Rivista Italiana di Antitrust
Italian Antitrust Review
N. 1 (2017)
The New Frontiers of Innovation and Competition
Big Data
Case Law

# BIG DATA, DATA PROTECTION AND ANTITRUST IN THE WAKE OF THE BUNDERSKARTELLAMT CASE AGAINST FACEBOOK

**Giuseppe Colangelo**[1], **Mariateresa Maggiolino**[2]

**Keywords:** Antitrust; Big data; Privacy; Multi-sided markets; Free goods

## 1. INTRODUCTION

Information has always shaped the decisions that economic agents take. To determine their supply, firms need to know what consumers want and how their rivals behave. To take purchase decisions, consumers demand to know the potential and actual features of the goods put up for sale. Today, however, a change regarding the availability of this precious resource called "information" is taking place.

In recent years, the quantity and variety of data from which this information can be inferred have incredibly increased at a very high speed.[3] We are witnessing the age of "Big Data",[4] that is, times where technologies can turn empirical phenomena as well as human behavior into sequences of numbers that can be first gathered and then processed to extract information.[5] Likewise, we are witnessing an equally significant number of (online and offline) businesses dedicated to collect, store, analyze, and use such data.[6] Striking examples – at least, for their popularity and revenues – are digital platforms such as Google Search, Facebook, or Amazon, which offer services in exchange for advertising revenues and data.

---

[1] Jean Monnet Professor of EU Innovation Policy, University of Basilicata and LUISS Guido Carli.

[2] Associate professor, Bocconi University.

[3] Here, we are quicky referencing to the so-called "DIKW pyramid" that, though subject to many critiques, is popular among information scientists. According to the DIKW pyramid, information results from data and brings about knowledge and wiseness. See, e.g., D.P. Wallace, *Knowledge Management: Historical and Cross-Disciplinary Themes*, Westport, Libraries Unlimited, 2007.

[4] For a preliminary analysis of the phenomenon and its business implications see, e.g., V. Mayer-Schoneberger, K. Cukier, *Big data. A revolution that will transform how we live, work and think*, New York, Hodder & Stoughton, 2013; and T. Davenport, *Big data at work: dispelling the myths, uncovering the opportunities*, Boston, Harvard Business Review Press, 2014.

[5] Indeed, see Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, 2016, at 5 (observing, «[i]n our increasingly networked world, the building blocks of big data are everywhere»). For other studies analyzing the business impact of big data, see Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, 2014; DotEcon and Analysys Mason (report for the UK Competition and Markets Authority), *The Commercial Use of Consumer Data,* 2015; Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?,* 2016.

[6] See, e.g., H.A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. Pa. L. Rev. 1663 (2013); and L. Einav and J. Levin, *The Data Revolution and Economic Analysis*, in Innovation Policy and the Economy (J. Lerner and S. Stern, eds.), vol. 14, University of Chicago Press, 2014, 1 (on the many scenarios where big data may be used profitably).

Namely, we all know that Internet users get access to the services offered by search engines, social networks, and the e-commerce platforms at zero price. More, we all know that, consistently with the business models of media companies, advertisers pay for those services: advertisers use those services to attract more and more "eyeballs" for the advertising claims that they obtain to display on search engines, social networks and e-commerce platforms.

Yet, today we learn something more. Users who interface with these platforms provide them with personal data that become an important source of business information for the platforms to develop accurate algorithms, better services, and tailored advertising. Firstly, platforms add these volunteered data (the data that users leave them) to the other data that they already hold, such as the observed data (the data collected automatically thanks to crawling and tracking softwares) and the inferred data (the data derived via analysis techniques). Secondly, platforms analyze this rich haul of data to better describe and understand users' needs and wants, as well as rivals' choices, and thus to improve their strategies. In this wake, hence, user data become meaningful for digital platforms that are thus interested in exchanging their services for these data – the new Internet currency.[7]

However – and it is here where "pure" privacy issues peep – this exchange (personal data vs. services at zero price) may violate data protection law in both overt or subtle ways that consumers are not capable to detect. Furthermore, the same exchange might incentivize many ill-educated consumers to overlook the protection of their privacy: the appeal of zero price services could push Internet users to disregard the value of their data and, hence, allow firms to over-intrude in their privacy. Finally, the use of big data intended to profile consumers may deprive them of their digital identities, that is, of the control that they should have on their preferences, their consumption habits, and on all those many characteristics that identify and characterize persons.

But if these are "mere" privacy issues that someone could as well consider as matters of education and consumer protection law, digital platforms may raise data protection law problems that, according to someone, urge antitrust law concerns as well. The present work looks – indeed, with deep skepticism – at this overlap, that is, at the growing demand for an antitrust action directed to neutralize the risks associated with the collection and use of personal user data. Truth be told, some data protection provisions, such as that about data portability reducing switching costs and the risk of the lock-in effect, could facilitate competition among digital platforms.[8] Yet, this is another story to be told.

[7] See, e.g., M.S. Gal and D.L. Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, 80 Antitrust L. J. 521 (2016); J.M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. Pa. L. Rev. 149 (2015); and Shelanski, *supra* note 4.

[8] EU Regulation 2016/679 of 27 April 2016, *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*.

## 2. PRIVACY AND ANTITRUST

In their recent position paper the French Autorité de la Concurrence and the German Bundeskartellamt, though broadly speaking, do not refute the convergence between antitrust and privacy issues.[9] They maintain that, «privacy policies could be considered from a 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».[10]

Then, aside from such a broad approach, four are the main theories of harm that try to comingle privacy and antitrust issues. Two of them trace back to what the former FTC Commissioner, Pamela Jones Harbour, already observed a few years ago. In writing her dissenting statement about the *Google/DoubleClick* merger, she argued that mergers between companies that hold big data, by increasing their joint data booty, would allow the entity resulting from the merger to have even more tools to profile individuals and invade their privacy.[11] Afterwards, by talking of digital markets in a scienfitic publication, she observed that the network effects and the other structural features characterizing these markets strengthen the market power of digital platforms and, thus, decrease their incentives to compete to offer better goods, such as privacy-friendly services.[12]

The third theory of harm bringing together antitrust and privacy issues comes from the elaboration of some law scholars and runs as it follows.[13] Broadly speaking, the quality of

[9] 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.

[10] Autorité de la concurrence and Bundeskartellamt, *supra* note 7, at 23-24, where they further wrote that, «*[E]ven 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*».

[11] P.J. Harbour, Dissenting statement, In the matter of *Google/DoubleClick,* at 4, «*[t]he transaction will combine not only the two firms' products and services, but also their vast troves of data about consumer behavior on the Internet. Thus, the transaction reflects an interplay between traditional competition and consumer protection issues. The Commission is uniquely situated to evaluate the implications of this kind of data merger, from a competition as well as a consumer protection perspective. The Commission should maximize its opportunity to do so, especially where the merged firm will be capable of dominating the "Database of Intentions"*».

[12] P.J. Harbour and T.I. Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 Antitrust L.J. 769 (2010), at 794: «*[C]onsider whether a dominant or potentially dominant firm would have the same incentives to adapt its privacy policies - either in response to consumer demand or as a reaction to competition from other firms. If achieving a dominant market position might change the firm's incentives to compete on privacy dimensions, this is a consequence that antitrust enforcers might wish to explore further*».

[13] See 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); A.P. Grunes, *Another Look at Privacy,* 20 Geo. Mason L. Rev. 1107 (2013); F. Pasquale, *Privacy, Antitrust, and Power,* 20 Geo. Mason L. Rev. 1009 (2013); P. Swire,

products and services may be assessed by taking into consideration whether they are privacy-friendly or not. That is, antitrust authorities may wonder whether a good has been conceptualized and/or offered by intruding in individuals' privacy or not. If we accept to consider that goods which are not privacy-friendly are low-quality goods, then we must conclude that these goods make consumer welfare decrease, because consumer welfare depends not only on prices and quantities (short run effects), but also on quality, variety and innovation (medium-long run effects). Therefore – and this is the conclusion of the reasoning – any practice (a merger,[14] a unilateral behavior, or an agreement) leading to goods which are not privacy-friendly harmm consumer welfare and, hence, must be held anticompetitive.

Finally, the fourth privacy-driven theory of harm is the one used by the Bundeskartellamt in its proceeding against *Facebook*. Here, the German authority is exploring whether, when undertaken by dominant firms, practices that violate data protection law and mislead users can as well be deemed as abuses of dominance pursuant to article 102(a) of the TFEU.

Referencing to the following paragraph for the *Facebook* case, a few words are due in connection to the other above-mentioned theories of harm that do admit some counter-arguments and critiques.[15]

Firstly, it must be recalled that, up to now, EU courts and the European Commission did not use antitrust law as a sward against privacy law violations. Nor have they intended antitrust law to work as a remedy for the flaws and gaps of data protection law. In *Asnef-Equifax*, the Court of Justice established 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».[16] More recently, the Commission has endorsed the very same approach in *Facebook/WhatsApp*,[17] after the FTC 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».[18] Nevertheless, times

*Protecting Consumers: Privacy Matters in Antitrust Analysis*, Center for American Progress, 2007.

[14] To be sure, up to now scholars have been focusing on mergers enabling firms to control more and more big data: see A.P. Grunes and M.E. Stucke, *Big Data and Competition Policy*, Oxford University Press, 2016.

[15] See M.K. Ohlhausen and A.P. Okuliar, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, 80 Antitrust L.J. 121 (2015): «*[S]uch commingling of the competition and consumer protection laws under any of these approaches is unnecessary and could lead to confusion and doctrinal issues in antitrust, without true gains to consumer protection. The history of the FTC's approach to competition and consumer protection offers valuable lessons about the bifurcated, but complementary, nature of the antitrust and consumer protection laws*».

[16] EU Court, 23 November 2006, case C-238/05, §63.

[17] European Commission, 3 October 2014, case COMP/M.7217, para. 164: «*Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*».

[18] Federal Trade Commission, 20 December 2007, case 071-0170, at 2: «*[T]he sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that*

could change and the European and U.S. institutions could explore whether they could use antitrust law to remedy to the gaps and violations of privacy law. For example, in the very recent decision about the *Microsoft/LinkedIn* merger, the Commision observed that, «[p]rivacy related concerns as such do not fall within the scope of EU competition law but can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor. In this instance, the Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction».[19]

Secondly, as to the Harbour's idea that the structure of digital markets conduces firms to offer services that are not as good as privacy-friendly services are, it may be true that firms with high market power are plaugued with a kind of slack and, thus, do not invest to improve their goods. Yet, not only is this lack of incentives not specific of digital markets or digital business models. Not only, no firm has an antitrust obligation to provide the absolute best quality product it can, even if not profit maximizing.[20] Also, as a general matter, antitrust law does not intervene on market features and structure. Thus, with all due respect for data protection law, if network effects and the like are what disincentives digital platforms from producing privacy-friendly services, economic regulation rather than antitrust law should intervene.[21]

Finally, two main counterarguments play against the idea that antitrust law should intervene because of the relationship between privacy law and goods' quality – the same relationship that seems to justify the former corcern raised by Pamela Jones Harbour. First of all, the idea that well-educated consumers would be privacy-sensitive should not be taken for granted.[22] This is an empirical point that should be tested,[23] also to understand – from a "true" antitrust perspective – whether there is a market for privacy-sensitive consumers that

*harm competition. Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry*».

[19] European Commission, 6 December 2016, press release, *Microsoft/LinkedIn*, case M.8124.

[20] See, D.D. Sokol and R. Comerford, *Antitrust and Regulating Big Data*, 23 Geo. Mason L. Rev. 1129 (2016), at 1142.

[21] B.J. Koops, *The trouble with European data protection law*, 4 International Data Privacy Law 250 (2014), at 258.

[22] Likewise, it cannot be taken for granted the idea that if consumers knew the real value of their personal data, they would stop using digital platforms or, more realistically, they would pay for Internet services rather than giving personal data away. 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.

[23] See, e.g, Sokol and Comerford, *supra* note 17; 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).

"someone" (who?) is stifling "somehow" (how?). Indeed, there could be well-educated consumers that, for example, prefer zero-price, personalized, quick services in lieu of privacy-friendly, not accurate, slow services. Thus, even granted that for some consumers the quality of goods decreases when goods result from the analysis of personal data, there could be other users that 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 behaviors invading privacy should not be assumed to be negative; rather, it should be established on a case by case base.[24] And here it comes the second counterargument against the privacy-quality argument. Away from easy assumptions, such as any privacy harm equals a consumer welfare harm, to assess quality is very difficult and, thus, antitrust authorities could have hard times in including privacy-quality issues in their analyses.

In summary, it seems that those supporting the commingling between privacy and antitrust laws would like the latter to work as as a substitute of and a partner for the former. Away from the privacy-quality theory of harm that forces data protection concerns into the traditional antitrust law framework, some scholars maintain that competition law should take a position either to forbid practices that no other piece of law (not even data protection law) prohibits or to fine practices that already consist in privacy law violations. This, at least, is what is happening in the *Facebook* case, indeed.

## 3. The Bundeskartellamt proceeding against Facebook

Recently, the Bundeskartellamt has started a proceeding against Facebook pursuant to article 102 (a) of the TFEU. Facebook has been charged for having abused its dominat position in the market for social networks by imposing some terms and conditions for user data collection in violation of data protection law. According to Andreas Mundt, the president of the Bundeskartellamt, «[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 also examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected».

While waiting for the decision, it seems quite clear that the German authority will overcome some hurdles. Firstly, it will have to prove Facebook's market dominance, after having defined the two-sided market for social newtwork services. Secondly, as the same press

[24] See, e.g., European Commission, *Microsoft/LinkedIn*, *supra* note 17: «*The Commission analysed potential data concentration as a result of the merger with regard to its potential impact on competition in the Single Market. Privacy related concerns as such do not fall within the scope of EU competition law but can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor. In this instance, the Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction*».

release states, the authority will have to demonstrate a link between Facebook's possible dominant position and the privacy violation encompassed in the terms and conditions under scrutiny. Finally, it will have to identify a parameters to demonstrate the unfairness of these contractual terms.

These are three steps that seem quite difficult to meet, and yet in light of the position paper published together with French colleagues, we assume that the German authority may arrive at a different result.

As for Facebook's market position, although the European merger proceedings considered inadvisable to identify a position of hegemony in highly dynamic markets, the Bundeskartellamt could circumscribe the relevant market to that of social network services, rather than to the (wider) market for ad-supported Internet services when other big firms as Google operate. In addition, it is possible that the Bundeskartellamt will focus on network effects and the like to assess Facebook's power. In any event, it should be open to the choice of a relatively reflection.

The next step (the proof of the link between abuse of dominant position and invasion of privacy) will risk to assume the contours of a tautological reasoning about dominance. Indeed, as can be seen from the above disclaimer of Mundt, dominant firms' special responsibility seems to represent the point of departure and arrival of the reasoning so that everything makes sense – better, everything is made to make sense. It should be added that the position paper (co-authored with the French competition authority) expressly states that the policies of privacy are likely to affect competition when they are carried out by a dominant undertaking for which data serve as the main production input.[25]

Arrived at the final hurdle, given the impossibility of identifying an antitrust treshold below which a privacy violation occurs, one could wonder whether the Bundeskartellamt will use the criteria proper of privacy law or will use other parameters to assess unfairness. In the former scenario, the Bundeskartellamt will define an equation between the abuse of dominant position and the invasion of privacy by a dominant undertaking. After all, it is difficult to frame the analysis under subparagraph a) of Art. 102 according to the criteria of moder competition law that does not place unfairness at its heart. Indeed, the European case law on the subject of unfair trade conditions is somewhat limited and not particularly relevant in recent times, whereas consumer protection and unfair commercial practices could be better tools to tackle unfairness.

## 4. CONCLUSIONS

Since Warren and Brandeis times,[26] the debate is animated by proposals that are scrambling in an attempt to balance the expectations of privacy with the benefits of technological development. On the one hand, there are those

[25] Autorité de la concurrence and Bundeskartellamt, *supra* note 7, at 23-24.

[26] S.D. Warren and L.D. Brandeis, *The Right to Privacy*, 4 Harvard L. Rev. 193 (1890).

who defend the free market reasons – government intervention, they argue, should be kept to a minimum, because consumers' demand for privacy will autonomously generate a market for the protection of personal data. On the other hand, there are those who support the urgent need for a government screening of the collection and use of personal data aimed at protecting citizens' privacy against business intrusions.

The specific digital markets' dowry lies in the emergence of business models that revolve around the collection and use of personal data in a context where European data protection laws are not very effective[27] and the U.S. approach towards privacy is not complete or flawless. Thus, one main concern regards user awareness[28] as to digital platforms' ability to trace users' digital behaviors and thus create detailed profiles available to behavioral advertisers.[29] Another concern looks at users' ability to control their digital identities, granted that consent is no more deemed as an effective protection tool.[30] A further concern has to do with pay-for-pricing services whereby users get cheaper Internet services just in exchange for their personal data – services that, hence, could make privacy a luxury good available only to wealthy people.

Not by chance, hence, the FCC drove data value and consumer awareness at the heart of a recent proposal for regulation currently subject to public consultation.[31] There, the FCC proposes, first, to replace the current opt-out mechanism with an opt-in system: the broadband providers that would be required to obtain the prior express consent of users before sharing your 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). In addition, the FCC calls into question the legitimacy of the business models that offer financial incentives in exchange for users' consent to use and share confidential information with third parties.

However, next to all these and other issues that are inherent to the privacy world, we have analyzed the possible comingling between personal data protection and competition law – a comingling which is meant to ensure that privacy violations are also analyzed from the (much more deterrent) antitrust standpoint.[32]

---

[27] Koops, *supra* note 19.

[28] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, 2012, at 56.

[29] A. Acquisti, C. Taylor, and L. Wagman, *The Economics of Privacy*, 54 Journal of Economic Literature 442 (2016).

[30] Koops, *supra* note 19, at 251-252: «*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*».

[31] Federal Communications Commission, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 2016.

[32] See Ohlhausen and Okuliar, *supra* note 13. For a different point of view, see W. Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data*

In this brief work, we showed that this goal could be misplaced and difficult to achieve. To be sure, big data launches new challenges.[33] No one contests the commercial importance that user data play for digital platforms. No one refutes the privacy constitutes an increasingly important component of non-price competition, either. The critical point pertains to the gap between privacy protection and the objectives that competition law is called to pursue.[34] Historically, and in recent times especially in its European version, the antitrust has been subservient to the pursuit of diverse objectives, far from promoting economic efficiency. At the same time, we must remember that such an expansionist drive has been widely condemned, by pointing out the need for the antitrust to mirror economic analysis and economic-driven theories of harm. As the *Facebook* case shows, big data are likely to be an opportunity to turn the clock back and reintroduce in antitrust investigations aspects that have nothing to do with competition.[35]

*Protection*, 7 GRUR Int 639 (2016), (arguing that, for addressing properly the concerns about privacy in the digital economy, it is not sufficient to look for policy solutions only in one field of the law, but that an integrated approach from different regulatory perspectives is necessary).

[33] J.D. Levin, *The Economics of Internet Markets*, NBER workin paper no. 16852 (2011), 28.

[34] According to the EU Commissioner for Competition, Margrethe Vestager (*Making data work for us*, speech at Data Ethics event on Data as Power, Copenhagen, 9 September 2016), «*we can't expect competition enforcement to solve all our privacy problems. Our first line of defence will always be rules that are designed specifically to guarantee our privacy. Rules like the new data protection regulation*». See also Autorità Garante della Concorrenza e del Mercato, 28 October 2016, press release, *WhatsApp* (launching two investigations related to the exchange of personal data with Facebook and oppressive clauses). It is worth noting that, quite differently from the German perspective, the practices at issue are evaluated as potential violations of the Consumer Code instead of the antitrust law. According to the press release, the first proceeding aims to ascertain whether the U.S. company has forced WhatsApp Messenger users to wholly accept the new "Terms and Conditions", in particular 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 could have possibly 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 is directed at ascertaining the possible oppressive nature of some contractual clauses included in WhatsApp Messenger's "Terms of Use" concerning, in particular, 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 to interrupt the service without justifications, the choice of Jurisdiction in case of disputes, which is currently established exclusively in US courts.

[35] Ohlhausen and Okuliar, *supra* note 13: «*[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*».