Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 31

Data Accumulation and the Privacy-Antitrust Interface: Insights from the *Facebook* case for the EU and the U.S.

Giuseppe Colangelo & Mariateresa Maggiolino

2018

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Giuseppe Colangelo is a Jean Monnet Professor of European Innovation Policy and Associate Professor of Law and Economics at University of Basilicata, Italy. He is also Adjunct Professor of Markets, Regulation and Law, and of Legal Issues in Marketing at LUISS Guido Carli and Bocconi University, Italy.
He graduated in Law from LUISS Guido Carli, earned an LL.M. in Competition Law and Economics at the Erasmus University of Rotterdam, Netherlands, and a Ph.D. in Law and Economics at LUISS Guido Carli.
His primary research interests are related to innovation policy, intellectual property, competition policy, market regulation, and economic analysis of law.
Giuseppe has been a TTLF Fellow since 2017.

Mariateresa Maggiolino is Associate Professor of Business law at Bocconi University, Italy. In 2015, she has been a visiting professor at Fordham Law School, New York. From 2010 to 2014, she participated in two EU-sponsored thematic networks on Public Sector Information.
Mariateresa earned her Master Degree in Economics and Social Sciences (M.S.ESS), summa cum laude, from Bocconi University in 2001; her Master Degree in Law (J.D.), summa cum laude, from Statale University of Milan in 2006; and her LL.M. Degree from Iowa University School of Law in 2007.
Mariateresa has published many articles in international and national journals and a monograph with Edward Elgar (2011, "Intellectual Property and Antitrust. A Comparative Economic Analysis of US and EU Law"). Her main fields of interest are antitrust law, IP law, and data law. Her present research focuses on big data and the power of information.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Giuseppe Colangelo & Mariateresa Maggiolino, Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook case for the EU and the U.S., Stanford-Vienna TTLF Working Paper No. 31, http://ttlf.stanford.edu.

Copyright

Abstract

The emergence of multi-sided media platforms occurred in parallel with the success of business models that revolve around the collection and use of personal data, generating revenue from user-data-based profiling and advertising. In such a context, data protection rules do not appear to be very effective, and thus the main privacy concerns relate to users' ability to control their digital identities. However, together with mere privacy issues, another concern lies at the heart of the debate about the data economy: that the collection and aggregation of data (including personal data) by dominant firms entrenches their dominant positions.

This paper discusses these issues by analysing the *Facebook* case initiated by the German Competition Authority. The Bundeskartellamt takes the view that Facebook is abusing its dominant position by leveraging its social network to amass, without limitation, a broad range of data generated by its users when they visit third-party websites. Facebook then merges this data with users' Facebook accounts. By focusing on these activities, the Bundeskartellamt takes the position that Facebook may use such data to optimize its commercial activity and tie more users to its network.

Based on a consideration of both EU and U.S. legislation, this paper will analyse the conditions under which the Facebook's conduct could fall within the scope of antitrust rules.

Keywords: Antitrust; Privacy; Big data; Facebook; Bundeskartellamt; Unfair practice

JEL Codes: D83, K21, L12, L4

Contents

1. Introduction.

The data economy has brought to the fore a particular concern: that individuals may lose control over their digital identities. They may be associated with profiles that risk not only being false or inaccurate, but also preclude them accessing certain goods and services, with the ultimate effect of damaging their dignity and their ability to live as free subjects. Given that in the digital economy only *some* of the firms elaborating those profiles hold monopoly power in the downstream markets where digital services are offered, the privacy-antitrust interface has gained momentum. Many have indeed wondered whether and when the law on abuses of dominant positions (or monopolist conduct) could be drawn upon in order to mitigate data protection shortcomings, in order to provide individuals a better guarantee of full control over their digital identities.

However, another concern lies at the heart of the debate about the data economy: that the collection and aggregation of data, including personal data, by dominant firms entrenches their dominant positions. The virtuous (or vicious) cycle that achieves this end runs as follows: the more data a firm gathers and analyzes, the better its products, the more users it attracts, the more data it collects and processes, and so on. Upon a *prima facie* consideration, antitrust law cannot break this cycle because firms amassing and elaborating on increasing quantities of data improve their products and thus increase consumer welfare, at least in the short run. However, one could wonder whether privacy law-based regulation of personal data collection could be used to compensate for this antitrust gap by stopping dominant firms from accumulating personal data. This is why the privacy-antitrust interface is of particular importance to this field.

This paper discusses this issue by considering the *Facebook* case, which was initiated by the German Competition Authority (GCA). The Bundeskartellamt is currently in the midst of a procedure brought against Facebook concerning an alleged abuse of its dominant position in the market for social networks – an abuse that consists of the imposition of unfair terms and conditions aimed at accumulating ever-increasing quantities of user data. In particular, the Bundeskartellamt takes the view that Facebook is conditioning the use of its social network on its being allowed to amass, without limitation, any kind of data generated by its users when using third-party websites and to merge these data with users' Facebook accounts. In its preliminary assessment of Facebook's terms and conditions, the Bundeskartellamt also applied privacy principles, arguing that those conditions violate both antitrust rules and data protection provisions.

This paper will be structured as follows. Section 2 will introduce the facts scrutinized by the Bundeskartellamt in its investigation. Section 3 will discuss how antitrust law could tackle and characterize those facts. Specifically, it will analyze the conditions under which Facebook's conduct could fall within the scope of Article 102 TFEU and Section 2 of the Sherman Act. It will then explore whether Facebook's conduct could be deemed, on the European side, to constitute an exploitative abuse within the meaning of Article 102(a) and, on the U.S. side, as an unfair method of competition pursuant to Section 5 of the FTC Act. Since the outcome to this analysis will show that antitrust law cannot do much against data collection and aggregation, especially when it results from unilateral practices, Section 4 will describe the privacy-antitrust interface by discussing the role that privacy rules (and

arguments) could play in filling the gaps within antitrust law. Paragraph 5 will then set out some concluding remarks.

2. The *Facebook* case.

In March 2016, the GCA launched an investigation of Facebook due to suspicions that, via its specific terms of service governing the collection of user data, Facebook had abused its dominant position in the social network market.[1] Andreas Mundt, the President of the Bundeskartellamt, stated that, "[d]ominant companies are subject to special obligations. These include the use of adequate terms of service as far as these are relevant to the market. For advertising-financed internet services such as Facebook, user data are hugely important. For this reason it is essential to […] examine [also with reference to] the aspect of abuse of market power whether consumers are sufficiently informed [regarding] the type and extent of data collected."

The press release accompanying the launch of the proceeding contains language that is worth recalling, as it pertains to the analysis in the following sections. Specifically, the Bundeskartellamt states its initial suspicion that Facebook's conditions of use are in violation of data protection provisions: "In order to access the social network, users must first agree to the company's collection and use of their data by accepting the terms of service. It is difficult for users to understand and assess the scope of the agreement accepted

[1] Bundeskartellamt, *Facebook*, Press release, 2 March 2016, http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568 .

by them. There is considerable doubt as to the admissibility of this procedure, in particular under applicable national data protection law."

Although not every infringement of the law by a dominant undertaking is relevant under competition law, in the case at stake, Facebook's use of unlawful terms and conditions could represent an abusive imposition of unfair conditions on users: "If there is a connection between such an infringement [of data protection provisions] and market dominance, this could *also* constitute an abusive practice under competition law."[2] Therefore, according to the press release, the proceedings will consider whether any of Facebook's terms and conditions for user data collection that violate data protection law and mislead users may *also* be deemed to constitute abuses of a dominant position pursuant to Article 102(a) TFEU.

The investigation is still in progress and the Bundeskartellamt has recently released its preliminary assessment.[3]

The Bundeskartellamt assumes that Facebook has a quasi-monopoly on the German market for social networks due to the massive number of users (around 30 million users per month, of which 23 million use Facebook on a daily basis) and the limited substitutability of rivals' products. Direct network effects play a crucial role in the latter market feature, as a result of both the size of the social network and the ability of users to find persons they want to

[2] Emphasis added.
[3] Bundeskartellamt, 'Preliminary assessment in *Facebook* proceeding', Press release, 19 December 2017, http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html . Further information are provided by a background paper: see Bundeskartellamt, 'Background information on the Facebook proceeding', 19 December 2017, http://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.html?nn=3600108 .

associate with (so-called "identity-based network effects"). According to the GCA, these direct network effects operate as significant barriers to entry, since users become locked-in and find it extremely difficult to switch to one of Facebook's competitors. Furthermore, Facebook's dominance is enhanced by indirect network effects. For instance, in advertising-supported platforms the advertising side profits from a large private user base, and a competitor must acquire a critical mass of private users in order to enter the market successfully. Moreover, German social network users appear to be bound to a single platform, and do not explore the possibility of participating in several different social networks at the same time (multi-homing). Multi-homing options would make it difficult for Facebook to lock-in users and consolidate its market dominance. Finally, according to the Bundeskartellamt, professional networks (such as LinkedIn and Xing) as well as messaging services (such as WhatsApp and Snapchat) or other social media (such as YouTube or Twitter) are not part of the relevant product market because, even though these services are in some respects competitive substitutes for Facebook, they merely serve a complementary need from the users' perspective.

Due to its dominant position, Facebook takes advantage of superior access to users' personal data, which is an "essential factor" for competition in data-driven markets. In order to secure and enhance this advantage, according to the Bundeskartellamt, Facebook has rendered usage of its service conditional upon users granting extensive permission to collect their personal data. In particular, the GCA alleges that Facebook makes usage of its social network conditional on its being allowed to amass without limitation any kind of data generated when using third-party websites and to merge it with the user's Facebook

account (the so-called "Facebook package"). Third-party sites include services owned by Facebook (such as WhatsApp or Instagram) as well as websites and apps of other operators with embedded Facebook application programming interfaces (APIs).[4] If a third-party website has embedded Facebook products such as the 'like' button or a 'Facebook login' option or analytical services such as 'Facebook Analytics', data will be transmitted to Facebook via APIs as soon as the user calls up that third party's website for the first time. Through APIs, data are transmitted to Facebook and collected and processed by Facebook even when a Facebook user visits other websites. Thus, the GCA differentiates between user data generated through usage of Facebook ('on Facebook') and user data obtained from third party sources ('off Facebook'), and has focused the proceedings on the latter

[4] Even if it is unrelated to the proceeding at stake, it is worth mentioning that, in May 2017, the European Commission fined Facebook €110 million for providing incorrect or misleading information during the investigation of Facebook's acquisition of WhatsApp under the EU Merger Regulation (European Commission, Case M.8228, *Facebook/WhatsApp*, (2017) OJ C286/06). Notably, when Facebook notified the Commission of the acquisition of WhatsApp in 2014, it stated that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. The Commission has found that, contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility. Several national protection data regulators are also digging into the issue of WhatsApp's user data sharing: for instance, on 18 December 2017 the French data protection Commission (CNIL) issued a formal notice to WhatsApp to comply with the Data Protection Act within one month (https://www.cnil.fr/en/data-transfer-whatsapp-facebook-cnil-publicly-serves-formal-notice-lack-legal-basis). On the antitrust side, see Italian Competition Authority, 11 May 2017, Cases PS10601 and CV154, *WhatsApp* (http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html), closing two investigations related to the exchange of personal data with Facebook and oppressive clauses. In contrast to the German perspective, the practices at issue were evaluated as potential violations of the Consumer Code instead of antitrust law. The first proceeding ascertained that Facebook forced WhatsApp Messenger users to wholly accept the new terms and conditions, in particular the terms regarding the sharing of their personal data with Facebook, by allegedly making them believe, through a message made visible when opening the application, that it would have been otherwise impossible to continue using it. Moreover, the conditioning effect has been reinforced by making Facebook the default option in the secondary level page to which the user was redirected through a link contained in the main message. The other proceeding ascertained the oppressive nature of some contractual clauses included in WhatsApp Messenger's terms of use, specifically those concerning the right granted to the company to unilaterally change contractual provisions, the termination right granted exclusively to the firm, the exclusions and limitations of liability established in its favor, the possibility of interrupting service without justification, and the choice of jurisdiction in case of disputes.

only, leaving open the possibility of evaluating the collection and usage of data on the Facebook network itself for a later stage.

The Bundeskartellamt is mainly concerned with the collection of data outside of Facebook's social network and the merging of this data into a user's Facebook account. It considers that Facebook "can use [these data] to optimize its offer and tie more users to its network. With the merging of the data the 'identity-based network effects' and, consequently, the 'locking-in' of users increase, to the detriment of other providers of social networks. In addition, with the help of the user profiles generated, Facebook is able to improve its targeted advertising activities. As a consequence, Facebook is becoming more and more indispensable for advertising customers. This is also reflected in the rapidly increasing turnover Facebook has been able to generate in the past years. There is also potential for competitive harm on the side of the advertising customers who are faced with a dominant supplier of advertising space." In other words, the Bundeskartellamt is arguing that Facebook's practice of forcing users to choose between accepting the whole Facebook package or not using Facebook at all indicates that Facebook is imposing unfair conditions and/or foreclosing rivals, with the ultimate effect of impairing competition in the advertising market.

However, as has been argued by Bundeskartellamt President Mundt, "[d]ata protection, consumer protection and the protection of competition interlink where data, as in Facebook's case, are a crucial factor for the economic dominance of a company." Similarly, in its preliminary assessment, the Bundeskartellamt "*also* applies data protection

principles."[5] Mundt remarks that "users are unaware of this [the collection and processing of data outside Facebook's social network]. And from the current state of affairs we are not convinced that users have given their effective consent to Facebook's data tracking and the merging of data into their Facebook account. The extent and form of data collection violate mandatory European data protection principles." Although users should expect a certain level of processing of their data if they use such a free service, they cannot anticipate that the data they generate on third-party websites will be added to their Facebook account on this scale.

The damage to users due to Facebook's exploitative terms of business consists of a "loss of control," since users are no longer able to control how their personal data are used: "*Within the network* they can considerably influence the extent to which their data are being collected by paying attention to the way they use the network and the content they post."[6] In this regard, according to the Bundeskartellamt, data protection law pursues the same objective as competition law, which is to protect individuals from having their personal data exploited by the opposite side of the market. Since users are oblivious as to which data from which sources are being merged to develop a detailed profile of them and their online activities, Facebook's data merging "*also* constitutes a violation of the users' constitutionally protected right to informational self-determination."[7] In sum, according to the Bundeskartellamt's preliminary assessment, Facebook's terms and conditions are neither acceptable under competition law standards nor justified under data protection principles.

[5] Emphasis added.
[6] Emphasis in the original.
[7] Emphasis added.

Nevertheless, by considering the antitrust-privacy interface and comparing the press release concerning the preliminary assessment with the previous press release announcing the launch of the proceeding, it seems that the pendulum has been swinging back and forth.

On the one hand, in the first press release the Bundeskartellamt challenged Facebook's terms and conditions which were applicable to the collection of user data on the grounds that they were incompatible with data protection rules. They also explored whether there was any connection between such an infringement of data protection law and market dominance, finding that Facebook's terms and conditions may "*also*" be regarded as abuses of a dominant position pursuant to Article 102(a) TFEU. That line of reasoning cast some doubts on the notion that the judgment regarding the unfairness of Facebook's contractual terms and conditions would depend on the existence of a privacy violation. In other words, the concern was that a privacy violation could automatically turn out to constitute an abuse of dominance.[8]

On the other hand, the recent preliminary assessment seems to clarify these doubts. According to the related press release and background paper, the Bundeskartellamt is asserting that Facebook's contractual terms and conditions are unfair, apart from any privacy infringement. Indeed, the Bundeskartellamt regards the proceedings as a case of exploitative terms of business, taking the view that Facebook is imposing unfair conditions by making use of its service conditional upon users' grant of extensive permission to

[8] G. Colangelo and M. Maggiolino, 'Data Protection in Attention Markets: Protecting Privacy Through Competition?', 2017 *Journal of European Competition Law and Practice* 363, 367 (2017). See also T. Körber, 'Is Knowledge (Market) Power? On the Relationship between Data Protection, "Data Power" and Competition Law', (2018) 23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112232, noticing that it remains unclear what role a violation of data protection laws would play.

collect their personal data. Therefore, the GCA is attempting to establish a violation of antitrust law, which would stand even in the absence of any privacy concerns, but with the 'peculiarity' that it occurred alongside a self-standing privacy violation. According to the preliminary assessment, while the Bundeskartellamt's focus is mainly on the antitrust issue of Facebook's strategy, it is "*also*" applying data protection principles.

3. The antitrust assessment of Facebook's conduct.

Put simply, the GCA is accusing Facebook of collecting user data from third-party websites without users' consent. The Bundeskartellamt not only suspects that Facebook users are unaware of this collection of "off-Facebook" user data, but also – most importantly – claims that Facebook's social networking services are so essential that the request for a general (rather than specific) authorization for the collection of user data is equivalent to a "take it or leave it" demand, even for well-informed and educated users.

As a matter of law, aside from any privacy concerns, the Bundeskartellamt is concerned with two antitrust issues. First, it claims that this accumulation of data is allowing Facebook to entrench its dominant position: Facebook "can use [these data] to optimize its offer and tie more users to its network […] to the detriment of other providers of social networks"; and Facebook "is becoming more and more indispensable for advertising customers […with…] [a] potential for competitive harm on the side of the advertising customers." Second, the GCA alleges that the Facebook's request for a single catch-all grant of consent is unfair within the meaning of Article 102(a).

Let us now explore these two legal characterizations of Facebook's conduct, after considering a preliminary doubt. There are grounds to conclude that third-party websites have authorized Facebook to embed its applications. In other words, unless one seeks to claim that Facebook is also abusing its bargaining power in its business dealings with the websites, the embedding also furthers the economic interests of third-party websites, which may be willing to take advantage of Facebook's popularity and portfolio of users. Therefore, it may be questioned whether the conduct at stake constitutes truly unilateral conduct within the meaning of Article 102, or rather an agreement constituting a restraint of trade within the meaning of Article 101.

3.1 Facebook's conduct as an exclusionary and anticompetitive practice: are there grounds for Article 102(b) TFEU or for Section 2 of the Sherman Act to apply?

According to settled case law in the European Union and in the United States, a dominant firm's unilateral practice violates antitrust law if two conditions are met: if the practice is capable of excluding rivals and if it is liable to reduce consumer welfare.[9]

In the *Facebook* case, the behaviour whereby the social network acquires increasing quantities of data consists of embedding Facebook products in third-party websites, such as the 'like button', the 'Facebook login option', or analytical services such as 'Facebook Analytics'. In this regard, it is true that a firm which collects and analyzes increasing quantities of data will be able to improve its services and make them more attractive for

[9] See *U.S. v. Microsoft Corp.,* 253 F.3d 34 (D.C. Circuit 2001) and, recently, CJEU, Case C-413/14 P, *Intel Corp. v. European Commission,* EU:C:2017:632.

consumers. Processing big data is a way of acquiring knowledge about users and making services more suitable for them. It is also true that data accumulation contributes to strengthening firms' market positions. However, the fact that a third-party website embeds Facebook's products does not necessarily prevent that website and others from incorporating the products of other social networks, such as Twitter, Pinterest or Google Plus. Moreover, given digital systems, there is reason to expect that a variety of different products can be embedded in a website's architecture. In addition, the fact that one firm receives increasing quantities of personal data does not prevent its rivals from doing the same, as many U.S. and EU mergers cases have already shown. As long as there is no bottleneck in access to personal data, even data accumulation carried out by a dominant firm does not constitute an exclusionary practice.

Nevertheless, suppose that a dominant firm could embed its products into third-party websites as part of a kind of pre-emptive strategy to exclude rivals. Or, suppose that a dominant firm could increase the volume of its own data, thus preventing its rivals from gathering alternative personal data. In both cases, there is a question as to whether such behaviour could also be anticompetitive.

It is clear that the act of embedding the 'like button' or the 'Facebook login option' into third-party websites does not reduce market output. In addition, it does not seem to decrease the rate of innovation. Finally, one could argue that such conduct increases the variety of supply and meets consumer demands for the service that Facebook is actually providing. Thus, there are two remaining ways of establishing a reduction in consumer welfare. Neither is easy to substantiate; both are rooted in privacy considerations, as they

are based on the notion that the 'like button' or the 'Facebook login option' are tools for extracting personal data.

It could be argued that, by incorporating these into third-party websites, Facebook is increasing the implicit prices of the Internet services offered by those websites. In other words, if it is admitted that data are the currency of the Internet – as will be further argued in section 4.1 – then the more data a website asks its users to provide, the higher the price of its services will be. Therefore, one could attempt to establish that this additional accumulation of personal data is essentially tantamount to a price increase on the markets for the services offered by those third-party websites. However, this claim seems to be quite difficult to substantiate. Not only do we not know the competitive level of personal data that a website should ask its users to provide (and thus cannot establish whether there has been a price increase), but it is quite apparent that an increase in the price of a specific Internet service – one that has the like button or the login option embedded – does not amount to an overall increase in market price.

As for the second theory of harm, it could be argued that by collecting personal data via the 'like button' or the 'Facebook login option', Facebook debases the quality of the services offered by third-party websites. In other words, if it is assumed that the quality of Internet services decreases as those services become less privacy-friendly – as will be further argued in section 4.2 – then the more data a website asks its users to provide, the lower the quality of its supply will be. Therefore, one could try to show that the additional accumulation of personal data via the 'like button' or the 'Facebook login option' equates to a reduction in consumer welfare on the markets for the services offered by those third-

party websites. However, this claim appears to be difficult to prove (and this is not to mention the substantiation of its relevance on privacy grounds), as it would be necessary to demonstrate that a reduction in privacy-friendliness is sufficient to cause an overall reduction in quality, which in turn should be enough to support an overall reduction in consumer welfare.

In summary, it is not disputed that the act of accumulating (personal) data may serve to better shelter dominant positions. However, as long as the data accumulation results in the provision of new services that satisfy consumer needs and wants, it is hard to show that it amounts to an anticompetitive act. This is because the application of the foreclosure theory cannot be taken for granted, but also because no reduction of consumer welfare is apparent, unless any privacy-related arguments establish grounds for the application of the antitrust theory of harm.

It may be the case that the Bundeskartellamt is aware of the hurdles that it must overcome in order to show the exclusionary and anticompetitive nature of the twofold act of embedding Facebook applications into third-party websites and then of accumulating data via those sites. Thus, in order to remain within the four corners of its claim and also within the boundaries of 'traditional' antitrust law, the German Authority must follow a different direction from its normal path and attempt to apply Article 102(a) to such behaviour.

3.2 Facebook's conduct as an exploitative abuse: are there grounds for the application of Article 102(a) of TFEU?

Article 102(a) TFEU prohibits the dominant firm from imposing *unfair* trading conditions on its counterparties. Since the collection of personal data takes place under the terms of an agreement reached between the users of a website and the firm managing that website, one could argue that the act of data collection amounts to an exploitative abuse where the arrangements applicable to it are unfair.

The notion of unfairness has only been analyzed by the Court of Justice and the European Commission in a few decisions.[10] For example, in some old judgments and decisions, the injustice of the clauses analyzed was traced back to two facts: the circumstance that such clauses were not functional to the achievement of the purpose of the agreement, and the fact that the clauses were unjustifiably restricting the freedom of the parties. In particular, in *SABAM*, the Court held that an exploitative abuse may occur when "the fact that an undertaking entrusted with the exploitation of copyrights and occupying a dominant position … imposes on its members obligations which are not absolutely necessary for the attainment of its object and which thus encroach unfairly upon a member's freedom to exercise his copyright."[11]

More recently, the objective element of the above interpretation of Article 102(a) – namely, the association between unfairness on the one hand and the absence of a functional relationship between the contractual clauses and the purpose of the contract on the other

[10] K.J. Cseres, 'Towards a European model of economic justice: the role of competition law', in *The many concepts of social justice in European private law* (H.W. Micklitz ed.), Edward Elgar 2011, 427. See also H. Kalimo and K. Majcher, 'The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace', 42 *European Law Review* 210 (2017)

[11] CJUE, Case 127/73, *Belgische Radio en Televisie e société belge des auteurs, compositeurs et éditeurs v. SV SABAM e NV Fonior*, EU:C:1974:25, para. 15. See also European Commission, Case IV/26.760, *GEMA*, (1981) OJ L94/91; Case IV/26.760 *GEMA II*, (1972) OJ L166/22; Case IV/29.971, *GEMA III*, (1982) OJ L94/12.

hand – was highlighted in *Tetra Pak II*[12] and in *Duales System Deutschland (DSD)*.[13] Furthermore, in the latter case the Commission referred back to the findings of the Court of Justice in *United Brands* to state that "[u]nfair commercial terms exist where an undertaking in a dominant position fails to comply with the principle of proportionality."[14]

Moreover, it may be inferred from a reading of some of the Commission's other decisions that in some cases unfairness has been associated with opaque contractual conditions that have increased the weakness of the dominant firms' counterparties, which ended up being unable to understand the actual terms of the commercial offer in question. In particular, in *Michelin II* the Commission concluded that a discount program implemented by the French company was unfair because it "placed [Michelin's dealers, that is, its counterparties] in a situation of uncertainty and insecurity," because "it is difficult to see how [Michelin's dealers] would of their own accord have opted to place themselves in such an unfavourable position in business terms," and because Michelin's retailers were not put in a condition to carry out "a reliable evaluation of their cost prices and therefore [could not] freely determine their commercial strategy."[15]

[12] European Commission, Case IV/31.043, *Tetra Pak II*, paras. 105-108, (1992) OJ L72/1.
[13] European Commission, Case COMP D3/34493, *DSD*, para. 112, (2001) OJ L166/1; affirmed in GC, Case T-151/01, *DerGrünePunkt – Duales System DeutschlandGmbH v. European Commission*, EU:T:2007:154 and CJEU, Case C-385/07 P, EU:C:2009:456.
[14] CJEU, Case C- 27/76, *United Brands Company and United Brands Continental BV v. Commission of the Euopean Communities*, EU:C:1978:22, para. 190.
[15] European Commission, Case COMP/E-2/36.041/PO*, Michelin (Michelin II)*, paras. 220-221 and 223-224, (2002) OJ L143/1, where the Commission further argued that, "[the discount scheme] was unfair not only because the dealers were placed in a weak psychological position during negotiations, but also because, during the negotiations, they were not able to base themselves on a reliable estimate of their cost prices and thus to determine their business strategy freely."

As has been noted in the literature,[16] if this interpretation of Article 102(a) is followed, the clauses subject to scrutiny in the *Alsatel* case may have been found to be unjustifiably burdensome, although the case was not resolved on the grounds that the firm in question held a dominant position.[17] Specifically, in that case the parties objected that "the fact that the price … is not determined but is unilaterally fixed by the [dominant firm] and the [the fact that the] renewal of the contract for a 15-year term [was automatic] may constitute unfair trading conditions prohibited as abusive practices."

Taken together, there is scope to argue that the notion of unfairness under Article 102(a) captures clauses that are *unjustifiably unrelated* to the purpose of the contract, *unnecessarily limiting* the freedom of the parties, *disproportionate*, *unilaterally imposed* or *seriously opaque*. Therefore, the GCA could be correct in taking the view that a dominant firm exploits its market position when, in order to offer its services, it asks for more data than is necessary. In particular, the Bundeskartellamt could arrive at this conclusion without giving any consideration to the minimization principle dear to EU data protection law.

Nevertheless, there is an outstanding issue. If we suppose that the abusiveness of Facebook's practice is actually rooted in its opacity, what should the remedy against it be? Should it be disclosure in order to ensure user awareness – a typical privacy-related (or consumer protection-related) remedy which addresses a structurally inherent privacy (or consumer-protection) concern? However, would such a remedy prevent data accumulation?

---

[16] P. Akman, *The concept he Concept of Abuse in EU Competition Law,* Hart Publishing, 2012, 155-157.

[17] CJEU, Case C-247/86, *Société alsacienne et lorraine de télécommunications et d'électronique (Alsatel) v. Novasam SA*, EU:C:1988:469, paras. 9-10. As to the unfairness of contractually clauses unilaterally imposed, see again *Michelin II, supra* note 15, para. 265, where the Commission observed that, "[the discount scheme] was unfair since, though it appeared to be based on an agreement, it amounted in fact to a requirement unilaterally imposed by the manufacturer to increase purchases of Michelin tyres on the market."

Would it prevent Facebook from using "[these data] to optimize its offer and tie more users to its network […] to the detriment of other providers of social networks"? Would it prevent Facebook from "becoming more and more indispensable for advertising customers […with…] [a] potential for competitive harm on the side of the advertising customers?" This remedy would only guarantee *fair* data collection – which is clearly an important result. However, it would not exclude the possibility that, through such data collection, Facebook could make its dominant position harder to challenge.

After all, when there is a mismatch between the goal pursued and the tools available to pursue it, there are two viable options: either enforcers refrain from intervening or they impose a forced interpretation of a particular provision, such as Article 102(a), and end up with remedies that cannot genuinely realize the goal pursued, while incurring the potential drawbacks of this forced interpretation.

3.3 Facebook's conduct as an unfair method of competition: are there grounds for the application of Section 5 of the FTC Act?

On the basis of the EU experience with Article 102(a), one might wonder whether any U.S. federal rules could be used to tackle dominant firms' unfair practices. Section 5 of the FTC Act seems to be the best candidate. Indeed, Section 5 has been also considered as a "bridge toward convergence" with Europe.[18]

Throughout the history of the Federal Trade Commission, the scope of Section 5 has been the subject of considerable debate within the antitrust community, involving practitioners,

[18] A.A. Foer, 'Section 5 as a Bridge Toward Convergence', 8 *Antitrust Source* 1 (2009).

legal scholars, and enforcers alike.[19] In declaring unlawful all unfair methods of competition, Section 5 provides a very broad mandate for enforcement, empowering the FTC to "proscribe an unfair competitive practice, even though the practice does not infringe either the letter or the spirit of the antitrust laws," and "to proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition."[20] Thus, the main discussion has concerned the boundaries and range of possible interpretations of Section 5, namely how the FTC exercises its discretion in enforcement, the scope of free-standing Section 5 claims, and their relationship with Section 2 of the Sherman Act.

Some commentators have pointed out the virtues of Section 5, as it enables the FTC to challenge anticompetitive conduct where the Sherman Act cannot, and it provides a faster, lighter-touch and better suited tool for resolving unsettled questions of law by sheltering infringers from follow-on litigation and treble damages.[21] In contrast, others report an undisciplined expansion of Section 5, which has launched the Commission into "a sea of uncertainty,"[22] and thus invoke principles that could limit the scope of Section 5 and define

[19] In 2008 the FTC held a workshop on "Section 5 of the FTC Act as a Competition Statute" seeking the views of the legal, academic, and business communities in order to explore the scope of the prohibition of unfair methods of competition. Materials and comments are available at https://www.ftc.gov/news-events/events-calendar/2008/10/section-5-ftc-act-competition-statute .

[20] *FTC v. Sperry & Hutchinson Co.,* 405 U.S. 233, 239 (1972).

[21] See, e.g., T. Wu, 'Section 5 and 'Unfair Methods of Competition': Protecting Competition or Increasing Uncertainty?', Columbia Law and Economics Working Paper No. 542 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2760162; J.T. Rosch, 'The Great Doctrinal Debate: Under What Circumstances is Section 5 Superior to Section 2?', remarks before the New York State Bar Association Annual Antitrust Conference New York City, New York, January 27, 2011, https://www.ftc.gov/sites/default/files/documents/public_statements/great-doctrinal-debate-under-what-circumstances-section-5-superior-section-2/110127barspeech.pdf .

[22] M.K. Ohlhausen, 'Section 5 of the FTC Act: principles of navigation', 2 *Journal of Antitrust Enforcement* 1 (2014).

unfair competitive practices.[23] Moreover, low settlement costs will deter defendants from testing the validity of the FTC's case in court, as they will prefer to sign consent agreements that are premised on a pure Section 5 theory, thereby avoiding litigation with an uncertain outcome.[24]

In order to face down these concerns (which have mainly been raised with regard to the application of the Section 5 in the context of the standard-setting process), the FTC released a Statement in 2015 describing the underlying principles that guide its Section 5 enforcement policy.[25] In an attempt to provide guidance, the Statement sets out three principles to which the FTC must adhere when challenging unfair methods of competition on the standalone basis of Section 5: a) the Commission will be guided by the public policy underlying the antitrust laws, namely the promotion of consumer welfare; b) the Commission will evaluate the act or practice under a framework similar to the rule of reason (that is, an act or practice challenged by the Commission must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated

[23] See J.M. Rybnicek and J.D. Wright, 'Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines', 21 *Geo. Mason L. Rev*. 1287, 1288 and 1312 (2014), arguing that "the failure to identify what precisely comprises an unfair method of competition remains an unfortunate and persistent black mark on the Commission's record. … In practice, the scope of the FTC's authority to prosecute unfair methods of competition is as broad or as narrow as a majority of the commissioners believes it to be. Indeed, the Commission's interpretation of Section 5 can vary significantly as the composition of its membership changes over time." In same vein, J.C. Cooper, 'The perils of excessive discretion: the elusive meaning of unfairness in Section 5 of the FTC Act', 3 *Journal of Antitrust Enforcement* 87, 90 (2015): "Not only does the FTC lack meaningful external constraints on its discretion to define Section 5, there are no internal restraints on FTC actions under Section 5. … The Commission's discretion under Section 5 is in the Zeitgeist of the antitrust policy community."

[24] Cooper, *supra* note 23, 89.

[25] Federal Trade Commission, 'Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act', 13 August 2015, https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf . However, see M.K. Ohlhausen, Dissenting statement, https://www.ftc.gov/public-statements/2015/08/dissenting-statement-commissioner-ohlhausen-ftc-act-section-5-policy, holding that the guidance provides "more questions than answers."

cognizable efficiencies and business justifications); c) the Commission is less likely to challenge an act or practice as an unfair method of competition on a stand-alone basis if enforcement of the Sherman or Clayton Act is sufficient to address the competitive harm arising from the act or practice.

Therefore, considering how the *Facebook* case might be handled in the U.S. under Section 5 of the FTC Act, it is apparent that the framework outlined by the policy Statement will require the fulfilment of conditions that are informed by economic analysis, and which are different from and narrower than those defined under EU case law. In fact, instead of relying on the allegation that Facebook's terms and conditions are unjustifiably unrelated to the purpose of the contract, unnecessarily limit the freedom of the parties, are disproportionate, unilaterally imposed, or seriously opaque, potential U.S. proceedings under Section 5 will be guided by a policy goal that is consistent with traditional antitrust laws, namely the protection of consumer welfare. Indeed, the Statement excludes the consideration of non-competition goals from the analysis.[26] Moreover, it has been suggested that, in aligning Section 5 with other antitrust laws, the Statement makes clear that not all consumer harm is cognizable under Section 5, since not all forms of consumer harm result in cognizable antitrust injury.[27] For example, since in *Trinko* the Supreme Court held that excessive pricing did not constitute an antitrust violation, Section 5 should not be

[26] J.D. Wright and A. Diveley, 'Unfair Methods of Competition after the 2015 Commission Statement', 15 *Antitrust Source* 1, 5-6 (2015).
[27] Wright and Diveley, *supra* note 26, 8.

interpreted as extending to excessive pricing because that conduct falls outside the scope of antitrust law.[28]

However, Section 5 of FTC Act is not limited to the prohibition of unfair methods of competition. The provision also contains a second prong concerning "unfair or deceptive acts or practices in or affecting commerce." This is the primary source of authority for FTC privacy enforcement, so much so that the Commission is viewed not only as a consumer protection authority, but also as the *de facto* federal data protection authority.[29]

Therefore, these various powers derived from Section 5 allow the FTC to protect consumers directly by addressing a wide array of practices affecting consumers, including those associated with the development of new technologies and business models. In this regard, Section 5 of the FTC Act resembles the EU Directive concerning unfair business-to-consumer commercial practices.[30] In fact, according to EU provisions, the prohibition of unfair commercial practices covers unfair, misleading and aggressive commercial practices. These are practices capable of distorting consumers' economic behaviour by, for instance, appreciably impairing their ability to make an informed decision, thereby causing consumers to make a transactional decision that they would not otherwise have made.[31] In particular, practices (actions and omissions) that contain false information or omit (or provide in an unclear, unintelligible, ambiguous or untimely manner) information that

[28] *Verizon Communications, Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398 (2004).
[29] D.J. Solove and W. Hartzog, 'The FTC and The New Common Law of Privacy', 114 *Columbia Law Review* 583 (2014).
[30] Directive 2005/29/EC, (2005) OJ L 149/22. See also European Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices', SWD(2016) 163 final.
[31] Directive 2005/29/EC, *supra* note 30, Articles 2 and 5.

consumers need in order to take an informed transactional decision are considered to be misleading.[32]

From this perspective, if a social network fails to inform users that their personal data will be collected and processed for economic purposes, it could be argued that the social network is omitting material information that consumers need to take an informed transactional decision. In same vein, the FTC has developed a theory that the collection of personal information in a deceitful manner constitutes an unfair act.[33]

In sum, if the various prongs of Section 5 are considered, the FTC is allowed to pursue violations of various antitrust and consumer protection laws. However, after taking into consideration the different standards that the enforcer must satisfy, it is apparent that the appropriate way to handle the *Facebook* case would be to consider its conduct to be an unfair or deceptive practice. Under these circumstances, from an enforcement perspective an unfair practice procedure provides 'competitive' advantages compared to an antitrust case, since the relevant investigative standards are lower (for instance, there is no need to define the relevant market and to demonstrate market power). Moreover, the remedy would be the same even if the enforcer decided to proceed with an antitrust case. Aside from a pecuniary fine, the only remedies available against Facebook's conduct are those aimed at increasing user awareness by requiring it to modify its terms and conditions and to fully disclose the way in which data are gathered and processed. Hence, an antitrust investigation

[32] Directive 2005/29/EC, *supra* note 30, Articles 6 and 7.
[33] Solove and Hartzog, *supra* note 29, 641. The Authors remark (at 667) how the FTC has moved beyond enforcing broken promises of privacy to substantive privacy protections, also challenging broken expectations of consumer privacy. See also G.S. Hans, 'Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era', 19 *Mich. Telecomm. & Tech. L. Rev.* 163 (2012).

would solve privacy concerns and would at most guarantee *fair* data collection, but it would not address the issue of data accumulation and thus would not prevent the alleged entrenchment of Facebook's dominant position.

In the same way, the EU framework sets out rules forbidding unfair commercial practices, which appear to be better suited to dealing with the lack of transparency and information asymmetries in the user-platform relationship with regard to online privacy. In keeping with this position, the Italian competition authority, acting under the consumer protection law, recently closed proceedings with a finding that Facebook's conduct amounted to an unfair commercial practice, and thus a violation of the Consumer Code rather than of antitrust law.[34] In the Italian case, Facebook was fined because it forced WhatsApp Messenger users to accept its new terms and conditions in their entirety, in particular with regard to the sharing of their personal data with Facebook by allegedly making them believe that it would have otherwise been impossible to continue using the service.

It is worth noting that the German landscape is different, which may be the main explanation for the antitrust procedure in the *Facebook* case. In Germany, unfair commercial practices fall under the scope of the Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb, last amended in 2016) and are thus a matter of civil law. Consequently, market participants (competitors, consumers and associations) have the right to object to unfair practices before the civil courts and there is no state authority that monitors the market in order to ensure compliance with the provisions of the Unfair Competition Act. Therefore, unlike the FTC and other European antitrust enforcers, the

[34] Italian Competition Authority, 11 May 2017, Case PS10601, *supra* note 4.

Bundeskartellamt has no mandate to challenge unfair commercial practices, which may have induced the German Authority to handle the case under antitrust law.

4. The privacy-antitrust interface.

Until now, scholars have explored the privacy-antitrust interface from two complementary perspectives. On the one hand, they have first considered whether, in an economy where data are collected in exchange for free services, low levels of privacy could be indicative of high levels of market power. Second, they have discussed whether antitrust law can make up for the pitfalls of privacy law. For example, it has been asked whether a practice that renders a product less privacy-friendly could be considered to be anticompetitive, or whether antitrust law could intervene to protect privacy-enhancing technologies. Additionally, it has been asked whether a specific business practice that violates privacy law could also be prosecuted as an antitrust violation. On the other hand, the *Facebook* case suggests that the privacy-antitrust interface can be interpreted in the other "direction", that is, by considering whether privacy arguments can support a finding of an antitrust violation. This "bidirectional" analysis will be developed in the following paragraphs.

4.1 Privacy and market power.

Thus far, scholars have attempted to establish a link between market power and personal data by pursuing two different lines of reasoning.

The first one is centred on the business model of multi-sided media platforms, such as Facebook and Google Search. On this view, multi-sided media platforms do not offer their services for free,[35] but rather in exchange for attention[36] and personal data.[37] While attention is offered to advertisers, personal data are used by the platforms themselves not only to develop tailored advertising, but also to develop more accurate algorithms and enhanced user services and experiences. Therefore, in the digital economy, attention and personal data have acquired a clear role and value,[38] although this value is difficult to measure and consumers are not fully aware of it.[39] More importantly, today it is almost

[35] See, e.g., V. Zeno-Zencovich and G. Giannone Codiglione, 'Ten Legal Perspectives on the "Big Data Revolution', 23 *Concorrenza e Mercato* 29, 40-41 (2016), observing that, "[o]ne had only to look at the business model to understand the reality, which now has become clear to everybody, except for Facebook which insists on using as a motto on its home page "It is free, and will always be", a phrase which, at its least, is a misleading and deceptive commercial statement, as one can easily see if one takes the time to read the general terms and conditions of service."

[36] See D.S. Evans, 'Attention Rivalry Among Online Platforms', 9 *J. Competition L. & Econ.* 313 (2013); and J.M. Newman, 'Antitrust in Zero-Price Markets: Foundations', 164 *U. Pa. L. Rev.* 149, 172 (2015), writing that, "[f]or consumers in many zero-price markets, money is replaced by attention — these consumers literally pay attention. Where advertisements are solicited, consumers exchange their attention to advertisements for corresponding products. And because such attention costs are also the media of exchange, such transactions allow for economic gains from trade. These attention costs are market-signaling. Transactions where attention serves as currency are "trade" or "commerce" under the meaning of the antitrust laws."

[37] See D.S. Evans, 'The Antitrust Economics of Free', 7 *Competition Policy International* 71, 82 (2011), observing that, "[p]rofit maximizing firms do not provide products for free unless it helps them make money somewhere else;" Newman, supra note 36, 165; I. Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms', 38 *World Competition* 473, 477 (2015), observing that "[i]n return for giving users free access to their functionalities, providers of search engines, social networks and e-commerce platforms gather data about their profile, interests and online behaviour." Furthermore, A. Goldfarb and C. Tucker, 'Privacy Regulation and Online Advertising', 57 *Mgmt. Sci.* 57 (2011).

[38] See H.A. Shelanski, 'Information, Innovation, and Competition Policy for the Internet', 161 *U. Pa. L. Rev*. 1663, 1678 (2013), writing that, "[w]hile customer information is perhaps always valuable for a business, it is even more so for digital platforms. There are two main reasons for this: (1) digital platforms generally have much greater access than conventional businesses to a broad range of information about their consumers, and (2) digital businesses may be better able to process and use that data for a variety of purposes." See, also, R.T. Rust, P.K. Kannan, and N. Peng, 'The Customer Economics of Internet Privacy', 30 *Journal of the Academy of Marketing Science* 455, 456 (2002), arguing that, "while the costs of obtaining and processing information about consumers are decreasing with the advances in technology, the value of consumer information for businesses has been increasing."

[39] See, e.g., C. Argenton and J. Prüfer, 'Search Engine Competition with Network Externalities', 8 *J. Competition L. & Econ*. 73 (2012); S. Vaidhyanathan, *The Googlization of Everything (And Why We Should*

universally accepted that personal data are the currency of the Internet,[40] so much so that the quantity of personal data exchanged for the platforms' services can be conceptualized as the implicit prices of those services.[41]

That said, it is only a short step to link market power to these "prices quantified in terms of data." First, it can be claimed that multi-sided media platforms with monopoly power exercise that power by extracting more data than they could obtain under conditions of perfect competition. Second, it can be argued that it is precisely when these platforms hold big data that there is scope to conclude that they hold significant market power. In other words, one could maintain *both,* that the big data of platforms signal their monopoly power, *and* that platforms with monopoly power extract supra-competitive amounts of personal data, just as in the analogue economy they would extract supra-competitive prices.[42]

However, this reasoning attracts three criticisms, at least. First, it is hard to identify a competitive quantity of consumer data (the quantity of personal data that firms would naturally collect in competitive markets). Whereas in the analogue economy the

---

Worry), University of California Press (2011), 3, observing that, Google users allow their "fancies, fetishes, predilections, and preferences to be captured by Google and resold to the company's advertisers."

[40] See, e.g., M.S. Gal and D.L. Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement', 80 *Antitrust Law Journal* 521 (2016); Newman, *supra* note 36; and Shelanski, *supra* note 38.

[41] See D. Auer and N. Petit, 'Two-Sided Markets and the Challenge of Turning Economic Theory into Antitrust Policy', 60 *The Antitrust Bulletin* 426, 443 (2015), where the Authors, dealing with SSNIP, observe that, "Google charges an implicit price on users, which consists in extracting personal data from them" to then maintains that, "it is unclear how to operationally simulate the effects on demand of a small but significant increase in data extraction." See also A. Gebicka and A. Heinemann, 'Social Media & Competition Law', 37 *World Competition* 149, 165 (2014); F.A. Pasquale, 'Privacy, Antitrust, and Power', 20 *Geo. Mason L. Rev.* 1009, 1022 (2013), observing that, "[d]ominant firms see little to no reason to compete to improve their privacy practices when users are so unlikely to defect. A lemons equilibrium prevails;" J. Whittington and C.J. Hoofnagle, 'Unpacking Privacy's Price', 90 *N.C. L. Rev.* 1327 (2012); and A.P. Grunes, 'Another Look at Privacy'*,* 20 *Geo. Mason L. Rev.* 1107, 1123 (2013).

[42] By moving along this path, in the EU one could even argue that, like excessive prices, an unjust amount of the extracted user data equals an exploitative abuse within the meaning of letter (a) of Articles 102. See Gebicka and Heinemann, *supra* note 41, 165.

competitive level of the market price can be approximated by looking at marginal costs (or other measures of costs), in the digital economy no one has quantified the benchmark for assessing the competitive quantity of personal data. Even data protection law cannot help in this regard; it only regulates the ways in which personal data are collected, but does not say anything about the quantities of personal data that individuals may transfer to firms.

Second, the analogy between personal data and currency seems to be unfounded. Money has a nominal value that is equal for all people, whatever the marginal utility each consumer derives from a unit of money. By contrast, the value of data, including personal data, not only varies according to the data considered,[43] but also cannot be measured in nominal terms.[44] It mirrors the utility that individual economic agents derive from the data themselves. Thus, data value does not lend itself to any form of inter-personal comparison, and cannot become a tool for measuring aggregated, or 'market', phenomena.[45]

Finally, it must be observed that the above reasoning and the resulting link between market power and personal data has been elaborated, as previously stated, in relation to multi-sided

[43] See Graef, *supra* note 37, 483, stating that "[w]hile some data including name and date of birth has lasting value and only has to be collected once by a specific entity, other types of data, such as the search queries that users have been looking for, are more transient in value and are relevant over a shorter period of time."

[44] Nonetheless, the growing demand for consumer data may lead to a transformation of privacy into a tradable product engendering various business offerings that, for instance, allow companies to purchase data directly from individuals or require consumers to pay an additional fee to prevent their data from being collected and mined for advertising purposes: see S.A. Elvy, 'Paying For Privacy And The Personal Data Economy', 117 *Columbia Law Review* 1369 (2017). See also Federal Communications Commission, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 2016, proposing to replace the current opt-out mechanism with an opt-in system (the broadband providers would be required to obtain the prior express consent of users before sharing information with third parties or use the same for purposes other than those relating to the service offered and, thus, for example, for targeted advertising) and calling into question the legitimacy of business models that offer financial incentives in exchange for users' consent to use and share confidential information with third parties.

[45] M. Sousa Ferro, 'Ceci N'est Pas un Marché': Gratuity and Competition Law', *Concurrences* 1 (2015).

media platforms, with the ultimate purpose of appreciating their market power.[46] However, other tools and variables can be used to this end, such as: (i) the price of advertising space; (ii) the amount of advertising space imposed on users (i.e., the amount of users' attention required);[47] and (iii) the quality of the "free" products and services. Therefore, one might wonder whether the link described between market power and personal data is really necessary, or is rather a brilliant, though unworkable, construct.

The second line of reasoning aimed at establishing a link between market power and personal data disregards the volumes of data collected by firms. It is rather focused on the notion that the more data firms hold, the lower the quality of their products/services. Therefore, one could argue either that the popularity of products and services that are not privacy-friendly *signals* the existence of firms with (significant) market power or that firms with monopoly power *exercise* it, by lowering the 'privacy-friendliness' of their products and services.

However, as will be noted in the next section, this thesis holds true if (or when) it is the case that a reduction in privacy entails a reduction in quality that, in turn, entails a reduction in consumer welfare. Therefore, in order to apply such an approach, one should at least test whether there is a market for privacy-sensitive consumers that an operator is somehow

[46] See B.J. Koops, 'The trouble with European data protection law', 4 *International Data Privacy Law* 250 (2014), remarking that business models that generate revenue from user-data-based profiling and advertising are the most prominent two-sided strategies in the online context.

[47] I. Reidel, 'The Taylor Swift Paradox: Superstardom, Excessive Advertising and Blanket Licenses', 7 *N.Y.U. J.L. & Bus.* 731, 748 (2011), observing that, "[a] station with market power over audiences will be able to increase advertising time, and one with power over advertisers will likely be able to increase advertising prices by reducing available air-time for ads;" and C.T. Mooney, 'Market Power and Audience Segmentation Drive Radio Advertising Levels', (2010), https://editorialexpress.com/cgi-bin/conference/download.cgi?db_name=IIOC2010&paper_id=203.

stifling.[48] Indeed, there could be well-educated consumers who, for example, prefer zero-price, personalized, and quick services rather than privacy-friendly, non-accurate, and slow services.

4.2 Privacy and anticompetitive business practices.

Several theories of harm have been proposed in order to comingle privacy and antitrust issues, and also to ask antitrust law to intervene in order to compensate for gaps within privacy law.

Two of these may be traced back to an observation made a few years ago by the former FTC Commissioner, Pamela Jones Harbour. In her dissenting statement concerning the *Google/DoubleClick* merger, she argued that mergers between companies that hold big data would, by increasing their joint data booty, allow the entity resulting from the merger to dominate the "database of intentions" by possessing even more tools for profiling individuals and encroaching upon their privacy.[49] In addition, she observed that network effects and the other structural features characterizing digital markets strengthen the market power of digital platforms, and decrease their incentives to compete to offer better goods, such as privacy-friendly services.[50] However, the alleged lack of incentives to improve goods is not specific to digital markets or digital business models. In addition, no firm is

[48] See, e.g, D.D. Sokol and R. Comerford, 'Antitrust and Regulating Big Data', 23 *Geo. Mason L. Rev.* 1129 (2016); G.A. Manne and R.B. Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework', 5 *CPI Antitrust Chronicle* (2015); J.C. Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity', 20 *Geo. Mason L. Rev.* 1129 (2013).

[49] P.J. Harbour, Dissenting statement, In the matter of *Google/DoubleClick,* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf .

[50] P.J. Harbour and T.I. Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets', 76 *Antitrust Law Journal* 769 (2010).

under an antitrust obligation to provide the absolute best quality product that it can, even if it does not maximize profits.[51] Moreover, as a general matter, antitrust law does not intervene in relation to market features and structure. Thus, if network effects disincentivize digital platforms from producing privacy-friendly services, then economic regulation, rather than antitrust law, should intervene.[52]

Antitrust law could also intervene against a merger suppressing a privacy-enhancing technology or against a boycott targeting the producers of privacy-friendly products/services. However, there would not be anything heterodox in such an approach. A traditional case-by-case analysis would be enough to establish whether there are markets for those products/services or technologies (i.e., if there are enough consumers who are privacy-sensitive). On the contrary, if we wanted to increase the number of privacy-sensitive consumers, we should act through regulation and once again refrain from engaging in any antitrust action.

Furthermore, another theory of harm that brings together antitrust and privacy issues has been elaborated by several law scholars and recently endorsed by the Canadian Competition Bureau.[53] It maintains that a practice that renders a product/service less privacy-friendly is anticompetitive. In fact, it would appear that this question can be answered in the affirmative *if and only if* it is true that a privacy reduction entails a quality

[51] Sokol and Comerford, *supra* note 48, 1142.
[52] Koops, *supra* note 46, 258.
[53] See Canadian Competition Bureau, 'Big data and Innovation: Implications for Competition Policy in Canada', Discussion Paper (2017), http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04304.html , 23; M.E. Stucke and A. Ezrachi, 'When Competition Fails to Optimise Quality: A Look at Search Engines', 18 *Yale Journal of Law and Technology* 70 (2016); A.P. Grunes and M.E. Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data', 14 *Antitrust Source* 1 (2015); Grunes *supra* note 41; Pasquale, *supra* note 41; P. Swire, 'Protecting Consumers: Privacy Matters in Antitrust Analysis', Center for American Progress, 2007.

reduction that, in turn, entails a consumer welfare reduction. However, this chain of implication does not always hold. Privacy policy has focused on the idea that, with enough transparency and enough choice, consumers would make better privacy decisions. However, the notion that well-educated consumers would be privacy-sensitive should not be taken for granted.[54] Likewise, it cannot be taken for granted that if consumers knew the real value of their personal data they would stop using digital platforms or, more realistically, would pay for Internet services rather than giving personal data away.[55] Whilst the quality of goods may decrease for some consumers when they result from the analysis of personal data, other users might prefer non privacy-friendly goods because they are more interested in other features of those services. Therefore, the net quality effect and the net consumer welfare effect of practices that encroach upon privacy should not be assumed to be negative. Rather, it is necessary to perform a case-by-case analysis. Otherwise, if we were to take that chain of implications for granted, then we would assume that 'privacy-

[54] On the difficulties in establishing consumer preferences over data use, see S. Athey, C. Catalini, and C. Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk', NBER Working Paper No. 23488 (2017), showing that, when expressing a preference for privacy is essentially costless, consumers are eager to express such a preference, but when faced with small costs this taste for privacy quickly dissipates. The experiment conducted by the authors investigated whether undergraduates at MIT would be willing to release what might be considered very personal data regarding their friends' contact information. On average many of them were willing to release the data; there was a subset of students who stated a preference for privacy and did not release the data; however, if this set of students were offered a slice of cheese pizza in exchange for this data, then they were as willing as the rest of the student population to share this information. On the privacy paradox see S. Kokolakis, 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon', 64 *Computers & Security* 122 (2017); A. Acquisti, C. Taylor, and L. Wagman, 'The Economics of Privacy', 54 *Journal of Economic Literature* 442 (2016).

[55] See Körber, *supra* note 8, 9, arguing that the theory of the "ignorant Internet user" seems far too generalized: "It is more likely that most users know that they are disclosing their data and that, even on the Internet, nothing is for free. … Furthermore, the thesis that customers' data are considerably more valuable than the services provided by companies like Google and Facebook is a mere allegation lacking verifiable proof." In addition, whether consumers are actually aware of the value of their personal data is a matter of education and one could legitimately wonder if antitrust law is in the best position to tackle such an issue.

friendliness' is a goal of antitrust law.[56] This, however, is a choice that should be left to policy makers, and not to the courts or the authorities.

Finally, as noted above, at the outset the *Facebook* procedure seems to embrace a fifth privacy-driven theory of antitrust harm, which has also been supported by the French Autorité de la Concurrence and the Bundeskartellamt in a recent position paper.[57] The two national competition authorities argued that, "even if data protection and competition laws serve different goals, privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature. … [T]here may be a close link between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings."[58] They added, "privacy policies could be considered from a

[56] M.K. Ohlhausen and A.P. Okuliar, 'Competition, Consumer Protection, and The Right [Approach] to Privacy', 80 *Antitrust Law Journal* 121 (2015): "[T]he application of competition law is appropriate only where the potential harm is grounded in the actual or potential diminution of economic efficiency. …. Attempting to unify the competition and consumer protection laws creates needless risks for the Internet economy and could destabilize the modern consensus on antitrust analysis, again pulling it away from rigorous, scientific methods developed in the last few decades and reverting back to the influence of subjective noncompetition factors. Indeed, trying to expand competition law as some have proposed better reflects legal thinking in 1915, not 2015. Although privacy can be (and is today) a dimension of competition, the more direct route to protecting privacy as a norm lies in the consumer protection laws." See also Körber, *supra* note 8, 29-30: "The application of competition law should require a connection between the conduct and competition, as well as at least normative causation between market dominance and abusive conduct. It is not the infringement of another law as such that is relevant for purposes of competition law." Moreover, see J. Kennedy, 'The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown', Information Technology & Innovation Foundation (2017), 16, http://www2.itif.org/2017-data-competition.pdf , stating that, "[t]he market for privacy is imperfect. Therefore, we should not expect it to solve all the privacy preferences of all users, since those preferences are so diverse. But this does not mean that decisions on antitrust issues should be driven by privacy concerns or that privacy laws are inadequate. There is no evidence that any lack of competition in providing services that feature greater privacy protections is due to entry barriers rather than a lack of consumer demand. Therefore, regulators should apply traditional competition analysis to the competitive aspects of a problem and use privacy laws to deal with privacy issues."

[57] Autorité de la concurrence and Bundeskartellamt, 'Competition Law and Data', report, 2016. See also European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', preliminary opinion, 2014.

[58] Autorité de la concurrence and Bundeskartellamt, *supra* note 57, at 23-24. See also W. Kerber, 'Digital

competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services." In keeping with in its preliminary assessment of the *Facebook* case, the Bundeskartellamt declared that, "[w]here access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is no longer only relevant for data protection authorities. It becomes a relevant question for the competition authorities, *too*." Therefore, in 2016 it seemed that the Bundeskartellamt took the view that a practice which violates data protection law might also encroach upon competition and infringe competition law; this author has argued that this possibility might well arise in accordance with the traditional boundaries of antitrust law if antitrust authorities conclude, on a self-standing basis, that a competition violation has occurred.

However, until now, both the EU courts and the European Commission have endorsed a hands-off approach to privacy issues: they have never used competition law to defend individuals' control over their personal data and digital identities.

In *Asnef-Equifax*, the Court of Justice held that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection."[59] More recently, the Commission endorsed the very same approach in *Facebook/WhatsApp*,[60] after the FTC

Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection', 7 *GRUR Int* 639 (2016), invoking a more synergic approach that merges together data protection law, competition law, and consumer protection law, in order to address properly the concerns about privacy in the digital economy.

[59] CJEU, Case C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v. Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, EU:C:2006:734, para. 63.

[60] European Commission, 3 October 2014, case COMP/M.7217, para. 164: "Any privacy-related concerns

maintained in *Google/DoubleClick* that "regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry."[61] Also, in the very recent decision concerning the *Microsoft/LinkedIn* merger, the Commission observed that privacy related concerns as such do not fall within the scope of EU competition law, and that "[the] data combination could only be implemented by the merged entity to the extent it is allowed by applicable data protection rules."[62]

In both *Facebook/WhatsApp* and *Microsoft/LinkedIn*,[63] the Commission has acknowledged the role that privacy may play as a driver of consumer choice, and thus as a parameter for competition between digital platforms. However, this acknowledgment has nothing to do with the use of antitrust law to solve some data protection law issues. Moreover, in *Microsoft/LinkedIn* the Commission highlighted that the data protection regulation "may further limit Microsoft's ability to have access and to process its users' personal data in the future since the new rules will strengthen the existing rights and empowering individuals with more control over their personal data."[64] Again, the Commission chose to refer to privacy rules in order to protect individuals' personal data and digital identities.

Nevertheless, it seems that the Bundeskartellamt has now endorsed another approach, or at least is moving in another 'direction'. The GCA does not look to antitrust law in order to rescue privacy, but rather to privacy law in order to rescue antitrust law.

---

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

[61] Federal Trade Commission, 20 December 2007, case 071-0170, 2.

[62] European Commission, 6 December 2016, *Microsoft/LinkedIn*, case M.8124, para. 177.

[63] *Facebook/WhatsApp*, *supra* note 60, para. 87; *Microsoft/LinkedIn*, *supra* note 62, nt. 330.

[64] *Microsoft/LinkedIn*, *supra* note 62, para. 177.

4.3 Another tile for the privacy-antitrust interface: privacy law to the rescue of antitrust law.

In the *Facebook* investigation, the Bundeskartellamt decided to evaluate Facebook's conduct independently of any privacy infringement, though it grants that such conduct could also violate the principles of data protection.

The GCA is clearly concerned about the potential market foreclosure effect deriving from Facebook's data accumulation strategy.[65] Facebook is considered to be a dominant player that is taking advantage of superior access to an "essential factor" for competition in data-driven markets (i.e. users' personal data), and is trying to enhance this advantage through the 'whole Facebook package' offering. Indeed, until now the procedure concerns only 'off Facebook' data (i.e., user data obtained from third party sources). As explained in the preliminary assessment, Facebook can use these data to optimize its offer and tie more users into its network, thereby increasing identity-based network effects to the detriment of both other providers of social networks and advertisers who are faced with a dominant supplier of advertising space.

Nonetheless, in order to consider Facebook's data accumulation as being anticompetitive, enforcers have to apply antitrust standards and hypothesise that data accumulation in itself

[65] See Kennedy, *supra* note 56, 18, arguing that, "[w]hen pointing to the competitive threats raised by amassing large amounts of data, advocates of expanding competition review often raise privacy concerns. Faced with the fact that data-rich platforms often offer users their services for free, they fear that the collection of large amounts of data will still shift market power from consumers to companies, forcing the latter to give up valuable data. The analysis is confused, however, by the fact that many of these advocates seem to value data privacy and security much more highly than does the general public. The true source of their frustration is not that the privacy authority lacks the power to impose higher safeguards, but that it won't."

constitutes harm. Moreover, as illustrated in the previous sections, in the case at issue it is quite difficult to rely on antitrust provisions related to exclusionary practices. Therefore, the Bundeskartellamt has opted for an exploitative abuse claim under Article 102(a), arguing that Facebook is imposing unfair conditions by forcing users to choose between accepting the whole Facebook package or not using Facebook at all. Furthermore, as we have seen it is hard to establish a self-standing violation of Article 102(a) without taking account of the fact that users' lack of awareness of how their personal data will subsequently be used is the harmful outcome alleged against the social network.

At this point, data protection principles come to the rescue of antitrust enforcement. Evaluating Facebook's terms and conditions, the GCA has declared that it is *also* applying privacy principles, and it stated that the damage for users caused by Facebook's practice consists of a "loss of control." Indeed, although users have to expect some level of processing of their data if they use such a free service, they cannot expect that the data generated when they use services other than Facebook will be added to their Facebook account on this scale. As noted above, any remedy aimed at increasing user awareness and/or limiting their loss of control over their digital identities would solve this twofold privacy concern, without addressing the antitrust issue associated with data accumulation.

5. Concluding remarks.

Within digital markets, the emergence of multi-sided media platforms has occurred in parallel with the success of business models that essentially revolve around the collection and use of personal data, generating revenue from user-data-based profiling and

advertising.[66] Within such a context, data protection rules do not appear to be very effective.[67] Thus, the main concerns in this field relate to user awareness of platforms' ability to trace digital conduct in order to create detailed profiles (which can then be made available to behavioural advertisers), and also users' ability to control their digital identities.

Alongside mere privacy issues, from a market perspective the emergence of the data-driven economy is subject to two different, although not necessarily conflicting, interpretations. Companies may use data in order to become more efficient and to improve their products and offerings. At the same time, the aggregation and commercial use of large quantities of data may give those companies a competitive advantage over rivals. Relating to the latter point, there are concerns that, strengthened by (direct and indirect) network effects, data may represent significant barriers to entry and may thus foreclose the market, providing their holders with business opportunities that are not available to others. As the argument goes, dominant firms that collect and aggregate data (including personal data) may entrench

[66] See Koops, *supra* note 46, 251-252, highlighting the limits of data protection regulation in the online context since consent is no more as an effective protection tool: "Often, there is little to choose: if you want to use a service, you have to comply with the conditions—if you do not tick the consent box, access will be denied. And there are no good alternatives: most other providers of the service you want apply the same practice and similar data-processing conditions, and with the most-used major services, such as Facebook, Google, or Twitter, there is no realistic alternative for most people. Underlying this is the fact that there are practically no alternative business models that generate revenue from other sources than user-data-based profiling and advertising." See also Körber, *supra* note 8, 18, suggesting that a well-designed data protection law should – like a well-designed competition law – presume the primacy of informed consumer choice over paternalism and it should provide users with "help to help themselves," reinforcing their data sovereignty.

[67] See Grunes and Stucke, *supra* note 53, 12: "The consensus is that the current notice-and-consent framework is inadequate to safeguard privacy. Consumers are generally unaware who has access to their personal information, what data are being used, how and when the data are being used, when the data are being sold, and the privacy implications of the data's use. "Data fusion" (i.e., linking data of diverse types from disparate sources in support of unified search, query, and analysis) may yield potential uses that the consumer never envisioned. Some apps do not even publish a privacy policy. Consumers have little inclination to read the lengthy, detailed, and often opaque privacy notices. Even if they read the privacy notices, consumers generally cannot negotiate better terms."

their positions, because the more data they can gather and analyze, the more sophisticated users' profiles they can hold, the better products and advertising they can offer, the more users they can attract, the more data they can collect and process, and so on.

These concerns animate the German *Facebook* procedure.[68] The Bundeskartellamt moves from the assumption that, because social networks are data-driven products, access to such data is an "essential factor" for competition in the market, and Facebook has superior access to the personal data of its users and other competition-relevant data. On this basis, by focusing on the collection of data from outside Facebook's social network and the merging of these data into users' Facebook accounts, the Bundeskartellamt is concerned that Facebook may use these data to optimize its offer and tie more users to its network. With the data-merging and the identity-based network effects, the locking-in of users would increase, to the detriment of other providers of social networks. Moreover, with the help of the user profiles generated, Facebook would be able to improve its targeted advertising activities, thus becoming even more indispensable for advertising customers.

However, the attention paid by European antitrust enforcers to dominant firms that collect and aggregate data diverges from the U.S. approach. In a recent speech, Barry Nigro, Deputy Assistant Attorney General at the U.S. Department of Justice Antitrust Division, expressed his scepticism at the usage of antitrust laws to force the sharing of data.[69] Rejecting the belief that data may be a source of market power and that access to data may be essential to compete within the market, Nigro relied on *Trinko* in order to state that the

[68] See Kennedy, supra note 56, 2, who, discussing about the concerns regarding data accumulation, wonders whether "the threat to competition is truly due to control of an important resource or to ungrounded fears about the uniqueness of data."

[69] B. Nigro, Remarks at The Capitol Forum and CQ's Fourth Annual Tech, Media & Telecom Competition Conference, New York, December 13, 2017, .

forced sharing of assets would reduce incentives to invest in innovation and would encourage rivals to free-ride on competitors' investments.[70]

Nonetheless, even if concerns that data accumulation may be anticompetitive are taken into account, the task is a difficult one, namely of applying antitrust hypotheses, categories and standards to data, unless antitrust enforcers chose to adopt new provisions and new tools for the unexplored landscape.[71]

As far as data sharing is concerned, the denial of access to an essential input may be considered to be anticompetitive under the essential facility doctrine (EFD). However, this doctrine has proven to be controversial, at the very least. While the EFD has been repudiated in the U.S. and even in the EU, despite its success, its application to data (namely the fulfilment of the 'exceptional circumstances' test) appears problematic.[72] Nevertheless, some data protection provisions help to overcome the fact that some types of data can only be stored on some platforms. In particular, the data portability right, as

[70] Nigro, *supra* note 69: "Data collection, storage, and analysis is not free and not always easily accomplished. Innovative companies - whether they are large tech firms or start-ups - can invest millions of dollars in developing programs to collect data, servers to store data, and computation programs and algorithms necessary to analyze data. It can be years before the firm realizes any type of profit or revenue from its investment, if ever. What motivates a firm to invest in the development of leap-frog technology and innovation? Often, the potential to obtain monopoly profits serves as an important incentive to create better products for consumers." See also Canadian Competition Bureau, 'Big data and Innovation: Implications for Competition Policy in Canada', Discussion Paper (2017), http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04304.html, 16: "Antitrust issues generally do not arise when firms collect more data and antitrust does not usually impose on firms an obligation to share data that they have collected and developed. To do so may very well chill innovation, which is the very behaviour that antitrust is designed to protect."

[71] Nigro, *supra* note 69: "Some have said that we need new tools to address these new data issues. Advocates for new tools tend to cite network effects, and argue that the winner-take-all nature of digital markets and the existence of tipping points mean that the typical means of assessing market power are ineffective. … Existing antitrust tools have been adequate to address these issues in the past, and they are adequate now too. The antitrust agencies have been analyzing network effects and winner take all or most markets for some time. While the existence of network effects is clearly relevant to an antitrust analysis, it does not prevent the use of the existing antitrust framework."

[72] G. Colangelo and M. Maggiolino, 'Big Data as Misleading Facilities', 13 *European Competition Journal* 249 (2017).

envisaged under the new EU General Data Protection Regulation (GDPR), could facilitate competition between digital platforms, reducing switching costs and the risk of the lock-in effect.[73]

Antitrust law also offers other tools for dealing with data accumulation and related concerns. Here, the appropriate (and more effective) instrument is the merger regulation. However, to date antitrust enforcers have not found any potential foreclosure effects, mainly because the data available to the entities resulting from the merger were also available to their rivals. In particular, in *Facebook/WhatsApp* the EU Commission has clearly stated that, notwithstanding the amalgamation of Facebook and WhatsApp user data, "there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control."[74] The Commission's decisions in *Google/DoubleClick,*[75] *Telefonica UK/Vodafone UK/Everything*

[73] Regulation (EU) 2016/679, (2016) OJ L 119/1. Article 20(1) states that "the data subject shall have the right to receive the personal data concerning him or her which he or she has provided to a controller, in a structured commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided." Thus, due to the data portability right, internet users will be allowed to transfer their data between online providers; in addition, they will be able to give their profiles, such as their past search history, to whoever will use them to offer value-added personalized services; furthermore, they will be able to exert influence over the trading and commercialization of their data. See also the French Digital Republic Act (Loi n. 2016-1321, 7 October 2016, pour une République numérique), introducing provisions that, in order to enhance the circulation of data and knowledge, oblige commercial companies to open up (under certain conditions) data they hold for re-use, namely data generated in the context of procurement, commercial data for the establishment of official statistics, certain electricity and gas production and consumption data held by transmission and distribution systems operators for re-use by any other party, and certain data relating to changes in real estate ownership for re-use by certain third parties. However, as highlighted by Körber, *supra* note 8, 18, since the EU Regulation applies regardless of market power as well as regardless of abuses of dominance or any evidence of an actual need for data portability, its competitive impact is at least ambivalent: "An obligation to create data portability can on the one hand promote competition, because taking the data to a new provider is made possible. But on the other hand it burdens companies with costs that start-ups may not be able to afford." Therefore, the data portability provision can also prove to be a barrier to market entry for new companies.

[74] *Facebook/WhatsApp*, *supra* note 60, paras. 188 and 189.

[75] European Commission, 11 March 2008, case COMP/M.4731, para. 365.

Everywhere,[76] and *Microsoft/LinkedIn*[77] followed similar reasoning. After all, in our increasingly networked world, the building blocks of big data are everywhere,[78] data are not rival or exclusive, and multi-homing is a quite frequent phenomenon.

From the antitrust perspective, it is clear why, the German procedure deserves attention and requires detailed investigation — it endorses a different approach that focuses on Article 102(a). Indeed, the Bundeskartellamt also seems to be aware of the hurdles that it would need to overcome in order to establish the exclusionary and anticompetitive nature of the twofold act of embedding Facebook applications into third-party websites and of subsequently accumulating data via them. Therefore, to remain within the boundaries of 'traditional' antitrust law, the GCA sidesteps; it tries to apply Article 102(a) to this behaviour.

Regarding the application of Article 102(a), it seems that the abusive nature of Facebook's practice is rooted in its opacity. However, it has two consequences. First, such a focus on the opacity of contractual clauses easily recalls a privacy concern, namely of showing how an antitrust theory of harm, which is in some senses shaky, uses privacy law as a crutch. Secondly, this link to privacy calls for a remedy that would at most guarantee *fair* data collection, but would not prevent the alleged entrenchment of Facebook's dominant position. Therefore, against the backdrop of an antitrust-privacy interface where the former makes up for the shortcomings within the latter, the Bundeskartellamt is now interpreting the privacy-antitrust interface in the opposite direction: it is using privacy in order to make

[76] European Commission, 4 September 2012, case COMP/M.6314, paras. 543 and 544.
[77] *Microsoft/LinkedIn*, *supra* note 62.
[78] Executive Office of the U.S. President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, 2016, 5.

up for antitrust pitfalls. On the other hand, it is questionable whether this route will lead the GCA to resolve the concern about data accumulation. Therefore, it is apparent that the appropriate way to handle the *Facebook* case would be to conclude that its conduct amounts to an unfair commercial practice. An unfair practice procedure would ensure the same outcome in terms of the remedy, without having to overcome the hurdles of an antitrust investigation.

The time is ripe for antitrust enforcers to appreciate that, in order to address their concerns regarding data accumulation, the most effective tools are not those available under antitrust law, but are instead based on regulatory intervention.