Facebook family of companies – could well be due to the merger lifting the competitive constrain that Facebook placed on WhatsApp. This is because the merged entity can recapture some of the consumer loss due to the privacy degradation to WhatsApp through an increase in usage of Facebook Messenger.[61]

B. Similarity in Privacy Policy Not Substitutability

The above critic relates to the Commission's approach in overlooking the possible competition from dissimilarity. However, the Commission's approach could be equally critiqued for overestimating the competition that arises from services with similar privacy policies but smaller size networks. As briefly noted above, in investigating whether WhatsApp could introduce targeted advertisement, the Commission concluded that data privacy concerns would constrain WhatsApp from doing so because WhatsApp has to change its privacy policy and start collecting more data from users.[62] According to the Commission, the introduction of advertisements in WhatsApp could lead to its users switching to ad free services.[63] Moreover,

59 See Keith Waehrer, 'Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions', (available at SSRN https://ssrn.com/abstract=2701927, 2015), 13 (arguing that if services compete in quality, such as privacy, 'the implication is that for any service an increase in its own quality level (all else equal) increases user demand for the service').

60 Stucke & Grunes (n 12) 132 (indicating that 'Facebook sought users who spend more time on its texting app Messenger than WhatsApp. WhatsApp, to induce Facebook social network users to switch from messenger, offered greater privacy protections.')

61 Waehrer (n 59)14 (noting that services competing in quality can, post-merger, reduce the quality if 'a decrease in quality by service 1 results in the merged firm recapturing some of the customers lost to service 1 through an increase in usage of service 2').

62 *Facebook/WhatsApp*, para 174.

63 Ibid.

the Commission indicated that the introduction of ads might lead to abandoning the end-end encryption in WhatsApp, which might create dissatisfaction among users that value their privacy.[64] In this regard, the Commission referred to a submission showing that, following the announcement of the acquisition by Facebook, many German WhatsApp users have downloaded alternative messaging services such as Threema and Telegram.[65] Threema advertises itself as a service designed 'to protect the users' privacy – an app that stores as little as possible and prevents surveillance and data misuse.'[66] Similarly, as indicated by the Commission, Telegram offers increased privacy protection such as end-to-end encryption, and an ad-free experience.[67]

To a certain extent, this shows that the Commission did investigate the potential degradation in privacy conditions in WhatsApp and the alternative messaging services for users in case that happens. However, the assessment remains incomplete.

On the one hand, the Commission focused on messaging services that have similar privacy policies but with little or no regard to their sizes. The fact that Threema and Telegram offer similar privacy protections does not necessarily mean that they can adequately constrain WhatsApp's post-merger behaviour on privacy policy. When people make decisions about joining a messaging app, their primary criteria is whether they can reach their family, friends and acquaintances rather than just privacy policy.[68] Thus, the size of the networks is crucial. This means whether Telegram or Threema can constrain WhatsApp's behaviour on privacy policy depends not only by their privacy policy but also their size. The Commission identified that size as a key utility in communications services. According to the Commission, 'the size of the user base and the number of a user's friends/relatives on the same consumer communications app is of important or critical value to customers of consumer communications apps.'[69] In this regard, the Commission noted that WhatsApp and Facebook were, at the time, the number one and number two messaging service providers with a respective user base of 600 million and close to 250-350 million worldwide.[70] By contrast, at the time of the merger, Threema had only 400,000 users and was mainly available in Germany whereas, according to TechCrunch, Telegram had around 50 million monthly active users.[71] Thus, despite recognising the importance, the Commission did not adequately factor in network size in its assessment and might have overestimated the competitive constraints that services such as Threema and Telegram might impose on WhatsApp's privacy policy.

Even assuming that these services are substitutes regardless of their size, the Commission's assessment remains limited. This is because the switch by some German WhatsApp users to these services alone does not provide sufficient indication that these services

64 Ibid.
65 Ibid.
66 Threema Press Release, 'Threema: The Best Selling Secure Messenger' (Threema Press-Info, 22 Dec 2015) available at (link).
67 *Facebook/WhatsApp*, para 116 and footnote 79.
68 Stucke & Grunes (n 12) 132.
69 *Facebook/WhatsApp*, para 129.
70 Ibid para 128.
71 See Mike Butcher, 'Telegram Claims 50M Monthly Active Users, Seems To Be Attracting Teams' (*TechCrunch*, 8 Dec 2014).

offer alternatives for privacy sensitive consumers. In assessing substitutability of two products where money changes hands, the test is not only whether an increase in price leads consumers switching to substitutes but also whether such switch makes the price increase unprofitable.[72] Although the absence of monetary price in the case makes it difficult to replicate this test, the lack of a comparable criterion could lead to an overly broad market. The assessment gets even more complicated because even if the change in privacy policy to introduce targeted ads leads to consumers deserting WhatsApp, it does not necessarily entail loss of revenue or is unprofitable. This is because the revenue generated from the advertisement, on Facebook using WhatsApp's data for example, might be superior to the loss of consumer resulting from the change of privacy policy. Despite this, the Commission only looked at the change of privacy policy as something that is inherently 'unprofitable' to WhatsApp. To some extent, this emanates from the lack of a minimum threshold relevant for determining when the loss of consumers from a service provided at 'zero' price becomes unprofitable and constrains the firm's behaviour.

The approach adopted by the Chinese Supreme Court in *Qhioo v. Tencent* could shed some light on this issue. In that case, the Court analysed whether non-integrated Instant Messaging ("IM"), similar to WhatsApp, can be considered to be substitutable Integrated IM service. The Court established what is referred to as the 'majority and important rule.'[73] This concept underlines that in defining the relevant market through demand substitution, the analysis need to be made whether there are 'adequate users who would regard a specific good as an alternative…based on the core demand of *majority* users and from the perspective of the key attributes of goods.'[74] More specifically, the Court underlined that in assessing the substitutability of products offered at "zero" price, one has to ask whether a 'majority' of users regard a certain product as a close substitute to the target product.[75] In these cases, the Court relied on statistical data to rule on the substitutability of Integrated and Non-Integrated IM services.[76] In the *Facebook/WhatsApp* merger, the Commission should have asked a similar question, i.e. whether, given their sizes and their privacy policies, an adequate number of users consider Telegram and Threema as close substitutes with WhatsApp.

Absent some threshold to assess unprofitability, the competitive constraints imposed by such networks could easily be overestimated. Perhaps another possible explanation for WhatsApp's post-merger behaviour to change its privacy policy and share consumer data with Facebook could be that the merged entity would not lose enough customers to messaging apps with superior privacy such as Threema and Telegram due to their sizes. The other possible explanation, which was noted above, is that the loss of customers to WhatsApp is compensated by increase in usage of Facebook Messenger. Or a combination of both.

Overall, the main point is that although services with similar privacy policies impose competitive constrains, given the size of its user base, Facebook imposes equally important, if

72 The price increase is unprofitable if the marginal profit from the price increase does not make up the loss sustained due to customers deserting to substitutes.
73 Huang Wei, 'Relevant Market Definition and Market Dominance Identification in 3Q War', *Competition Pol'y Int'l*, 11 (2015), 66.
74 Ibid.
75 Ibid.
76 Ibid 67.

not more important, competitive constrains on WhatsApp privacy policies. Similarly, by opting for a different privacy policy and luring users from Facebook, WhatsApp imposes constraints on Facebook to compete on privacy technology and privacy policies. Thus, in future mergers, the Commission should focus on the competitive constrains that entities impose on each other through providing more attractive alternatives to privacy-prioritizing consumers, and through the size of the networks. Alternatively, as proposed by Evans, when services are provided for free, the proposed relevant markets would need to also include complementary products.[77]

III. Theories of Harm and the Competitive Assessment

Underlying the recognition of privacy as a non-price parameter is the idea that privacy could be subject to competition as an element of quality, choice or innovation and a merger or unilateral conduct can reduce the incentives to compete based on these parameters. Despite the emerging consensus on how to incorporate privacy into a competition analysis, little attention has been paid in laying out a concrete theory of harm that outlines what constitutes reduction in privacy.[78] For example, although the FTC decision indicated that it 'has investigated the possibility that this transaction could adversely affect consumers privacy',[79] it offers little help regarding when and how a merger could be considered to reduce the level of data privacy. Until recently, the European Commission has also glossed over this task of outlining clear theory of harm, particularly in its *Facebook/WhatsApp* decision, although this seems to have been improved in the *Microsoft/LinkedIn* decision.

A. Facebook/WhatsApp

In *Facebook/WhatsApp*, although the Commission identified privacy as a key parameter of competition in the market for consumer communications,[80] it did not specifically assess how the merger might impact this competition parameter. However, the Commission did examine how a reduction in privacy might serve as a constraint on the merged entity's incentive to introduce targeted advertisements in WhatsApp.[81] According to the Commission, for WhatsApp to introduce targeted ads, it had to change its privacy policy and start collecting more data (age, gender, country and message content) from its users.[82] In so doing, the Commission did highlight, although implicitly, that demanding more data to introduce targeted ads could constitute a reduction in privacy provided it results from reduced competition.[83] Moreover, the Commission stated that the introduction of ads in WhatsApp might lead to abandoning the end-to-end encryption and create dissatisfaction among users who value their privacy.[84] In this

77 David Evans, 'Antitrust Economics of Free', *Competition Policy International*, Spring, (2011), 21.
78 For a general overview of the different theories of harm in relation to privacy, see Samson Esayas, Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers' *University of Oslo Faculty of Law Research Paper No. 2018-26* https://ssrn.com/abstract=3232701
79 *Google/DoubleClick FTC File*, (n 15) 2-3.
80 *Facebook/WhatsApp*, para 87.
81 Ibid para 174.
82 Ibid para 174 and 186.
83 See also Ocello, Sjödin, and Subočs (n 5) 6 (arguing to that a reduction in data privacy could be understood to involve an increase in the amount of personal data demanded or expansion in the usage of existing data for purposes other than initially promised). However, the Commission also noted that privacy concerns arising from mere combination of data fall outside of competition law. See *Facebook/WhatsApp*, para 164.
84 *Facebook/WhatsApp*, para 174.

sense, the Commission seems to address, *albeit* indirectly, two possible reductions in data privacy, one based on increase in data collection and another based on abandoning end-to-end encryption.[85]

This notwithstanding, the Commission held that WhatsApp is unlikely to change its privacy policy to collect more data and to abandon its end-to end encryption because this would create dissatisfaction among users who value their privacy and prompt WhatsApp users to switch to other texting apps that are 'less intrusive' and ad free.[86] This analysis of competitive constraints is predicated on two assumptions that are untenable given the consumer behaviour and the incentives of firms for collecting more data.[87]

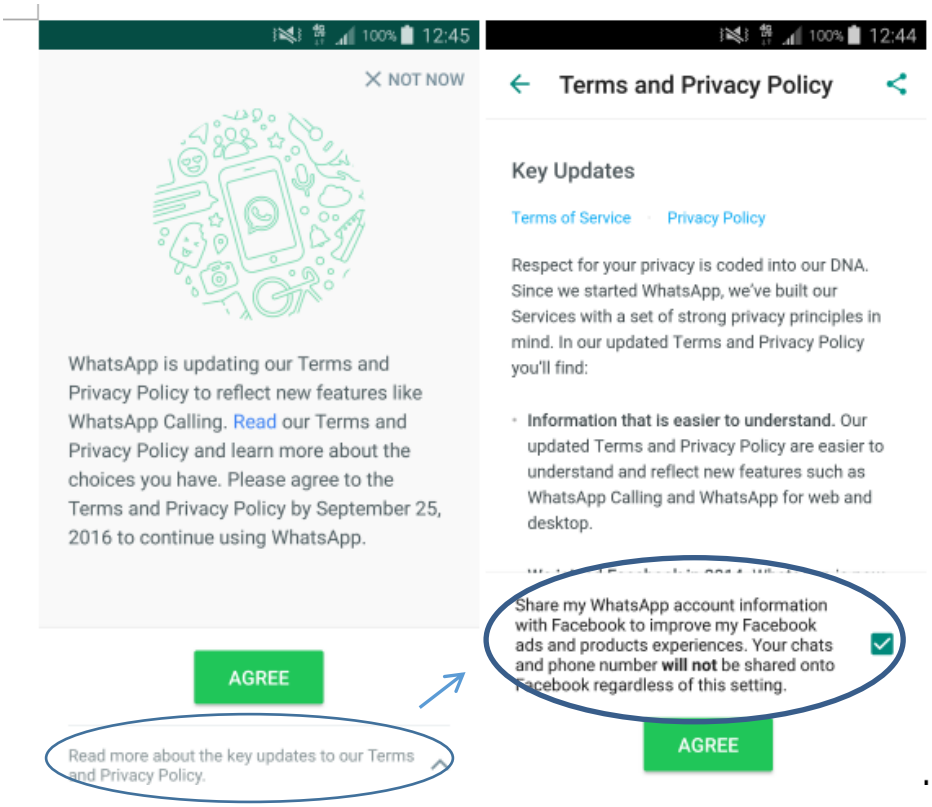
The first assumption is that users are able to impose effective competitive constraints on firm's data collection practices and privacy policies. However, the post-merger behaviour of WhatsApp to change the privacy policy without any adverse consequences demonstrates that the Commission's assumptions had been based on shaky foundations. Two years after the merger, despite public promises to the contrary, WhatsApp changed its privacy policy to the effect that data generated by WhatsApp will be shared with Facebook and other members of the Facebook family of companies with a view to improving the service by, for example, allowing Facebook to display more relevant ads on WhatsApp users' Facebook accounts.[88] Although there were some consumer uproars following the change,[89] unlike the Commission's prediction for users to punish such behaviour by WhatsApp, such change seems to have no or little impact on WhatsApp.[90] Even after such 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, in 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 relates to behavioural considerations that limit users' ability to discipline firms for their data privacy practices. 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. Although there are rules, at least in the EU context, which 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, [91] users hardly read those policies.[92] Even when they do, the policies

85 See Esayas (n 78) (discussing how the subsequent changes in WhatsApp's privacy policy could be, in retrospect, considered to reduce privacy by extending the usage of existing data for purposes other than initially promised).
86. *Facebook/WhatsApp*, para 174
87 Part of this text is adopted from Esayas, 'Competition in (Data) Privacy' (n 50).
88 See WhatsApp Blog, 'Looking ahead for WhatsApp' (WhatsApp, 25 August 2016). See also WhatsApp Privacy Policy, available at https://www.whatsapp.com/legal.
89 See informal survey in Complaint, Request for Investigation, Injunction, and Other Relief Submitted by The Electronic Privacy Information Center (EPIC) and The Center for Digital Democracy (CDD) to the FEDERAL TRADE COMMISSION in the Matter of WhatsApp Inc. (29 August 2016) 9-10.
90 See Georg Clemens and Mutlu Özcany, 'Obfuscation and Shrouding with Network Effects - The Facebook/WhatsApp Case', available at https://ssrn.com/abstract=3023467, (2017). See also Stucke and Grunes (n 12) 169 (noting that the post-merger privacy issues in WhatsApp 'did not prompt a significant exodus').
91 See GDPR, Article 11-13. See also 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).
92 According to 2015 Eurobarometer survey, only one in five (18%) fully read privacy statements. See TNS Opinion & Social, 'Special Eurobarometer 431: Data Protection', (2015) 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.

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.[93] Thus, unless consumers are able to understand properly how firms use their data, they are unable to discipline firms' behaviour in relation to privacy. 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).[94] Another behavioural phenomenon that might affect users' privacy decisions is status quo bias, particularly default settings.[95] 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.

The manner WhatsApp notified the change of its privacy policy and what it entails shows that firms are mastering how to exploit the above discussed consumer behaviour on privacy policies and the power of defaults. 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 employed by WhatsApp in mobile devices.



World Economic Forum and Boston Consulting Group, 'Unlocking the Value of Personal Data: From Collection to Usage', (2013) 11.

93 Ryan Calo, 'Privacy and Markets: A Love Story', *Notre Dame Law Review*, 91(2)(2016) 673.

94 Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, 'Privacy and Human Behavior in the Age of Information', *Science*, 347/6221 (2015) 510.

95 Ibid.

Figure 3 – WhatsApp's Mobile Notice on Privacy Policy Change

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 and Facebook families. 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, the user 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 irrelevant information with critical information can serve as a 'shrouding strategy' that limits the visibility of key terms and lead users to discount the significance of the latter (in this case the sharing of their data with Facebook).[96] Agreeing to the terms will allow Facebook to use account information, such as mobile number, contact lists of WhatsApp users and non-users, and information about the last time of using the service. Here it is important to underline that the default, as shown by the 'pre-ticked-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 his/her data with Facebook has to 'uncheck the box'. A closer look at the updates, which is not shown in the screen, also reveals that even if a user opts-out, their mobile number will be shared with Facebook for other purposes such as securing systems, and fighting spam. The complexity of the design clearly shows how market players can exploit the behavioural considerations of users through sophisticated design and defaults. The privacy policy change has led to fines for Facebook and WhatsApp both 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, although it has also provided a caveat that the fine does not concern privacy, data protection or consumer protection issues.[97] More importantly, the Italian Competition and Consumer Protection Authority (Autorità Garante della Concorrenza e del Mercato – hereinafter AGCD) has fined WhatsApp three million euros for forcing 'users of its service WhatsApp Messanger [*sic*] to accept in full the new Terms of Use, and specifically the provision to share their personal data with Facebook, by inducing them to believe that without granting such consent they would not have been able to use the service anymore'.[98] The agency criticized how the opt-out options were designed to make it difficult for users to make effective choices including the following:

> a) …excessive emphasis placed on the need to subscribe to the new conditions within the following 30 days or lose the opportunity to use the service; b) an inadequate information on the possibility of denying consent to share with Facebook the personal data on WhatsApp account; c) the pre-selection of the option to share the data (opt-in);

96 See Clemens and Özcany (n 90) 2. See also Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox', *Social Psychological and Personality Science*, 4/3 (2013), 343-344.

97 European Commission - Press Release Mergers: Commission alleges Facebook provided misleading information about WhatsApp takeover (Brussels, 20 Dec. 2016).

98 Autorità Garante della Concorrenza e del Mercato (AGCM), 'Press Release - WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook (Rome, 12 May 2017)'.

d) finally, the difficulty of effectively activating the opt-out option once the Terms of Use were accepted in full.[99]

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 'obfuscation and shrouding' 'strategy that allows companies to deliberately limit the visibility of cost', in this case, the cost of sharing users' data with Facebook.[100] One source of weakness in the decision is that the Commission's conclusion was based on replies given by firms (not consumers themselves). However, given that the Commission's conclusion was predicated on the consumer's ability to exert effective constrains on the data collection practices and privacy policy of firms, it should have also taken into account whether actual consumer behaviour supports that assessment.[101]

One could argue that the post-merger measures taken by the AGCD is an indication that other regulatory measures, such as unfair competition, consumer and data protection rules 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 considered a key parameter of competition for the merging entities. 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 may not be able to effectively exert such constraint on firms, the competition analysis should take such evidence into account and competition authorities must take the necessary measures to mitigate those limitations.

In other words, if the Commission's conclusion that the merger would not lead to a concentration in the online advertising market or would not lead to reduction in privacy were solely dependent on the ability of users to constrain WhatsApp from sharing users' data with Facebook but the market evidence shows the existence of factors that will hinder users from exerting such constraint, measures should be taken to prevent WhatsApp from sharing the data with Facebook. For example, some of the competition law measures suggested by the Japan Fair Trade Commission study include limiting or requiring changes in corporate privacy policies and restrictions on digital platforms data collection practices.[102] 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,

99 Ibid.

100 Clemens and Özcany (n 90) 2.

101 One could argue that the Commission need not conduct such survey as it did not accept that the sharing of data would lead to concentration. However, the Commission could have for the sake of future guidance indicate the need for conducting such assessment and why it was unnecessary in the particular situation to do so.

102 Japan Fair Trade Commission, Summary Report of Study Group on Data and Competition Policy (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.'[103] 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 entail loss of revenue or is unprofitable. This is because the revenue generated from the advertisement might be superior to the loss of consumer resulting from the change of privacy policy.

Forbes magazine estimated that the change in WhatsApp's privacy policy and its business model – introducing tools which would allow users to communicate with businesses via WhatsApp could 'yield revenues of around 5 billion US dollars for Facebook in 2020, contributing about 9-10% of the company's total revenues'.[104] 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' to the merged entity without counter balancing the possible gains from the advertising on Facebook. This problem is associated with the multi-sided nature of many data-driven businesses where the data collected in from the user side is monetized on another side of the market or on a different platform. By considering change of privacy as unprofitable strategy, the Commission seems to overlook the interdependence of the business models and the value generated from data on the advertising market. This implies that analysis of whether users can exert effective competitive constraints on data privacy practices and privacy policy should factor in not only the consumer behaviour but also the incentives of the firms to do so and the revenues that could be gained from changing the privacy policies on other markets.[105]

The Commission's decision in *Facebook/WhatsApp* is also important in the sense that it may contribute to the perpetuation of what Economist Joseph Farrell refers as the 'dysfunctional equilibrium'.[106] 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'.[107] This is partly because firms expect that users will not read privacy policies and reward firms for this behaviour.[108] Some surveys lend some support to this assertion. For example, research among

103 *Facebook/WhatsApp*, para 174.
104 Trefis Team, 'How Much Revenue Can Facebook's WhatsApp Generate in The Next Five Years?', (*Forbes*, 3 March 2016).
105 See Michal Gal and Daniel Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement', *Antitrust Law Journal*, 80/3 (2016) 553 (noting that in assessing market power in two-sided markets, the benefits of an action on the 'free' side 'should be sought elsewhere').
106 Joseph Farrell, 'Can Privacy be Just Another Good?', *J. on Telecomm. & High Tech. L.*, 10 (2012) at 257.
107 Ibid.
108 Ibid 259.

45 social networks shows that the majority social networking sites do not mention privacy as a promotional tool and no site attempted to use the contents of its privacy policy as a draw to its services.[109] Even those sites that mention privacy as a promotional tool do so in 'a vague and general fashion'.[110] This, together with 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 (still chase the revenue from monetizing their data) regardless of their privacy promises;[111] consumers become 'resigned'[112] or develop 'learned helplessness'[113]. 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.[114]

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.[115]

Such equilibrium can be very hard to escape because a) a consumer cannot suddenly start reading privacy policies as they learn that it is not a rewarding activity; and b) even if he/she does, they are likely to learn little or get a confirmation of his/her cynicism as firms still expect that few consumers read polices and opt for vague or noncommittal policies.[116] Similarly, a smaller firm's ability to break such equilibrium is limited because users do not reward such behaviour and firms demand would not shift significantly, thereby the firm can only sacrifice

109 For example, no site promised not to collect IP addresses and other personal information. 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* (Boston, MA: Springer US, 2010), 121-167, 134.

110 Ibid.

111 Farrell (106) 257.

112 See Joseph Turow, Michael Hennessy, and Nora Draper, 'The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation', available at SSRN: https://ssrn.com/abstract=2820060, (2015) at 3. See TNS Opinion & Social (n 92) 7.

113 The Economist, 'Fuel of the Future: Data is Giving Rise to a New Economy', (6 May 2017).

114 Bonneau and Preibusch (n 109) 153.

115 Farrell (106) 258-259. Farrell describes the dysfunctional equilibrium as 'cynical market failure' because it 'can make mutually beneficial trades impossible.' ibid., at 257. Others have discussed the 'lemons market for privacy' with respect to social networks where the lack of ability of users to assess the quality of privacy on offer, which in turn is a result of deliberate confusology, not only lessens the incentive of sites to compete on privacy but also leads to disregard of privacy promises even by sites using privacy as a promotional tool. See Bonneau and Preibusch (n 109) 149.

116 Farrell (n 106) 259.

revenue from monetizing data.[117] Thus, more often than not, Farrell argues, escaping such equilibrium requires actions of large players.

However, as shown elsewhere,[118] the leading digital players lack the incentive to break from this equilibrium. This is because key digital markets and gateways are dominated by a handful of players with business models that rely on monetization of personal data. In addition, given the nature of their business models, the interests of these leading 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). This implies that the interests of these leading players are better served in such equilibrium and these players can even contribute to its perpetuation by making it difficult for smaller players from breaking the equilibrium through blocking and demoting such players in their platforms. 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 dole an emerging competition. The acquisition of WhatsApp by Facebook and the subsequent change to WhatsApp's' privacy policy is a good example that 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. As indicated by the Commission, 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'[119] and the 'free' effect.[120] From its popularity,[121] WhatsApp was succeeding in disrupting the equilibrium[122] and overcoming the challenges of the 'free effect', which seem to be halted by the merger.

Following the merger, WhatsApp did not only change its privacy policy to share data with Facebook but also, around the same time, it announced its decision to abandon the subscription-based model for WhatsApp and introduce a monetization strategy by allowing users to communicate with businesses via WhatsApp. Further, WhatsApp introduced other functionalities, such as allowing its users to post status updates, a feature similar to Facebook. All these changes could be sources of new information as WhatsApp could get insights from users' communications (e.g., insights into health of users if a user is communicating with psychiatrist) and WhatsApp has indicated that it would not exclude the possibility of introducing ads into its services.[123] This implies that before the merger, users had the option to

117 Ibid.
118 See Esayas, 'Competition in (Data) Privacy' (n 50).
119 See Stucke and Grunes (n 12) 133.
120 '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 John Newman, 'Antitrust in Zero-Price Markets: Foundations', *University of Pennsylvania Law Review*, 164 (2015) 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.
121 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*, para 84.
122 Stucke and Grunes (n 12) 133.
123 Deepa Seetharaman, 'Facebook Tees Up WhatsApp to Make Money', (*The Wall Street Journal*, 5 Sep 2017).

choose among the leading messaging apps, one based on subscription fee, minimum collection of personal data and ad free experience; and another that heavily relies on collection and monetization of users' data, which seems to have disappeared after the merger.[124] Following the merger, the two leading messaging apps, each with 1.2 billion users, 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 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 perpetuate the 'dysfunctional equilibrium' and the competition on privacy and PETs will hardly mature.

B. Microsoft/LinkedIn

The *Microsoft/LinkedIn* merger is another decision where the Commission identified data privacy as 'a significant quality' parameter between Professional Social Networks (PSNs). However, unlike the *Facebook/WhatsApp*, the Commission's analysis of privacy as a non-price competition parameter seems to have improved significantly, both in recognising the possible competition in dissimilarities but also in articulating clear theory of harm on how a merger might lead to a market power and consequent reduction in privacy as a quality factor. The Commission's analysis also seems cognisant of the relevant data privacy principles.

In this decision, the Commission examined the extent that the pre-installation of LinkedIn with Microsoft Windows PCs Operating System (OS) and its integration with Office products such as Outlook, Word, Excel and Power Point can harm consumer privacy. Having already identified data privacy as 'a significant quality' parameter of competition between PSNs, the Commission held that if Microsoft were to pre-install LinkedIn in Windows and integrate it with the Office products, it would reduce consumer choice in relation to privacy.[125] More specifically, the Commission noted that given the large market share of Windows' OS in the market for PCs, LinkedIn's pre-installation can increase barriers to entry or expansion by making it difficult for other PSNs to acquire consumers or making switching more difficult.[126] This is because first, given that majority of users use LinkedIn on Windows PCs as opposed to other PCs or mobile devices, such pre-installation would increase LinkedIn's 'visibility to a very large number of users' and thereby 'potentially lead to a meaningful increase in LinkedIn membership and user activity.'[127]

Secondly, given that 'Windows PCs constitute the most important channel for PSNs to acquire new customers' and 'an important channel to ensure user engagement' the pre-

124 'The merger, therefore, has entailed a loss of options by the user. That is, where prior to the said merger two different models coexisted (WhatsApp – with greater data protection but with the requirement of an annual cash payment) and Facebook Messenger (less privacy protection but free) there is now just one (free service but with little privacy). Consequently, for those users who valued their privacy at a monetary amount higher than requested by WhatsApp, with the merger they have seen their welfare decrease (*decreased quality in terms of privacy*).' See Autoritat Catalana de la Competència, 'The Data-Driven Economy Challenges for Competition', (Barcelona, 2016) at 26 [emphasis added].
125 *Microsoft /LinkedIn*.
126 Ibid para 309.
127 See ibid para 318-319.

installation would make it difficult for competing PSNs to recruit new users.[128] Moreover, the Commission noted the lack of ‘‘effective counterstrategies’ for competing PSNs to offset the effect of the pre-installation of LinkedIn on Windows PCs … because OEMs may lack incentives to pre-install a second PSN application which would, in essence, duplicate the same functionalities as the LinkedIn application.’[129] This creates inertia in the sense that users are ‘unlikely to decide spontaneously to download an application that is not already pre-installed’.[130] Thus, the increase in number of users from such pre-installation, the network effects from more users together with the effect of inertia resulting from the pre-installation would deny competing PSN equivalent access to customers and ultimately lead to their foreclosure from the market.[131]

Similarly, the integration of LinkedIn into Office products was considered to have similar effect in increasing LinkedIn’s user base and its usage. More particularly, the Commission noted that LinkedIn’s integration with Outlook would ‘significantly expand’ its user base because it gives LinkedIn ‘the ability (subject to user consent) to access Outlook users’ address books and suggest new LinkedIn connections.’[132] This integration could be complemented by denying competing PSN access to Outlook (and other Microsoft) APIs, leaving competing PSNs with no ‘counterstrategy at their disposal to sufficiently counter the merged entity's actions’ and thereby leading to their foreclosure.[133]

Having noted the incentives and ability of Microsoft for engaging in both conducts, the lack of other factors that reduce such incentives, together with potential entry barriers from network effects, the Commission noted that the market could tip in favour of LinkedIn and make it ‘more difficult for actual competing providers of PSN services to regain their ability to compete and for potential competitors to enter the market’.[134] According to the Commission, this would harm consumers in two ways. First, the conduct 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, with no or limited prospects of entry by new PSN service providers.’[135] Secondly, and more importantly, the conduct would reduce consumer choice in relation to privacy. This is because such conduct may lead to marginalization and eventual foreclosure of PSN providers such as XING that ‘offer a greater degree of privacy protection than LinkedIn’.[136] Highlighting why XING was considered to offer better (quality of) privacy protection than LinkedIn, the Commission refers to the differences in privacy policies as follows:

> during the registration process, *XING asks users to actively accept XING's privacy policy and Terms & Conditions by ticking a box*, whereas LinkedIn users accept LinkedIn's privacy policy automatically when they press the button "join now". Moreover, *when XING introduces new services which have an implication on how it collects and/or uses its members' data, it explicitly seeks active consent from the members*. In addition, *regardless*

128 For example, Windows PC accounted ‘for more than half of total LinkedIn sign-ups’ and ‘for more than 30% of LinkedIn usage’. See ibid para 318.
129 Ibid para 320.
130 Ibid.
131 Ibid.
132 Ibid para 328.
133 Ibid para 329-330.
134 Ibid para 347.
135 Ibid para 349.
136 Ibid para 350.

of whether members give their consent in such specific cases or not, they will be able to continue to use XING as such without losing any of the functions to which they previously had access. In contrast, when LinkedIn makes changes to its collection, storing, processing or usage of personal data, LinkedIn only informs the members of those changes and considers that LinkedIn members agree with those changes, if they continue to use LinkedIn's services after they have been notified of the changes.[137]

Three points require particular mention from the above paragraph. Firstly, the theory of harm 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. In other words, user's valuation of privacy as a quality parameter is not limited to how much personal data is collected but also includes other dimensions such as users' ability to control their data and make informed decisions. This is an important clarification because one source of scepticism for incorporating data privacy into competition analysis as a non-price parameter is the alleged trade-off between increased data collection and improvements in the quality of the underling service.[138] However, this trade-off claim is based on the narrower view of competition in data privacy as anchored on more data collection. Collecting less data is only one dimension of competition in data privacy. This is because, as the above paragraph in *Microsoft/LinkedIn* decision shows, companies can compete through the quality of consent, by actively seeking users to tick-box, not only during registration but also when making policy changes. Moreover, even if users decline to consent to changes, they can still compete by allowing users to continue to use functionalities which they previously had access to.

Secondly, although the decision makes no reference to EU data privacy rules, the theory of harm reflects the different qualities of consent under these rules. The fact that 'XING asks users to actively accept XING's privacy policy and Terms & Conditions by ticking a box' and 'explicitly seeks active consent from the members' when introducing new features manifest competition based on the requirement (dimension) that consent must be 'unambiguous'. Unambiguity entails that the consent must be given before the processing activity starts and manifested through a positive and definite act – such as ticking a box.[139] In this regard, the Commission views XING's approach as *more unambiguous* and thus providing users a better quality of privacy than LinkedIn.

In addition, the possibility that users can 'continue to use XING without losing any of the functions to which they previously had access' even when withholding consent to new features manifest competition based on the requirement (dimension) that consent must be 'freely given'. This element entails that the user must be given the opportunity to make a genuine choice including the ability to withhold/withdraw her consent without fearing negative consequences.[140] In this sense, by allowing users to continue to use existing functionality while withholding consent for new features, the consent obtained by XING qualifies as *more* 'freely given' than the one obtained by LinkedIn and thus offering users a better (quality) of privacy than LinkedIn. Thus, the foreclosure of XING was considered anticompetitive because it

137 Ibid [emphasis added].
138 See Cooper (n 23) 1135-36.
139 See Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' adopted on 13 July 2011 (WP 187) 12.
140 Ibid 12-13.

deprives users a better quality PSN and if the merger was allowed, users may be left with all but a PSN, i.e. LinkedIn, with inferior quality of privacy to join. Thus, Microsoft offered remedies allaying the foreclosure concerns and thus precluding adverse effects on privacy.

Related with the above, the Commission noted the need for Microsoft to obtain consent from users in accordance with the EU data privacy law if it wants to integrate LinkedIn into Microsoft Outlook.[141] Although it is not clear if competition authorities would follow-up in case the merging parties fail to comply with such measures, it is a step in the right direction in the consistent application of competition and data privacy rules. Such measures would allow data subjects to reconsider whether they would like to entrust their data to the new entity or not.

Last but least, the decision is important because it shows that it is not always necessary to quantify reduction in privacy. This is important because the lack of a concrete benchmark for measuring degradation in privacy is one of the main sources of scepticism against the quality-based arguments. As the argument goes, the absence of concrete benchmarks with which to determine degradation in privacy could lead to a nebulous application of competition law with unpredictable outcomes.[142] However, as the Commission's decision in *Microsoft/LinkedIn* demonstrates, not all privacy degradations are difficult to measure and the classical anticompetitive conducts such as tying could lead to reduced competition in privacy as a competition parameter. This indicates that reductions in the level of privacy could fit easily into existing anticompetitive conduct provided competition authorities recognise data privacy as a form of non-price competition. In this instance, the Commission reached at the conclusion by looking at the foreclosing effect of the conduct, i.e. tying, without tackling the thorny issue of measuring quality of privacy.

Overall, the above discussions on the *Facebook/WhatsApp* and *Microsoft/LinkedIn* demonstrate that reductions in privacy as a quality can result from 1) an increase in the amount of personal data demanded or expanding usage of existing data; 2) abandoning end-to-end encryption; 3) a conduct that negatively affects users' ability to control their data and make informed decisions. The application of the theory in the *Microsoft/LinkedIn* merger further shows its maturity and that discussions are no longer restricted to academic circus. 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.[143]

141 *Microsoft /LinkedIn*, para 328.

142 See citations in Costa-Cabral and Lynskey (n 9)28-9.

143 The author has addressed some of these scepticisms in another work. 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).

Conclusion

This article has provided a critical analysis of the *Facebook/WhatsApp* merger infused with some lessons from the *Microsoft/LinkedIn* regarding the competition in privacy. As digital markets evolve towards services offered at 'zero' price but in exchange for personal data, the market definition and 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. The recognition of data privacy as a non-price parameter in the *Facebook/WhatsApp* and *Microsoft/LinkedIn* is a step in the right direction and a testimony to the flexibility of competition policy to accommodate such competition. However, as the analysis on the Commission's decision in *Facebook/WhatsApp* demonstrates, there is a room for improvement in terms of how the competition in data privacy is manifested. The article has underlined that 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 or policy can be just the beginning of a competition that exerts competitive pressure on others, rather than make the firms complementary. In this regard, data privacy principles could prove to be helpful for competition authorities to easily detect the manifestations of this competition.

Similarly, market power assessment should give due regard to 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. The Commission's decision in *Facebook/WhatsApp* could be criticized for the shaky assumptions in relation to the analysis of competitive constraints on and the incentives of the merged entity to change the privacy policies. The first assumption is that users are able to impose effective competitive constraints on firm's data collection practices and privacy policies. The second relates to the Commission's assumption that the potential change in privacy policy to collect data as an unprofitable strategy. It has been shown that these assumptions are untenable in light of consumer behaviour and possible revenue from increased targeting that comes from collecting more data. The article maintains that the Commission's decision in *Microsoft/LinkedIn* brings significant improvements in the discussions of privacy as a non-price (quality) competition parameter. More particularly, the decision represents a step forward in recognising the possibility that competition in privacy can be manifested through dissimilarities in privacy policies, but also in articulating clear theory of harm on how a merger might lead to a market power and consequent reduction in privacy as a quality factor.